AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Digital platform services inquiry

Interim report 8: data products and services – how information is collected and used by data firms in Australia

March 2024

Acknowledgement of country

The ACCC acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

Australian Competition and Consumer Commission
Land of the Ngunnawal people
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 03/24
www.accc.gov.au

Contents

Executive summary

Data is at the heart of today's economy. We generate it in almost all aspects of our lives. Virtually all businesses and government agencies collect data in some form. The importance of data only continues to increase with the rise of artificial intelligence (AI).

The collection and use of data is not limited to the online, digital economy. It increasingly powers the 'offline', physical economy, too. It plays an important role in the retail, property, financial services, infrastructure, grocery, and insurance industries, and in key government and business functions such as confirming identity and preventing fraud.

Data enables business and government to provide or enhance the products and services they offer to consumers, citizens and businesses. This contributes to overall economic growth and consumer wellbeing.

The collection and use of data also involves a significant transfer of information from individuals to businesses and government. Data may be collected and used in ways that consumers and citizens expect. However, it is often collected without their genuine awareness, or used in ways they do not expect or may not consider reasonable.

As the data economy has grown, many activities were once anonymous are now subject to detailed data collection. For example, a restaurant that requires you to order via a QR code may require you to share personal information such as your name, email address and mobile phone number.

In practice, it is difficult for consumers to understand or control what happens to such data once it has been collected. This is because privacy policies are typically long and complex, and consumers usually have no choice to accept them, if they wish to access the product or service.

Even if consumers did read privacy policies, they may not appreciate the breadth and depth of data they are agreeing to share, as illustrated in figure 1.1.

Figure 1.1: Examples of data that may be held on consumers

All this means that consumers are unlikely to have the opportunity to exercise choice or meaningful control over their data. This may be particularly problematic when consumers are required to provide personal information or other data on themselves to access important services, such as applying for a rental property or seeking quotes for services such as insurance.

Given the large amounts of data collected across the economy, data breaches and misuse of data can have significant impacts on individuals. Such incidents can also damage the very businesses that are collecting and using the data. This all has the potential to affect trust in the overall economy.

The importance of data may also mean that businesses have incentives to restrict or limit other businesses' access to data. This may be through acquiring other firms with unique or exclusive datasets, or placing limitations on the way their data may be used.

The significant role and use of data has important implications for consumer protection and competition, as well as privacy, data protection and broader issues such as national security. Accordingly, understanding how data flows is critical to understanding how the economy now operates. It is also important for the safety and security of Australian citizens and businesses.

Given the limited timeframe for this Report, the Report does not provide a comprehensive picture of data collection and use across the economy. It does, however, provide a snapshot of some data products and services, with a view to providing greater clarity on how products and services in this dynamic industry are now being supplied.

Focus of this Report

The data products and services that are the subject of this Report encompass data collection, storage, supply, processing and analysis services by firms that do not generally have a direct relationship with the consumer or individual the data is collected from. We refer to these as 'data firms'.

Information collected by data firms

Information or data underpins the products and services provided by data firms.

Data collected by data firms can include a wide range of categories, such as:

- identifying information (e.g. name, address, email address and phone number)
- demographic data (e.g. age, gender and marital status)
- financial and transaction data (e.g. income, debts, purchase history and habits)
- location data (e.g. from mobile phones, transactions, online activities and navigation services)
- interests and preferences (either gathered directly, such as through surveys or subscriptions, or inferred from online or offline behaviours).

Data may be collected in a range of ways:

- Individuals may explicitly share information about themselves, such as their name and age (volunteered data[1]).
- Data may be captured about an individual's activities, such as via their web browsing history (observed data).
- Data may be created through data analytics that processes volunteered and observed data and combines it with other data (inferred or derived data).
- Data may be acquired from other parties.

A key example of observed data is an individual's location data. Location data is often obtained from mobile devices, including from apps that sell location data to other parties. Location data alone can be used to work out an individual's home address to a high degree of accuracy, even when the individual has not volunteered that information. It can also be combined with other data, such as transaction records, to identify an individual's movements and activities.

Data is also collected by government agencies, such as the Australian Securities and Investments Commission (ASIC), IP Australia, the Australian Taxation Office (ATO), state and territory land titles offices, and law enforcement agencies. Data firms often access data made available by government agencies to incorporate it into their datasets and the data products and services they offer.

Data products and services offered by data firms

Data firms offer a diverse range of data products and services that play an important role in the economy and have a range of benefits for businesses that use them. These include data products and services related to marketing and advertising, risk management and property services.

Data firms provide and facilitate a range of data-driven marketing and advertising products. This wide range of services assists business customers to identify, understand and reach their target audiences, deliver advertising content to those audiences, and measure the efficacy of those advertising activities and campaigns.

[1] We note that while consumers may 'voluntarily' provide this data to a business, as discussed in chapter 5, they may be required to do so to access a product or service. They may also not be aware that this volunteered data may be shared with other parties, nor who those parties may be.

A number of data firms also provide risk management products and services. These help business customers confirm the identity or other information provided by an individual, and prevent, detect and address fraudulent activity.

Some data firms supply property data and analytics services. These services include property data platforms, rental technology (RentTech) platforms, and construction and commercial property products. They support individuals and businesses looking to buy, sell or lease property, as well as businesses involved in property transactions and development.

The supply of data products and services in Australia is dynamic and continuously evolving. Beyond the direct sharing of personal and other information, data firms now often employ sophisticated proprietary data analytics techniques and use data management platforms in providing data products and services.

Lack of awareness of the use and collection of consumers' data

Many consumers are unaware of the extent to which data is collected on them and how that data may be used by data firms and others.[2]

Information about data collection and use is often contained in long and complex privacy policies. It has been estimated that if Australian consumers were to read all of the privacy policies they encounter in full, this would take nearly 46 hours every month, as shown in figure 1.2.

Figure 1.2: The approximate length and time taken to read an average privacy policy in Australia per month[3]

Understandably, many consumers do not engage with privacy policies, and in any event, usually have no choice but to accept the terms and conditions of use in order to access a product or service. This raises the question of whether this can be considered informed consent.

Further, privacy policies often contain broad terms and conditions that facilitate the sharing of consumer data with third parties. As these parties are often not identified, consumers are unable to determine who their information has been shared with.

Consequently, consumers are unable to exercise choice or meaningful control over their data. This is particularly problematic when consumers are required to use a data-related

[2] UNSW Allens Hub (K Kemp and G Greenleaf), Submission to the Report, 28 September 2023, p 8; Salinger Privacy, Submission to the Report, 28 September 2023, p 12; CPRC, Submission to the Report, 28 September 2023, p 3. Consumer surveys reviewed by the ACCC in preparing the Customer Loyalty Schemes Report suggested that many consumers are concerned about the sharing of their data with unknown third parties, targeted advertising, and whether their data is being used responsibly. See ACCC, Customer Loyalty Schemes: Final Report, 3 December 2019, p 55.

[3] Mi3, Aussies face 10-hour privacy policy marathon, finds study, 6 November 2023, accessed 15 March 2024.

product to access an important service, such as when applying for a rental property or seeking quotes for services such as insurance.

Data firms' products and services often use de-identified data, which is not necessarily subject to the *Privacy Act 1988* (Cth). 'De-identification' refers to the process of transforming personal information into information that is no longer about an identifiable or reasonably identifiable individual. The use of de-identified data may have some benefits for consumers' privacy. For example, it may lessen the amount of personal information that may be compromised in the event of a data breach.

However, even where data has been de-identified, there is a risk of it being re-identified in the future. This includes where de-identification processes are not applied correctly.

It can also occur where de-identified datasets are combined with additional data, enabling an individual to be identified based on unique characteristics within the combined dataset.

Further, even where the immediate identity of a person in a dataset is not known, it can still be possible to target consumers at a group or individual level, using only de-identified data.

Potential consumer harms

There are a range of consumer issues that may arise from data firms' collection and use of consumer data. Given that data firms can hold information on almost all Australians, there is the potential for significant overall consumer detriment where such harms occur.

The ACCC acknowledges that the likelihood of consumer harm occurring may differ significantly depending on the particular product or service in question.

The targeting of consumers based on information linked to them that is collected and shared without their explicit knowledge has the potential to result in discrimination and/or exclusion in how businesses offer services to consumers. This may be due to specific targeting itself, or from inaccurate data being used to profile a consumer.

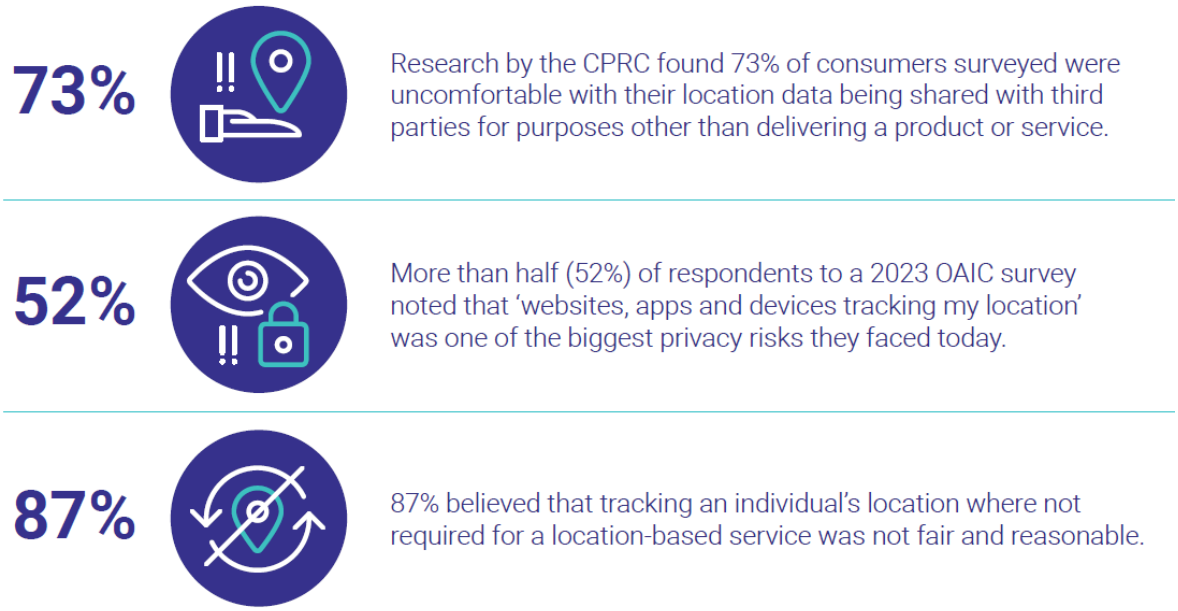
Consumers are often placed into 'segments' by data firms to enable businesses to categorise their existing customers and identify potential customers. These segments group together people based on common characteristics, such as 'households with young children' or 'those likely to purchase a budget holiday package'. These may be for innocuous purposes, such as a 'dog owner' segment being used to deliver targeted advertising for discounted pet food.

However, there is a risk of consumer segments being used to target vulnerable groups in potentially harmful ways. For example, a segment identifying people as 'frequent gamblers' may be used to serve gambling ads to people who may have a gambling addiction. Even if such sensitive segments are not available, there may be ways to combine other data points to achieve similar results. For example, combining location data on visitors to a particular address with data showing the address is a place of worship could serve as a proxy for a segment likely to include people of a particular faith.

There is also a risk that some data products and services may be misused by bad actors. Several submissions raised concerns that data products and services can facilitate, or contribute to risks of, scams and fraud activity in Australia. Some also raised concerns about the potential misuse of location data on individuals. A recent survey by the Consumer Policy Research Centre (CPRC) indicated that 87% of Australians believed that tracking an

individual's location when not required for a location-based service was not fair and reasonable, as shown in figure 1.3.

Figure 1.3: Consumer concerns regarding the collection and use of their location data[4]



Finally, data firms typically collect large volumes of data on consumers. This scale of data collection can make such firms attractive targets for cyber-criminals, potentially resulting in significant consumer harm arising from a data breach, cyber-attack or other data security incident.

Relevant measures

The ACCC continues to strongly support the implementation of privacy measures to better empower consumers, protect their data and support the digital economy.[5] The ACCC considers that the privacy-related issues discussed in this Report are best addressed in the first instance through strengthened privacy laws, supported by the allocation of further resources to the Office of the Australian Information Commissioner (OAIC).

In particular, as set out in its submission to the Privacy Act Review Report, the ACCC continues to support the following proposals from the review, which have been agreed in-principle by government:

- the proposed introduction of a right for an individual to have any of their personal information erased
- the proposed amendments to clarify the definition of personal information, including by changing the word 'about' to 'relates to' and listing some types of information that may be personal information
- the introduction of a 'fair and reasonable' test for the collection, use and disclosure of personal information.

4 CPRC, 2020 Data and Technology Consumer Survey, accessed 15 March 2024; OAIC, Australian Community Attitudes to Privacy Survey, August 2023, pp 23, 52.
5 ACCC, Privacy Act Review Report – ACCC submission, 31 March 2023.

This could be complemented by a registry of data firms, as seen in several US states, to support consumers to exercise such a right of erasure. This could assist consumers to identify which firms hold their data and potentially enable them to make a single deletion or 'do not collect' request.

However, we note certain practices that give rise to potential consumer harms in relation to data go beyond issues covered by privacy laws and any strengthening of privacy laws.

Certain issues around data use and misuse may be covered by existing provisions of the Australian Consumer Law (ACL). The ACCC also continues to support the introduction of an unfair trading practices prohibition to enhance protections for consumers and small businesses, including with respect to the issues explored in this Report.

Market dynamics

Data firms employ different approaches to pricing products and services, in part reflecting the breadth of what they offer. These include pricing models such as pay per use/transaction, subscription models and licensing models. It also includes non-monetary forms of consideration, such as reciprocal agreements to exchange information or services.

Despite these different approaches to pricing, the ACCC has observed that data firms compete mostly through non-price dimensions. These include:

- product differentiation by way of data analytics expertise or data infrastructure
- data firms differentiating themselves through access to, or use of, unique datasets or high-quality data
- data firms competing by improving the privacy and data security of their products and services.

Noting the level of product differentiation and industry specialisation among data firms, the ACCC also observes that some business customers use the products and services of multiple data firms as inputs to their own products or services.

Potential incentives to restrict access to data

Competition concerns may arise under the *Competition and Consumer Act 2010* (Cth) if a firm places restrictions on access to unique or exclusive datasets by rivals or potential downstream buyers, in a way that deters, hinders, or prevents competition.

Mergers and acquisitions by data firms are extensive. They are often used to build up the portfolio of a data firm's products and services.

However, mergers and acquisitions could provide the acquirer with the ability to restrict access to important datasets. Data firms may also be incentivised to put in place contractual limitations in their agreements with business customers or data suppliers, to limit others' access to data. This may have the practical effect of foreclosing rivals[6] horizontally or vertically, especially in certain industry sectors where only a small number of data firms offer services.

Incentives for data firms to restrict access may also overlap with privacy. Businesses may compete partly on the extent to which they protect individuals' privacy or the security of the

[6] Foreclosure refers to when a firm prevents or impedes a rival firm from competing.

data they collect. However, firms may also limit the amount of data they share with others, ostensibly to protect consumers' privacy, but in a way which can also limit the ability of others to compete.

Previous ACCC work on data

The ACCC has explored data collection and use in a range of previous inquiries. We have considered the collection and use of data by digital platforms in a series of inquiries into digital platform markets since 2017.[7] We also considered how customer loyalty schemes collect and use data in a 2019 report.[8]

Other areas of our work have also analysed data and how consumers are informed about its collection. In recent years, the ACCC has taken successful court action against Google for misleading consumers about personal location data collection,[9] and against Meta subsidiaries for misleading the public about the collection and use of data collected by the Onavo Protect VPN app.[10]

The ACCC's work in relation to data includes its responsibilities in relation to the Consumer Data Right scheme, which is an initiative to enable data sharing that supports consumer choice and competition. And data forms an integral part of our work in other roles such as Digital Identity and the National Anti-Scam Centre.

Only one part of the data ecosystem

In this Report, we consider an aspect of the data ecosystem that has not previously been studied by Australian regulators. That is, the data collection, storage, supply, processing and analysis services of firms that do not generally have a direct relationship with the consumer or individual the data is collected from.

The Ministerial direction for the Digital Platform Services Inquiry calls for, among other things, an inquiry into the data collection, storage, supply, processing and analysis services supplied by data brokers. The Direction defines a data broker as a supplier who collects personal or other information on persons, and sells this information to, or shares this information with, others.

Data products and services supplied today are not limited to what consumers or business customers might understand as a more traditional notion of 'data broking'. Such traditional forms may include businesses purchasing, selling or exchanging lists of consumer data with each other, such as names, addresses and phone numbers. Firms that deal with data now supply a much broader and diverse set of services.

We also observe that most data-focused firms do not describe themselves as 'data brokers'. A number objected to being termed a 'data broker' in the Issues Paper for this Report. We also note that the term 'data broker' has a specific, and in some cases different, definition in other jurisdictions, some of which have associated regulatory obligations.

Firms use a variety of different terms to describe themselves, such as 'information services companies', 'data and analytics businesses', or 'data collaboration platforms'. In this Report,

7 ACCC, Digital platforms and services, accessed 15 March 2024.
8 ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019.
9 ACCC, Google LLC to pay $60 million for misleading representations, 12 August 2022, accessed 15 March 2024.
10 ACCC, $20m penalty for Meta companies for conduct liable to mislead consumers about use of their data, 26 July 2023, accessed 15 March 2024.

we describe firms that offer data collection, storage, supply, processing and analysis services as ‘data firms’.

Separately, we note that because of the diversity of products and services they offer, and their different business models, we do not consider that the firms mentioned in this Report are necessarily directly comparable. Nor do we necessarily consider them direct competitors.

Further work on the broader data ecosystem

The ACCC acknowledges that this Report considers only a portion of the data ecosystem, that is, the data products and services offered by data firms that generally do not have a direct relationship with the consumer.

Data collection by firms directly from their customers is even larger in scope.

Accordingly, the ACCC considers that further work should be undertaken by government to understand the flow of data more broadly across and around the Australian economy.

Glossary

Term	Description
ACCC	Australian Competition and Consumer Commission
ACL	The Australian Consumer Law, contained in Schedule 2 of the *Competition and Consumer Act 2010* (Cth).
ACMA	Australian Communications and Media Authority
Ad Tech Report	The final report of the ACCC's Digital advertising services inquiry, published on 28 September 2021.
Application Programming Interface or API	A computing interface that allows interactions between multiple software programs, such as apps and the OS (operating system), for the purpose of simplifying programming.
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
Australian Privacy Principles or APP	The Australian Privacy Principles (APP) are contained in Schedule 1 of the *Privacy Act 1988* (Cth). They govern standards, rights and obligations around the handling and protection of personal information in Australia. *See also Privacy Act*.
Business-to-business or B2B	Refers to situations where one business enters into an arrangement or makes a transaction with another.
Business-to-consumer or B2C	Refers to situations where a business enters into an arrangement or makes a transaction with a consumer.
CCA	*Competition and Consumer Act 2010* (Cth)
CFPB	Consumer Financial Protection Bureau, US
Consumer data	Personal or other information on persons. This may include personal information, such as names, home addresses, email addresses, phone numbers, credit

	information and sensitive information. It may also include de-identified or pseudonymised information (such as hashed email addresses or mobile advertising identifiers) and other information on persons which is not necessarily personal information.
Customer Loyalty Schemes Report	The final report of the ACCC's review of customer loyalty schemes, published on 3 December 2019.
Customer relationship management or CRM	Software used by businesses to manage their relationships and communications with existing and potential customers.
Data aggregation	The process by which data is gathered, collated and presented in summarised form for subsequent data sharing and analysis. *Data aggregation is discussed in detail in box 1.2.*
Data broker	A supplier who collects personal or other information on persons, and sells this information to, or shares this information with, others (as defined in the Ministerial direction). *See also data firm.*
Data clean room	A digital environment designed for businesses to share and collaborate on the customer data they hold, to enhance and enrich the quality of their own existing datasets without directly sharing these datasets with each other. *Data clean rooms are discussed in detail in box 3.2.*
Data firm	Businesses which supply data products and services, including those which lack a direct relationship with the consumers whose personal or other information they collect, use, process, analyse, supply or otherwise deal with. This Report generally uses the term 'data firm', rather than 'data broker', to refer to suppliers of data products and services. *The terms 'data broker' and 'data firm' are discussed in detail in section 1.1.*

Data marketplace	An online platform which allows business customers to buy, sell or exchange consumer data.
Data products and services	Data collection, storage, supply, processing and analysis services, as described in s 5(2)(c) of the Ministerial direction.
Data pseudonymisation	The process of replacing direct identifiers, such as a consumer's name or email address, with a value which does not directly identify the consumer, such as a reference number or hashed code. *Pseudonymisation is discussed in detail in box 1.2.*
Derived data	Data created by processing and combining existing data but which cannot be readily identified in the original dataset. It can also be known as 'inferred data'. For example, an individual's religion may be derived from location data showing they visit a particular place of worship each week, or a business may infer that a consumer has a particular health condition based on their search history, purchase history at pharmacies and visits to medical facilities.
Digital Platforms Inquiry or DPI	The original Digital Platforms Inquiry (2017-2019). An inquiry conducted by the ACCC into digital search engines, social media platforms and other digital content aggregation platforms, and their effect on markets for media and advertising services.
Digital Platform Services Inquiry, DPSI or the Inquiry	Digital Platform Services Inquiry (2020-2025). The ACCC's 5-year inquiry into the supply of digital platform services, digital advertising services and data collection, storage, supply, processing and analysis services by digital platforms and data brokers. This Report on data products and services is the eighth interim report of the DPSI.
Direction or Ministerial direction	*Competition and Consumer (Price Inquiry – Digital Platforms) Direction 2020.* Under the Ministerial direction, the ACCC is directed to conduct an inquiry, and give an interim report to the Treasurer every 6 months (between September 2020 and March 2025), into the markets for the supply of digital platform services

	(including data collection, storage, supply, processing and analysis services).
Enrichment	The process of improving or augmenting a firm's existing data holdings by adding other data, often from an external source.
First-party data	Information collected by a business directly from its own customers.
FTC	Federal Trade Commission, US
Hashed or hashing	A data pseudonymisation technique which involves replacing direct identifiers (such as names and email addresses) with random alphanumeric codes generated by an algorithm. *See also data pseudonymisation.*
ICO	Information Commissioner's Office, UK
IP address	Internet Protocol address, a numeric address assigned to each device connected to a local network or the internet via the Internet Protocol.
Issues Paper	The Issues Paper for the eighth interim report of the Digital Platform Services Inquiry, published on 10 July 2023.
Mobile advertising identifier or MAID	A unique, pseudonymous identifier tied to an individual mobile device and generated by its operating system. A MAID enables advertisers to track user activity on the device for advertising purposes, including to help them target ads and measure the performance of their campaigns. Typical MAIDs include the Identifier for Advertisers (IDFA) on iOS devices and Advertising ID (AdID) on Android devices.
OAIC	Office of the Australian Information Commissioner
Observed data	Data captured by observing users' behaviour, events or other occurrences, such as browsing history, time spent and clicks performed on a web page. This term also captures data derived from users' devices, such as type of device, operating system and its version, browser and IP address, and location data if their privacy permission settings allow.

Personal information	Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable (as defined in section 6(1) of the Privacy Act).
Privacy Act	*Privacy Act 1988* (Cth). The Privacy Act, including the APPs, applies to Australian Government agencies and most organisations with an annual turnover of more than $3 million. Some small business operators (organisations with an annual turnover of $3 million or less) are also captured by the Privacy Act, including private sector health service providers and businesses that sell or purchase personal information. *The Privacy Act is discussed in detail in section 1.5.1.*
Privacy Act Review	A review of the Privacy Act led by the Attorney-General's Department, which published a final Privacy Act Review Report 2022 in February 2023. The government released its response in September 2023. *The Privacy Act Review is discussed in detail in section 1.5.2.*
Profiling	The process of combining data collected about an individual consumer from various sources to create an understanding of the individual.
Regulatory Reform Report	The fifth interim report of the DPSI on regulatory reform, published on 11 November 2022. This report made a range of recommendations to address harms from digital platforms to Australian consumers, small businesses and competition. This report also reiterated the ACCC's support for economy-wide reforms to consumer law.
Report on App Marketplaces	The second interim report of the DPSI on app marketplaces, published on 28 April 2021.
Report on General Online Retail Marketplaces	The fourth interim report of the DPSI on general online retail marketplaces, published on 28 April 2022.

Report on Online Private Messaging Services	The first interim report of the DPSI on online private messaging, search and social media services, published on 23 October 2020.
Report on Search Defaults and Choice Screens	The third interim report of the DPSI on web browsers, general search services and choice screens, published on 28 October 2021.
Report on Social Media	The sixth interim report of the DPSI on the provision of social media services in Australia, published on 28 April 2023.
Sample firms	The term used in this Report to refer to the 9 data firms named in the Issues Paper for this Report – CoreLogic, Equifax, Experian, illion, LiveRamp, Nielsen, Oracle, PropTrack and Quantium.
Second-party data	An industry term which generally refers to data that a business purchases from a supplying entity that collected the data directly from its customers. For example, if a business agrees to share its first-party data with another business, that data would become second-party data to the recipient.
Segmentation	The process of grouping together a number of people roughly based on common or similar characteristic, such as age, gender, religion, income level, ethnicity, interests or lifestyles.
Suppress or suppression	The exclusion or removal of particular data points from a dataset or list. For example, data suppression services may allow an advertiser to avoid sending direct marketing emails to consumers who have opted out of receiving such communications.
Third-party data	Data obtained from a source other than the consumer or the original collector of the data. For example, data collected about a consumer's interactions with a third-party website or app, which a business purchases from a data firm, to supplement the 'first-party' data it may have already on the consumer. Data may also become third-party data, such as if a data firm purchases another data firm's second-party data.

1. Introduction

1.1. Scope of this Report

In February 2020, the Treasurer directed the ACCC to conduct a 5-year inquiry into markets for the supply of digital platform services (Digital Platform Services Inquiry or the Inquiry). The Direction provides that the Inquiry is to be held in relation to goods and services of the following descriptions:

(a) digital platform services;

(b) digital advertising services supplied by digital platform service providers;

(c) data collection, storage, supply, processing and analysis services supplied by:

i. digital platform service providers; or

ii. data brokers.

This Report considers those aspects underlined above, that is, data collection, storage, supply, processing and analysis services (referred to in this Report as 'data products and services') supplied by data brokers in Australia.[11]

The Direction defines a data broker as 'a supplier who collects personal or other information on persons, and sells this information to, or shares this information with, others.'[12] This definition of 'data broker' encompasses information that is broader than 'personal information',[13] as it also includes 'other information on persons.'[14] In this Report, we refer to this overall concept of 'personal or other information on persons' as consumer data.

This Report focusses on the data products and services of a subset of these firms, namely those which do not generally interact directly with the consumers whose data they collect, license, analyse, sell or share.[15] This Report generally refers to these entities that supply data products and services in Australia as 'data firms'.

The focus in this Report on firms that do not generally interact directly with consumers complements previous ACCC work on how digital platforms and other firms may collect data directly from consumers, and sell or share it with others (this is discussed further in chapter 2).

This focus is also intended to inform government and other readers about practices that many Australians are unaware of.

11 *Competition and Consumer (Price Inquiry – Digital Platforms) Direction 2020*, s 5(2)(c).
12 *Competition and Consumer (Price Inquiry – Digital Platforms) Direction 2020*, s 4.
13 In the context of Australia's Privacy Act, the term 'personal information' means information or an opinion about an identified or reasonably identifiable individual, whether the information or opinion is true or not and whether it is recorded in a material form or not. See *Privacy Act 1988* (Cth), s 6.
14 ACCC, Digital Platform Services Inquiry, Issues Paper to the Report, 10 July 2023, pp 2–4; *Competition and Consumer (Price Inquiry – Digital Platforms) Direction 2020*, s 4.
15 ACCC, Digital Platform Services Inquiry, Issues Paper to the Report, 10 July 2023, p 4.

1.1.1. Credit reporting services and the operation of the Privacy Act are not considered in this Report

The Report does not review the credit reporting products and services offered by credit reporting agencies in Australia (including Equifax, Experian and illion), as these products and services are regulated separately under Part IIIA of the Privacy Act.[16]

The ACCC acknowledges that some consumer data used in credit reporting products and services may be de-identified and used for other purposes, or shared with others, including in connection with the types of data products and services that are considered in this Report. (De-identification practices are discussed in box 1.2, while the potential for data to be re-identified is discussed in chapter 5.) The ACCC also notes that an independent review into the operation of Australia's credit reporting framework, including Part IIIA, was recently announced and is due to be provided to the Attorney-General by 1 October 2024.[17]

More broadly, and in line with the Ministerial direction, the Report does not 'review the operation of' the Privacy Act.[18] The ACCC acknowledges there has been significant work undertaken to consider reforms to Australia's existing privacy regime over the past few years. Should they be enacted, many of these proposed reforms may have implications for the data products and services discussed in this Report. For this reason, section 1.5 provides an overview of the existing Privacy Act and the recommendations made in the Privacy Act Review Report.

1.2. Structure of this Report

The remainder of this chapter introduces the types of data products and services offered by data firms and how these have evolved over time (section 1.3), provides context on the importance of consumer data to the digital economy through the lens of past ACCC work (section 1.4), sets out a high-level summary of the relevant aspects of the existing Privacy Act and recommendations arising from the Privacy Act Review Report (section 1.5), and provides an overview of known overseas inquiries, reports, enforcement action and legislation relating to data brokers (section 1.6). This Report is then broken down into 5 further chapters which cover the following topics.

Chapter 2 explains the variety of ways in which consumers and businesses generate data in their day-to-day activities and why organisations are motivated to collect that data. It also describes challenges organisations can face in collecting data, and how such challenges can be overcome, including by acquiring products or services from a data firm.

Chapter 3 sets out the main categories of data products and services supplied in Australia: marketing and advertising products and services, risk management products and services, and data-driven property products and services.

Chapter 4 provides an overview of a range of firms that supply the data products and services described in chapter 3. It focuses primarily on 9 sample firms that supply the relevant types of products and services in Australia, but also notes a range of other firms that also supply some of these services in Australia. Chapter 4 also provides a high-level overview of the ways in which data firms supply data products and services in Australia.

16 See *Privacy Act 1988* (Cth), Part IIIA.
17 Attorney-General's Department, Review of Australia's Credit Reporting Framework, 27 February 2024, accessed 15 March 2024.
18 ACCC, Digital Platform Services Inquiry, Issues Paper to the Report, 10 July 2023, p 11.

This includes key sectors that business customers of these firms operate in, and the terms on which data firms supply their data products and services.

Chapter 5 outlines a range of potential consumer harms that may stem from the collection and use of consumer data in Australia. These include possible issues around:

- consumers' understanding, awareness and control (or lack thereof) over how their data may be collected by and shared with third parties
- risks from the use or misuse of consumer data.

Finally, **Chapter 6** sets out the market dynamics of firms providing data products and services in Australia. This includes the ACCC's observations of how such firms specialise in product types or industries, how they compete, and merger and acquisition activity relating to them. Chapter 6 also discusses how these firms' products and services may interact with those provided by digital platforms.

1.3. Data products and services offered by data firms

Data firms supply a range of data products and services to business customers across many industries for a variety of purposes. As set out in chapter 3, these include:

- Data-driven marketing and advertising products and services, which include enrichment, profiling, segmentation, targeted advertising, and ad measurement and optimisation products and services. Broadly, these are designed to support business customers' marketing activities by improving their data relating to their target audiences.
- Risk management products and services, including verification services that help to confirm an individual's identity or other information they have provided. Some of these products and services also assist with fraud detection and prevention.
- Property data and analytics services, encompassing PropTech (such as property data platforms), RentTech platforms, and construction and commercial property products. Renters, buyers and property professionals may use these services to research, buy, sell and manage properties.

This Report analyses matters relating to the supply of data collection, storage, supply, processing and analysis services, and conducts that analysis with reference to firms that supply those services.

The Issues Paper for this Report identified 9 firms as illustrations of firms operating in Australia which the ACCC considered provided the types of data products and services that are within the scope of the Inquiry.[19] The firms were initially identified through desktop research and are not intended to represent a comprehensive list of firms that provide data products and services. Chapter 4 sets out a profile of these 9 firms, which for the purposes of that chapter are categorised as:

- Credit reporting agencies: Equifax, illion and Experian
- Property data firms: CoreLogic and PropTrack
- Data analytics and other data firms that supply data products and services: Oracle, Quantium, LiveRamp and Nielsen.

[19] The identification and naming of these 9 sample firms in the Issues Paper occurred as a result of ACCC research which considered the publicly available information of these 9 firms.

Some submissions received in response to the Issues Paper identified additional firms for consideration in this Report.[20] Chapter 4 highlights a number of other data firms that offer the data products and services considered in this Report.

The purpose of identifying particular firms in this Report is to illustrate to stakeholders the kinds of data products and services offered by these and other firms in the industry.

1.3.1. Evolution of the data broking industry and terminology

Through its research and stakeholder submissions on the matters relevant to this Report, the ACCC understands that over time there has been an evolution in the nature of the supply of data products and services, and in the types of firms that supply those services in Australia. This has involved an expansion beyond more 'traditional' data products and services, such as those that enable businesses to purchase, sell or exchange personal information,[21] to incorporate the kinds of broader data products and services discussed in chapters 3 and 4.

Given this evolution, the ACCC considers that what may have been typically understood, particularly by consumers, by the terms 'data broker' and 'data broking' may not fully capture the suppliers and the products and services that are important parts of the modern Australian data ecosystem that this Report focusses on.

Firstly, the variety of data products and services offered by data firms in Australia today extends well beyond what may have been typically understood by the term 'data broking'. For example, as discussed in chapter 4, this includes products and services designed for use in marketing and advertising, risk management and property data analysis. Not all of these products and services necessarily involve the direct exchange of personal information, as may have been associated with 'traditional' data broking services.[22]

Secondly, the ACCC has observed that many firms which operate in Australia's data ecosystem do not characterise themselves as 'data brokers'. For example, several of the sample firms named in our Issues Paper instead use terms such as 'data and analytics business'[23], 'data analytics firm'[24] and 'data collaboration platform'[25], or state that they offer data-based 'tools'[26], 'insights'[27], 'information services'[28] or 'data analytics services'.[29] In addition, some firms submitted that they share little or no personal information with third

[20] Salinger Privacy, Submission to the Report, 28 September 2023, pp 4–5, 14; Reset.Tech Australia, Submission to the Report, 28 September 2023, pp 2–4.

[21] For example, through certain types of online data marketplace (discussed in box 2.2 of this Report) that involve the sale or exchange of personal information. A data marketplace is a platform which allows businesses to buy, sell or exchange consumer data with each other, or with the data firm operating the marketplace. For example, Oracle's US business offers what it describes as the world's largest third-party data marketplace, with data on over 300 million internet users – see Oracle, Oracle Data Marketplace, accessed 15 March 2024 (though note that Oracle's Australian business does not offer this product). For an earlier discussion of data marketplaces in a US context, see FTC, Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data, 13 March 2001, accessed 15 March 2024.

[22] For example, IAB Australia submits that the practices of "data brokers" and other organisations which handle data have changed significantly in recent years, and the industry 'has evolved from accumulation of email lists to the point where they now provide comprehensive services' to businesses which seek to operate effectively online. See IAB Australia, Submission to the Report, 28 September 2023, p 5.

[23] Illion, Submission to the Report, 28 September 2023, p 2.

[24] Quantium, Submission to the Report, 28 September 2023, p 1.

[25] LiveRamp, Submission to the Report, 28 September 2023, p 3.

[26] LiveRamp, Submission to the Report, 28 September 2023, p 3; PropTrack, Submission to the Report, 28 September 2023, p 1.

[27] PropTrack, Submission to the Report, 28 September 2023, p 1.

[28] Equifax, Submission to the Report, 28 September 2023, p 16.

[29] Nielsen, Submission to the Report, 28 September 2023, p 1.

parties in supplying their data products and services in Australia.[30] These submissions are discussed in box 1.1.

The ACCC considers that the evolution of the data industry described above may be attributed to a range of developments. Some of those the ACCC include:

- As consumers continue to spend significant amounts of time online making purchases, attending work or school and socialising with their friends and family members,[31] the amount of data collected about their interests, preferences and behaviour has continued to expand. As a result, there has been an expansion in both the types of consumer data that may be collected, as well as the volume of information available for businesses to access, or for data firms to use in their data products and services.[32]
- Several high-profile data breaches in Australia have led to a sharp rise in consumer concern about such incidents, according to a recent survey by the Office of the Australian Information Commissioner (OAIC).[33] In the same survey, consumers viewed privacy as the third-most important factor when choosing a product or service, behind quality and price but ahead of reputation, reliability and convenience[34], and 82% of consumers said they cared enough about their privacy to do something about it.[35] As a result of this growing consumer consciousness of privacy issues[36], it is likely that many advertisers which wish to gather data on consumers may seek to minimise the amount of personal information they collect.
- Digital platforms making changes to their privacy policies and practices, including browser restrictions to limit third-party cookies and tracking. For example:
  - Apple introduced its AppTracking Transparency Framework (ATT) in April 2021, which amended its identifiers for advertisers (IDFA) system. All apps must use the ATT to request the user's permission to track them or to access their device's advertising identifier. Unless developers receive this permission from the user, the device's advertising identifier will be all zeros and developers may not track them[37], which may reduce developers' ability to supply targeted advertising.[38] However, it is worth noting that Apple is offering its own advertising tools for developers to use instead.[39] It has also been reported that app developers including Snap and Facebook have been allowed to continue collecting consumer data from iOS users, as long as the data 'is anonymised and aggregated rather than tied to specific user profiles'.[40]

30 For example, see PropTrack, Submission to the Report, 28 September 2023, p 1; Quantium, Submission to the Report, 28 September 2023, p 1.

31 For example, in January 2024, Australians spent an average of 6 hours and 14 minutes online per day, compared to 5 hours and 51 minutes in January 2023. See S Kemp, Digital 2024: Australia, *Data Reportal*, 21 February 2024, accessed 15 March 2024; ACCC, Digital Platform Services Inquiry – Interim Report No. 7 – Expanding ecosystems of digital platforms, 27 November 2023, p 3.

32 For example, as noted in section 2.1 of this Report, technological advances have increased the scale of consumer data collection that can occur and the value it can bring, across a wide range of categories.

33 OAIC, Data breaches seen as number one privacy concern, survey shows, 8 August 2023, accessed 15 March 2024.

34 OAIC, Australian Community Attitudes to Privacy Survey – August 2023, 8 August 2023, pp 27–28.

35 OAIC, Australian Community Attitudes to Privacy Survey – August 2023, 8 August 2023, p 17.

36 Note, however, that for a number of reasons, this high-level awareness of privacy risks often does not translate to consumers understanding how their data is being used, as discussed in section 5.1 of this Report.

37 Apple, Upcoming AppTrackingTransparency requirements, 20 April 2021, accessed 15 March 2024.

38 J Loveless, How Does Apple's App Tracking Transparency Framework Affect Advertisers?, *Forbes,* 22 August 2022, accessed 15 March 2024; Apple, Data Privacy Day at Apple: Improving transparency and empowering users, 27 January 2021, accessed 15 March 2024.

39 These tools include SKAdNetwork, which can tell a developer how many times its app was installed after an ad was seen. Another tool, Private Click Measurement, can tell the developer how many times users clicked on an ad for a product within an app. See C Gartenberg, Why Apple's new privacy feature is such a big deal, *The Verge*, 28 April 2021, accessed 15 March 2024.

40 P McGee, Apple reaches quiet truce over iPhone privacy changes, *Ars Technica,* 9 December 2021, accessed 15 March 2024.

– Google has announced it will introduce its Privacy Sandbox in 2024, which will lead to third-party cookies being phased out.[41]

These changes from digital platforms, and the resulting decline of more traditional online identifiers, have prompted many businesses which collect consumer data to review and improve their existing data governance and compliance processes. In addition, given these developments, many businesses are likely seeking alternative ways to track consumers' online activity, such as for the purposes of targeted advertising. For example, data firm LiveRamp offers a product called Authenticated Traffic Solution (ATS), which uses pseudonymous[42] identifiers known as RampIDs instead of third-party cookies or device IDs.[43] LiveRamp submits that adoption of this product has scaled quickly with publishers that want to get ahead of the deprecation of third-party cookies.[44]

Collectively, the above developments have led many data firms to pivot to non-traditional kinds of data products and services, particularly those which do not rely on personal information or traditional online identifiers such as IP addresses and third-party cookies. Examples of these non-traditional data products and services include:

- data clean rooms (discussed in box 3.2 of this Report), where firms can collaborate with each other on marketing campaigns or enrich their own data with insights from other businesses' data
- data analysis and consulting services, which may occur within a business customer's own data environment[45]
- pseudonymous identifiers, which may represent an alternative way for business customers to measure consumers' online activity in a 'post-cookie' world.

This is exemplified by a number of data firms which queried their categorisation as data brokers and inclusion in the Report, or sought to distinguish themselves from traditional data broking practices.[46] These firms are further discussed in box 1.1.

Box 1.1 Evolution of the services of sample firms

The evolving and diversifying nature of the data ecosystem in Australia is exemplified by the evolving business activities of several of the firms discussed in the Issues Paper. These firms do not categorise themselves as data brokers. For example:

- **LiveRamp:** in 2014, LiveRamp was acquired by Acxiom, a 'marketing and audience solutions' business,[47] which has been described as one of the largest brokers with data on billions of people worldwide.[48] However, Acxiom sold its original marketing business in 2018.[49] More recently, in 2021, LiveRamp Australia made the decision to

41 F Lardinois, Google will disable third-party cookies for 1% of Chrome users in Q1 2024, *TechCrunch*, 18 May 2023, accessed 15 March 2024; Google, The Privacy Sandbox, accessed 15 March 2024. For a detailed discussion of Privacy Sandbox, including potential implications for competition in ad tech, see ACCC, Digital Advertising Services Inquiry – Final Report, 28 September 2021, pp 126–131.

42 Pseudonymisation is explained and discussed in more detail in box 1.2.

43 LiveRamp, Submission to the Report, 28 September 2023, p 5.

44 LiveRamp, Submission to the Report, 28 September 2023, p 5.

45 For example, Quantium submits that for many of its bespoke consulting services, customers will require Quantium to perform its data analysis in their own systems and environment, such that Quantium does not receive the data in its own systems. See Quantium, Submission to the Report, 28 September 2023, p 2.

46 Quantium, Submission to the Report, 28 September 2023, pp 1–2; LiveRamp, Submission to the Report, 28 September 2023, p 3; Nielsen, Submission to the Report, 28 September 2023, p 1; PropTrack, Submission to the Report, 28 September 2023, p 1.

47 LiveRamp, Submission to the Report, 28 September 2023, p 3.

48 LiveRamp, Submission to the Report, 28 September 2023, p 3; J Sherman, Data Brokers Know Where You Are—and Want to Sell That Intel, *Wired*, 23 August 2021, accessed 15 March 2024.

49 LiveRamp, Submission to the Report, 28 September 2023, p 3.

discontinue its third-party[50] data marketplace and remove Australian-based buyers from it.[51] LiveRamp Australia now describes itself as a data collaboration platform.[52] It says it provides technology and tools to enable business customers to use their own first-party data[53] for marketing purposes.[54] Specific marketing use cases include:

  - data activation and suppression, which lets business clients activate segments of consumers within their first-party data for targeted advertising, or avoid sending advertising to current customers and consumers who have asked not to be marketed to
  - closed loop measurement, which allows business customers to analyse their own data and better understand the impact of their marketing campaigns
  - data collaboration, whereby business customers can exchange data insights from their respective datasets by agreement with each other.[55] Unlike more traditional methods of data sharing, LiveRamp submits this approach to data collaboration does not involve the sale of any 'raw' personal information, though it still allows business customers to share data for purposes such as activation and suppression or lookalike modelling to identify potential new customers.[56]

- **Quantium:** Quantium supplies a range of data-driven marketing and advertising products and services. Starting in 2015, 3 data firms – Acxiom, Experian and Quantium – participated as third-party data providers in Facebook's (now Meta) Partner Categories program in Australia.[57] Until Facebook discontinued the program in 2018,[58] these firms packaged ad targeting options for marketers to reach Facebook users based on their activity outside Facebook.[59] The data on this off-platform activity was supplied by the 3 data firms and paired with Facebook user data using a data-matching process.[60] In Quantium's case, it reportedly used de-identified data to categorise consumers into segments such as 'outdoor enthusiasts' and 'travellers'.[61] The ACCC has previously observed that in 2016, Quantium held datasets from National Australia Bank, Foxtel, Woolworths Rewards and News Corp.[62]

  Separately, in a 2018 YouTube video, Quantium claimed to offer an 'unrivalled picture of the behaviours of more than 80% of Australian households, spanning banking, household and retail transactions' through products such as Q.Segments and Q.Profile.[63]

---

50 Third-party data is an industry term generally referring to data obtained from a source other than the consumer or the original collector of the data. A business may purchase such data from a data firm to supplement the 'first-party' data it has already collected directly from its own customers.

51 LiveRamp, Submission to the Report, 28 September 2023, p 4.

52 LiveRamp, Submission to the Report, 28 September 2023, p 3.

53 First-party data is an industry term which generally refers to information collected by a business directly from its own customers. Examples include a consumer's contact information and purchase history, or details of their interactions with the business' website and mobile app.

54 LiveRamp, Submission to the Report, 28 September 2023, p 3.

55 LiveRamp, Submission to the Report, 28 September 2023, p 3.

56 LiveRamp, Submission to the Report, 28 September 2023, pp 3–4.

57 Meta, Partner Categories launching in Australia, 20 July 2015, accessed 15 March 2024.

58 Meta, Shutting Down Partner Categories, 28 March 2018, accessed 15 March 2024.

59 Meta, Partner Categories launching in Australia, 20 July 2015, accessed 15 March 2024.

60 Meta, Partner Categories launching in Australia, 20 July 2015, accessed 15 March 2024.

61 A Bogle, I asked everyone from Facebook to data brokers to Stan for my information. It got messy, *ABC News*, 28 April 2018, accessed 15 March 2024.

62 ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019, p 72.

63 Quantium, Our media solutions can help solve a number of business challenges, YouTube, 22 October 2018, accessed 15 March 2024. Segmentation and profiling products are discussed further in chapter 3 of this Report.

However, in its submission to this Report, Quantium says it does not operate as a data broker, because it does not share or sell personal information or any other information on persons to third parties.[64] Instead, Quantium characterises itself as a data analytics firm which provides insights based on its clients' own data as consulting services and/or products.[65]

- **PropTrack**: PropTrack submits that it supplies valuation tools and data insights related to residential property, and that it is distinct from the ACCC's definition of a data broker because its business is not focussed on personal information.[66] PropTrack says the limited personal information it collects is peripheral to its core activities and generally used (if at all) in a manner that does not involve disclosure to third parties of information relating to an identified or identifiable person.[67]
- **Nielsen:** Nielsen's submission focusses on its role as a provider of independent audience measurement and data analytics services.[68] Such services include:
  - Television Audience Measurement – measuring the audiences of broadcast television and streaming services, including through metrics such as reach, frequency of viewing and duration of viewing
  - Digital Content Ratings – similar to Television Audience Measurement, but for media content viewed on computers and mobile devices, and
  - Digital Ad Ratings – measuring the audiences exposed to advertising campaigns on computers and mobile devices, including impressions (views), reach and frequency.[69]

  Nielsen submits that audience measurement is its primary business, and that this business model is distinct from traditional data brokers and firms that collect and process data for targeted advertising and personalised marketing.[70] The ACCC understands that unlike some other data products and services discussed in this Report, Nielsen collects much of its audience measurement data with the knowledge of consumers who agree to participate in 'panels'.[71]

  We note that Nielsen's website also lists a range of other Nielsen services, including Nielsen Marketing Cloud which is shown as having 'full coverage' in Australia[72] and has been registered as a data broker service in California.[73]

We note that, separately, Nielsen sold its information services business, NielsenIQ, in 2021.[74] NielsenIQ submits that it has extensive expertise and experience in data brokerage, including in Australia, but that it is no longer affiliated with Nielsen or any of its subsidiaries.[75]

64 Quantium, Submission to the Report, 28 September 2023, p 1.
65 Quantium, Submission to the Report, 28 September 2023, p 1.
66 PropTrack, Submission to the Report, 28 September 2023, p 1.
67 PropTrack, Submission to the Report, 28 September 2023, p 1.
68 Nielsen, Submission to the Report, 28 September 2023, p 1.
69 Nielsen, Submission to the Report, 28 September 2023, p 1.
70 Nielsen, Submission to the Report, 28 September 2023, pp 1–3.
71 For example, in order to become a panel member for Nielsen's Television Audience Measurement service, a consumer must agree to have a box installed in their household to capture their TV viewing habits. See Nielsen Television Audience Measurement, Who is Nielsen Television Audience Measurement?, accessed 15 March 2024.
72 Nielsen, Marketing Cloud, accessed 15 March 2024.
73 State of California Department of Justice – Office of the Attorney General, Data Broker Registration for Nielsen Marketing Cloud, 11 August 2020, accessed 15 March 2024. Note that Nielsen Marketing Cloud's registration for 2023 is listed as incomplete.
74 Nielsen, Nielsen Announces Completion of Sale Of Global Connect Business to Advent International, 5 March 2021, accessed 15 March 2024.
75 NielsenIQ, Submission to the Report, 28 September 2023, p 2.

As noted above, many data firms have moved to data products and services that do not rely on the use of personal information. Rather, they use data that has been de-identified. In Australia, de-identification is a concept defined in the *Privacy Act 1988* (Cth) (Privacy Act) and discussed further in box 1.2. We note that in some cases, de-identified data may still be able to be re-identified and linked back to particular individuals, as discussed in section 5.2.1.

Box 1.2 Data de-identification

Under the Privacy Act, personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.[76] Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context (or data access environment).[77]

Information that has undergone a robust de-identification process is no longer considered personal information and is therefore not subject to the Privacy Act. However, the OAIC notes that de-identification is not a fixed or end state, and previously de-identified data may again become personal information if this context changes, or as technology advances.[78]

The de-identification process generally involves two steps:

- the removal of direct identifiers, such as an individual's name, address or other identifying information
- removing or altering other information that may allow an individual to be identified, and/or putting controls and safeguards in place in the data access environment to appropriately manage the risk of re-identification.[79]

The government has agreed in-principle to a proposal in the Privacy Act Review Report to amend the definition of 'de-identified' in the Privacy Act to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context (proposal 4.5).[80] The Privacy Act Review Report is discussed further in section 1.5.2.

Other ways data firms state that they de-identify data

The ACCC has observed other ways in which data firms may claim to 'de-identify' data. We understand that some of the techniques that are applied in practice by data firms include the following:

---

76 *Privacy Act 1988* (Cth), s 6(1), definition of 'de-identified'. Personal information refers to information about an identified individual, or an individual who is reasonably identifiable. See *Privacy Act 1988* (Cth), s 6(1), definition of 'personal information'.

77 OAIC, De-identification and the Privacy Act, 21 March 2018, accessed 15 March 2024; OAIC and CSIRO Data61, The De-identification Decision-Making Framework, 18 September 2017, accessed 15 March 2024, p 1.

78 Change in context refers to the particular circumstances surrounding the release of any de-identified information. For example, the OAIC notes consideration should be given to the nature and amount of information being released, who will hold and have access to the information, the other information that is available to the person or people who will have access to the information and the practicability of using that information to identify an individual. See OAIC, De-identification and the Privacy Act, 21 March 2018, accessed 15 March 2024.

79 OAIC, De-identification and the Privacy Act, 21 March 2018, accessed 15 March 2024. We note that the types of information that may be used to re-identify an individual will depend on context but could include, for example, public transport usage data being combined with publicly available information about people's travel patterns, as discussed further in box 5.5.

80 Attorney-General's Department, Government response to the Privacy Act Review Report, 28 September 2023, p 15; Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 37 (Proposal 4.5).

- **Data anonymisation:** Some overseas data protection laws use the terminology of 'anonymisation'. For example, under the EU's General Data Protection Regulation (GDPR), anonymisation is defined as the process of rendering personal data anonymous. Once data is truly anonymous and individuals are no longer identifiable, the data no longer falls within scope of the GDPR.[81]
- **Data pseudonymisation:** Pseudonymisation involves replacing any direct identifiers, such as a person's name or email address, with a pseudonym (such as a reference number or hashed code) which does not directly identify the person.[82] In other words, pseudonymisation can reduce the risk of an individual being identified in a dataset by replacing their individual identifiers with artificial ones.

  This process has the potential to mitigate against the loss of an individual's data in the event of a data breach. However, the OAIC notes that pseudonymisation alone does not necessarily de-identify personal information for the purposes of the Privacy Act.[83] For example, an entity may have access to additional information that enables it to identify an individual.[84] In some cases, this means additional data protection techniques or controls may be required if an entity wishes to de-identify information in a particular context.
- In addition, the use of pseudonyms does not necessarily prevent consumers from being individually targeted. For example, Salinger Privacy submits that pseudonyms can be used to draw links between unrelated datasets. It argues that if companies 'enrich' their pseudonymised consumer data at the addressable individual level by exchanging insights in a data clean room, the outputs from this process may still be personal information (which implies these outputs could be used to target individuals), even if no company can see another's 'raw' customer data.[85]

  Data aggregation: Data aggregation refers to the process by which raw data is gathered, reformatted and presented in summary form for subsequent data sharing and analysis.[86] Broadly speaking, the ACCC acknowledges that many of the risks to consumers associated with re-identification can be minimised where the data has been aggerated to a point that re-identification is very difficult or impossible.
- However, for data aggregation to be effective, we note the need for a number of statistical controls, such as a minimum number of data subjects, in order to avoid the risk that individuals may still be identified within the data.[87] Data firms and other entities may use some of these controls and techniques in sectors where sensitive data about individuals from multiple sources is joined in a controlled environment for data analytics, such as data-driven medical research.[88]

It is worth noting that unless the meanings of these terms are clearly explained, consumers' ability to understand their meaning is likely to be limited. For example, in a

81 OAIC, Privacy Act Review Issues Paper Submission – Part 2: Definition of personal information, 11 December 2020, accessed 15 March 2024; *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Recital 26.

82 Data Protection Commission (Ireland), Guidance note: guidance on anonymisation and pseudonymisation, June 2019, p 3.

83 OAIC, Chapter 2: APP 2 Anonymity and pseudonymity, 22 July 2019, paragraph 2.7, accessed 15 March 2024.

84 OAIC, Chapter 2: APP 2 Anonymity and pseudonymity, 22 July 2019, accessed 15 March 2024.

85 Salinger Privacy, Submission to the Report, 28 September 2023, pp 9–11.

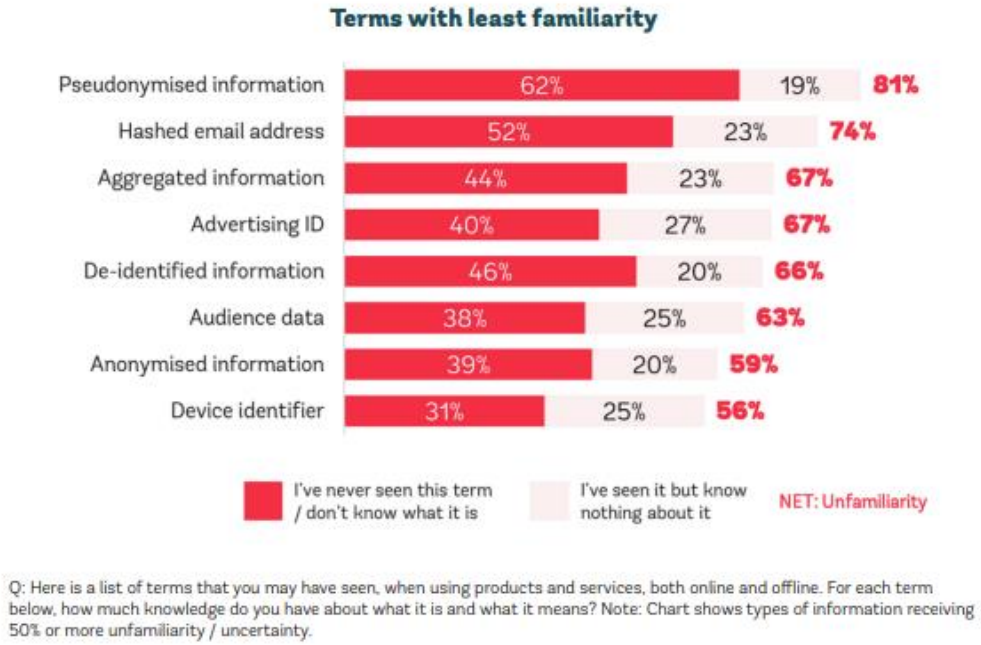
86 T Wem, Data Aggregation, *Encyclopedia of Big Data*, 31 March 2020, accessed 15 March 2024.

87 This is referred to as the 'threshold' or 'frequency' rule, which sets the minimum number of data points, below which may be considered to pose an unacceptable risk of disclosure. Other rules to help ensure data is effectively aggregated include the 'cell dominance rule' and the 'P% rule'. See Australian Bureau of Statistics, Treating aggregate data, 8 November 2021, accessed 15 March 2024.

88 See, for example, Department of Health, Framework to guide the secondary use of My Health Record system data, May 2018.

recent survey by the Consumer Policy Research Centre (CPRC), 2 in 3 Australian consumers (66%) said they had either never seen the term 'de-identified information' or knew nothing about it.[89] Most consumers were also unfamiliar with the terms 'anonymised information' (59%), 'aggregated information' (67%) and 'pseudonymised information' (81%)[90], as shown in figure 1.4.

Figure 1.4: Data-related terms that consumers are least familiar with[91]



1.4. Understanding data and the digital economy

The ACCC's previous work on digital platforms has shown the collection of user data is central to the business models of advertiser-funded platforms. The range of ways in which data is generated, collected and used is discussed in chapter 2. This section discusses the ACCC's previous work on the consumer and competition implications of data, which are also discussed in chapters 5 and 6 respectively.

1.4.1. The significance of consumer data for competition

The original Digital Platforms Inquiry observed that incumbent digital platforms, particularly Google and Facebook (now Meta), held a strong competitive advantage due to the breadth

89 K Kemp, C Gupta and M Campbell, Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them, CPRC and UNSW Sydney, February 2024, p 13.

90 K Kemp, C Gupta and M Campbell, Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them, CPRC and UNSW Sydney, February 2024, p 13. The issue of consumer awareness (or lack thereof) of how data may be used is discussed further in section 5.1 of this Report.

91 K Kemp, C Gupta and M Campbell, Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them, CPRC and UNSW Sydney, February 2024, p 13.

and depth of user data they collect, which also creates barriers to rivals entering and expanding in relevant markets.[92]

The report noted that platforms often have significant discretion in how the data they collect on consumers is used and disclosed to other entities.[93] In addition, the report noted that Google and Facebook's extensive tracking of consumers and collection of their data helped them improve their services to attract more users and advertisers, creating a 'virtuous feedback loop' for those companies.[94]

The Ad Tech Report highlighted the importance of data in digital advertising markets in concluding that Google's dominance across much of the ad tech supply chain is due in part to its data advantage – specifically its broad range of first-party data gathered from its consumer-facing services and third-party data from third-party sites and apps.[95] The Report on General Online Retail Marketplaces also found third-party sellers often did not have access to the same breadth and depth of data collected by an online marketplace, which can hinder sellers in their ability to test and improve their product range and strategies.[96]

Given the importance of consumer data to competition, the Regulatory Reform Report raised the possibility that data portability or access measures could be included in future codes of conduct for digital platforms. However, the report also noted that:

- it is important to holistically consider interrelated privacy, competition and consumer protection issues for any measures[97]
- current privacy laws are insufficient for some data access mechanisms to be implemented without considerable consumer detriment, and
- any measures that propose to increase third-party access to data without appropriate safeguards in place risk harming consumers through reduced privacy and data security, and increase the risk of consumer harm through discrimination, exclusion and profiling.[98]

More broadly, and in recognition of the competitive advantages that access to data can bring, it is worth noting that some data portability schemes already exist in Australia, as discussed in section 2.4.1.

1.4.2. Potential consumer benefits and risks of consumer data collection and sharing

The original Digital Platforms Inquiry noted that data-based innovations can bring benefits for businesses and consumers. Such benefits may include digital platforms providing businesses with a cheaper and more targeted way of reaching consumers online, and providing consumers with access to services at zero monetary cost in exchange for their attention and the collection of their data.[99] It also noted the OECD's statement that 'more extensive and innovative uses of personal data are bringing increasing economic and social benefits' for both groups.[100]

92 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 11.
93 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, pp 2–3.
94 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 11.
95 ACCC, Digital Advertising Services Inquiry – Final Report, 28 September 2021, p 67.
96 ACCC, Digital Platform Services Inquiry – Interim Report No. 4 – General online retail marketplaces, 28 April 2022, p 10.
97 The intersection between competition and privacy issues, as relevant to the data products and services of data firms, is discussed further in chapter 6 of this Report.
98 ACCC, Digital Platform Services Inquiry – Interim Report No. 5 – Regulatory reform, 11 November 2022, p 173.
99 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 61.
100 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 442.

However, the report noted that realising these benefits relies on maintaining consumer trust in data-driven technologies to enable the free flow of information. It suggested that trust may be undermined if consumers do not understand or cannot control an organisation's use of their personal information.[101]

As well as decreased trust, the original Digital Platforms Inquiry noted that if Australian consumers lack control over their personal information, this could lead to:

- decreased consumer welfare from a lack of privacy or a lack of competition
- risks from increased profiling, discrimination and exclusion
- particular risks for vulnerable consumers such as children and people with a low socio-economic background.[102]

The report also observed that the potential for these data-related harms was not confined to customers of digital platforms, given a growing number of businesses across the economy are collecting and monetising data on Australian consumers.[103] Such businesses include financial institutions, telecommunications companies, major retailers and airlines. The report noted that data brokers also play a central role in exchanging and combining personal information and data across a wide variety of sectors in Australia.[104]

The Report on General Online Retail Marketplaces stated that consumers can benefit from the use of their data for more targeted tailoring of the products displayed to them. However, extensive data collection practices can result in harm when consumers do not have adequate information and control about what data is being collected and how it is being used.[105]

In that report, the ACCC found that some marketplaces' data collection policies allowed them to collect data from third parties, such as data brokers, and combine it with the first-party data they collected from consumers.[106] The ACCC also noted a range of potential and real consumer harms that could arise from data collection. These included:

- reduced consumer welfare from decreased privacy, particularly if the targeted advertising activities of online marketplaces leads to unsolicited marketing, data breaches, online identity fraud or other scams
- risks to consumers from increased profiling, in circumstances where consumer profiles (discussed further in section 3.2.2 of this Report) may allow an online marketplace or third-party advertisers to influence the behaviour of particular groups or demographics
- risks to consumers from discrimination and exclusion, particularly if consumer profiles allow an online marketplace, ad tech provider, or third-party advertiser to segment and potentially discriminate against particular consumer groups.[107]

101 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, pp 442–443.
102 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, pp 444–448.
103 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 3.
104 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 449.
105 ACCC, Digital Platform Services Inquiry – Interim Report No. 4 – General online retail marketplaces, 28 April 2022, pp 4–5.
106 ACCC, Digital Platform Services Inquiry – Interim Report No. 4 – General online retail marketplaces, 28 April 2022, p 33.
107 ACCC, Digital Platform Services Inquiry – Interim Report No. 4 – General online retail marketplaces, 28 April 2022, p 35.

1.5. The Privacy Act and Privacy Act Review

1.5.1. The Privacy Act

The Privacy Act is the principal piece of Australian legislation protecting the handling of personal information about individuals, which includes the collection, use, storage and disclosure of personal information.[108] The Privacy Act defines personal information as 'information or an opinion about an identified or reasonably identifiable individual, regardless of whether the information or opinion is true or not, and whether it is recorded in a material form or not'.[109]

The Privacy Act currently applies to private sector organisations with an annual turnover of more than $3 million, Australian Government organisations and some other organisations.[110] Among other objectives, the Privacy Act seeks to balance protecting the privacy of individuals with the interests of organisations in carrying out their functions or activities.[111]

To the extent that they handle personal information, data firms and other entities which are covered by the Privacy Act are required to comply with it.

The Privacy Act includes the Australian Privacy Principles (APP). The OAIC, which is the government agency responsible for overseeing compliance with the Privacy Act, describes the APPs as the cornerstone of the privacy protection framework in the Privacy Act.[112]

Among other matters, the APPs contain standards, rights and obligations around the collection, use, storage and disclosure of personal information and the rights of individuals to access and correct their personal information.[113]

Some submissions to the Issues Paper for this Report cite the relevance of the existing Privacy Act provisions, including several of the APPs, to data products and services in Australia. For example:

- the OAIC's submission notes that the Privacy Act, including the APPs, apply to any entities which collect or disclose personal information from, or to, anyone else for a 'benefit, service or advantage'.[114] It states that whether information is 'personal information' under the Privacy Act should be assessed on a case-by-case basis and depending on context, and that even information which is not personal information on its own may become personal information when combined with other information that is held by or accessible to an organisation.[115] The OAIC's submission also highlights the potential relevance of APPs 1, 3, 5, 6, 10 and 11 to data firms that handle personal information.[116]
- Dr Katharine Kemp and Professor Graham Greenleaf submit that third-party data brokers have not explained how they are complying with APP 3.6.[117] APP 3.6 requires an APP

[108] Attorney-General's Department, Privacy, accessed 15 March 2024.
[109] *Privacy Act 1988* (Cth), s 6.
[110] OAIC, The Privacy Act, accessed 15 March 2024.
[111] *Privacy Act 1988* (Cth), s 2A.
[112] OAIC, Australian Privacy Principles, accessed 15 March 2024.
[113] OAIC, Australian Privacy Principles, accessed 15 March 2024.
[114] OAIC, Submission to the Report, 28 September 2023, p 5.
[115] OAIC, Submission to the Report, 28 September 2023, pp 5–6.
[116] OAIC, Submission to the Report, 28 September 2023, pp 7–12.
[117] UNSW Allens Hub (K Kemp and G Greenleaf), Submission to the Report, p 6; *Privacy Act 1988* (Cth), Schedule 1, Part 2 (APP 3.6).

entity[118] to collect personal information directly from an individual unless an exception applies.[119] APP 3.6 is discussed further in Box 1.3 below. Dr Kemp and Professor Greenleaf state that they have also not seen any explanation of how businesses which obtain personal information on their own customers from data firms (rather than directly from the individuals concerned) are complying with this law.[120]

- Likewise, Salinger Privacy submits that the market for data firms' customer enrichment products and services is built on non-compliance with APP 3.6, and that the sharing of first-party data with third-party data firms 'may involve widespread non-compliance with APP 6'.[121] APP 6 provides that an entity can only use or disclose an individual's personal information for the purpose it was collected for, unless the individual has consented to a secondary purpose or an exception applies.[122]
- Conversely, IAB Australia's submission states that some data brokers' services can help protect data privacy, such as data verification services which help organisations comply with APP 10.[123] APP 10 requires entities to take reasonable steps to ensure the personal information they collect, use and disclose is accurate, up-to-date and complete.[124]

Box 1.3 APP 3.6 – Personal information to be collected directly from the individual

APP 3.6 requires an APP entity to collect personal information about an individual only from the individual, unless an exception applies.[125]

Exceptions to the direct collection rule

Under APP 3.6, an entity must collect personal information about an individual directly from that individual, unless one of the following exceptions applies:

- the entity is an agency,[126] and the individual consents to the collection of the information from someone other than the individual
- the entity is an agency, and is required or authorised by or under an Australian law, or a court or tribunal order, to collect the information from someone other than the individual, or
- it is unreasonable or impractical to collect the information from the individual.[127]

The OAIC notes that whether it is 'unreasonable or impractical' to collect personal information directly from an individual will depend on the circumstances, including:

- whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
- the sensitivity of the personal information being collected
- whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected

118 The Privacy Act defines an 'APP entity' as an agency or organisation (terms which are also defined under the Privacy Act). The term is often used collectively to refer to any entity covered by the Privacy Act. See *Privacy Act 1988* (Cth), s 6; OAIC, Australian Privacy Principles guidelines, 22 July 2019, accessed 15 March 2024.
119 OAIC, Australian Privacy Principle 3 — collection of solicited personal information, accessed 15 March 2024.
120 UNSW Allens Hub (K Kemp and G Greenleaf), Submission to the Report, 28 September 2023, p 6.
121 Salinger Privacy, Submission to the Report, 28 September 2023, p 3; *Privacy Act 1988* (Cth), Schedule 1, Part 3 (APP 6).
122 OAIC, Australian Privacy Principle 6 – use or disclosure of personal information, accessed 15 March 2024.
123 IAB Australia, Submission to the Report, 28 September 2023, pp 8-10; *Privacy Act 1988* (Cth), Schedule 1, Part 4 (APP 10).
124 OAIC, Australian Privacy Principle 10 – quality of personal information, accessed 15 March 2024.
125 *Privacy Act 1988* (Cth), Schedule 1, Part 2 (APP 3.6).
126 'Agency' is defined in the Privacy Act and includes federal courts as well as most Australian Government agencies, departments and Ministers. See *Privacy Act 1988* (Cth), s 6(1).
127 *Privacy Act 1988* (Cth), Schedule 1, Part 2 (APP 3.6).

- any privacy risk if the information is collected from another source
- the time and cost involved in collecting directly from the individual.[128]

The OAIC notes, however, that an APP entity is not excused from collecting information from the individual by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impractical will depend on whether the burden is excessive in all the circumstances.[129]

Application to data firms

The OAIC notes that to the extent third-party data brokers collect personal information, they must comply with the requirements of APP 3 and other privacy obligations, and that these obligations apply to the collection of personal information from publicly available sources, such as web pages.[130]

The OAIC states that 'collection' includes the 'generation' or 'creation' of personal information, such as inferences in relation to an individual's characteristics, behaviours or preferences. The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source, and by any means.[131]

The OAIC acknowledges that there is underlying tension between the data minimisation requirements of APP 3 and the activities of data brokers, whose business model is reliant on maximising the amount of data that they collect in order to find correlations between disparate datasets.[132] The OAIC's guidance on data analytics observes that the collection of 'all data' that is available for 'unknown purposes' may expose entities to privacy compliance risks.[133]

As noted in section 1.3.1, the ACCC has observed significant changes in the ways that consumer data is collected and used, and data firms often use de-identified data in their products and services, which is not necessarily subject to Australia's Privacy Act (as discussed further in box 1.2). We acknowledge that APP 3.6 applies to personal information, and it could be the case that some of the consumer data collected and used by data firms in Australia falls beyond its scope. As discussed in chapter 5, there are still harms that can arise in relation to these broader categories of consumer data.

As also discussed in chapter 5, there appears to be a disconnect between what consumers expect the Privacy Act to cover and the exclusion of some categories of de-identified data from its remit.[134] To address some of these concerns, the ACCC supports Proposal 4.1 in the Privacy Act Review Report (discussed further at section 1.5.2).[135] This proposal would amend the definition of 'personal information' in the Privacy Act from information 'about' an individual, to refer to information that 'relates to' an individual.[136]

128 OAIC, Submission to the Report, 28 September 2023, p 9.
129 OAIC, Submission to the Report, 28 September 2023, p 9.
130 OAIC, Submission to the Report, 28 September 2023, p 8.
131 OAIC, Submission to the Report, 28 September 2023, p 9.
132 OAIC, Submission to the Report, 28 September 2023, p 8.
133 OAIC, Submission to the Report, 28 September 2023, p 9; OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 15 March 2024.
134 See, for example, CPRC, Not a fair trade: Consumer views on how businesses use their data, March 2023, pp 7–8.
135 The ACCC's submission to the Privacy Act Review Report also indicated support for this proposal – see ACCC, Privacy Act Review Report – ACCC submission, 31 March 2023, p 3.
136 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, pp 5, 24–27. In the original Digital Platforms Inquiry, the ACCC recommended that the definition of 'personal information' be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual – see ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 34.

1.5.2. The Privacy Act Review and other Australian Government consideration

In the original Digital Platforms Inquiry, the ACCC recommended that the government should:

- strengthen protections in the Privacy Act (Recommendation 16)
- carry out broader reform of Australian privacy law (Recommendation 17)
- ask the OAIC to develop an enforceable privacy code of practice for digital platforms in consultation with industry stakeholders (Recommendation 18)
- introduce a statutory tort for serious invasions of privacy (Recommendation 19).[137]

On 12 December 2019, the Attorney-General announced that the government would conduct a review of the Privacy Act to ensure privacy settings empower consumers, protect their data and best serve the Australian economy.[138] After an extensive review led by the Attorney-General's Department, the Privacy Act Review Report was published on 16 February 2023.[139] Following submissions from a wide array of stakeholders, including the ACCC,[140] the government released its response on 28 September 2023.[141]

A number of key proposals supported by government[142] would have implications for some data products and services supplied in Australia. For example, such proposals may include:

- Proposals 4.1 to 4.5, to clarify or amend the definitions of key terms in the Privacy Act such as 'personal information', 'collection' and 'de-identified'. This includes in-principle agreement with:
  - Proposal 4.1, to change the word 'about' in the definition of personal information to 'relates to', in order to clarify that personal information is an expansive concept that can include technical and inferred information such as IP addresses and device identifiers[143]
  - Proposal 4.2, to include a non-exhaustive list in the Privacy Act of information that may be personal information.[144] The Privacy Act Review Report proposed that this list should include identification numbers, online identifiers or pseudonyms.[145]
- Proposal 4.10, to require consumer consent for the collection of precise geolocation tracking data[146]
- Proposals 12.1 to 12.3, to create a 'fair and reasonable test' for personal information collection, use and disclosure, regardless of whether consent has been obtained (discussed further in chapter 5)[147]
- Proposal 13.4, to require that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3[148]

137 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, pp 34–37.
138 Australian Government, Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 12 December 2019, p 18.
139 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, accessed 15 March 2024.
140 ACCC, Privacy Act Review Report – ACCC submission, 31 March 2023.
141 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023.
142 Either through agreement or in-principle agreement.
143 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 5, 21.
144 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 5, 21.
145 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, pp 28–29.
146 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 15, 22.
147 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 8, 27.
148 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 10, 28.

- Various protections for children, including a Children's Online Privacy Code (Proposal 16.5), a prohibition on trading in the personal information of children (Proposal 20.7), and prohibitions on direct marketing and targeting to a child, unless it is in the child's best interests (Proposals 20.5 and 20.6)[149]
- Proposals 18.1 to 18.6, to introduce or expand on various 'rights of the individual' such as rights to access, erasure and correction of personal information[150]
- Proposals 20.1, 20.2 and 20.4, to define 'direct marketing', 'targeting' and 'trading', give consumers an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes, and require a consumer's consent to trade their personal information[151]
- Proposal 23.6, to introduce a definition of 'disclosure' of personal information.[152]

The potential implications of some of these proposals for data firms are discussed in chapter 5. In addition, a number of submissions to this Report expressed support for specific recommendations of the Privacy Act Review Report, as outlined in box 1.4.

Box 1.4 Submissions commenting on the Privacy Act Review Report

Several submissions to this Report express support for recommendations in the Privacy Act Review Report. For example:

- The Australian Communications Consumer Action Network's (ACCAN) submission identifies a series of recommendations which it states would 'address harms from third-party data brokers', namely the proposals to:
  - clarify de-identification
  - criminalise malicious re-identification of de-identified information
  - introduce measures around fair and reasonable information handling
  - require an individual's consent to trade in their personal information
  - prohibit trading in children's personal information
  - protect personal information shared overseas.[153]
- In its submission, the Australian Retailers Association stresses the importance of the proposed reforms relating to collection, processing and use of personal data, which it says are fundamental issues for data brokerage in the retail sector.[154]
- CHOICE recommends that the government implement the recommendations of the Privacy Act Review and increase funding to the OAIC.[155]

The OAIC's submission highlights some Privacy Review Report proposals that, in its view, would improve privacy protections and individuals' control in relation to the handling of personal information across the economy, including in relation to data products and services.[156]

149 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 13, 30, 33.
150 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 18, 30–31.
151 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 12, 32–33.
152 Attorney-General's Department, Government Response – Privacy Act Review Report, 28 September 2023, pp 15, 35.
153 ACCAN, Submission to the Report, 28 September 2023, p 2.
154 Australian Retailers Association, Submission to the Report, 28 September 2023, p 1.
155 CHOICE, Submission to the Report, 28 September 2023, p 4.
156 OAIC, Submission to the Report, 28 September 2023, pp 13–15.

Aside from the Privacy Act Review and this Report, the ACCC understands that regulatory scrutiny of the activities of data brokers or data firms in Australia has previously been limited, compared to some other jurisdictions. One emerging area is in cyber security. In November 2023 the government released its 2023–2030 Australian Cyber Security Strategy. As part of this strategy, the government states that it will review the data brokerage ecosystem, to assess whether further action is required to address risks associated with the transfer of data to malicious actors via data markets.[157] The government notes that this review will complement the proposed reforms to the Privacy Act.[158]

1.6. International context

In the past decade, regulators and policymakers in a number of jurisdictions have shown increased interest in data firms, with several inquiries, enforcement cases and new legislation. Some examples of these are listed below. The ACCC notes that there are varying definitions used across different jurisdictions in relation to data products and services and suppliers of these products and services.

1.6.1. United States

Federal Trade Commission (FTC)

The FTC's 2012 report on consumer privacy concluded that companies which collect and use consumers' data should take steps to better promote consumer privacy, increase transparency and simplify consumer choice.[159] The report also called on Congress to consider enacting baseline privacy legislation, as well as data security and data broker legislation, and urged industry to accelerate the pace of self-regulation.[160]

Subsequently, in May 2014, the FTC published a report which focussed more specifically on data brokers.[161] This report found that data brokers' datasets are comprehensive, covering most consumers, and are enriched with various pieces of data, including sensitive inferred data.[162] It also observed that data brokers obtain much of their data from other data brokers, rather than directly from an original source, and that consumers are largely unaware that data brokers are collecting and using this information.[163]

In 2022, the FTC brought an action against data broker Kochava Inc. The FTC alleged Kochava had collected US consumers' geolocation data and marketed it to clients who could then use it to track consumers' movements to and from 'sensitive locations'. These included psychiatrists' offices, reproductive health clinics and particular houses of worship.[164] While a judge dismissed the FTC's case in May 2023, he allowed the regulator to revise its case.[165]

157 Australian Government, 2023–2030 Australian Cyber Security Strategy, 22 November 2023, p 32.
158 Australian Government, 2023–2030 Australian Cyber Security Strategy, 22 November 2023, p 32.
159 FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, March 2012, pp vii–viii.
160 FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, March 2012, p viii.
161 FTC, Data Brokers: A Call for Transparency and Accountability, May 2014.
162 FTC, Data Brokers: A Call for Transparency and Accountability, May 2014, p iv.
163 FTC, Data Brokers: A Call for Transparency and Accountability, May 2014, p iv.
164 FTC, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations, August 29 2022, accessed 15 March 2024.
165 Reuters, Judge tosses FTC lawsuit accusing broker of unfair geolocation data sales, 6 May 2023, accessed 15 March 2024.

At the time of writing, the case has yet to proceed to trial after the FTC refiled its complaint.[166]

Finally, in January 2024, the FTC announced it had reached its first settlement with a data broker concerning the sale of sensitive location information.[167] Under the terms of the settlement, data broker X-Mode Social and its successor company Outlogic will be prohibited from sharing or selling sensitive location data.[168] This followed FTC allegations that X-Mode/Outlogic had violated consumers' privacy and exposed them to potential discrimination, physical violence, emotional distress and other harms by selling precise location data that could be used to track their visits to sensitive locations. These included medical and reproductive health clinics, places of religious worship and domestic abuse shelters.[169]

We note that the FTC brought its actions against both Kochava and X-Mode/Outlogic under section 5(a) of the FTC Act, which prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[170] The ACCC has previously recommended a new economy-wide unfair trading practices prohibition under the Competition and Consumer Act in Australia.[171] As noted in chapter 5, we consider that such a prohibition could help address some of the consumer harms that may arise from harmful data practices in the digital economy.

Consumer Financial Protection Bureau (CFPB)

In March 2023, the CFPB issued a Request for Information on 'companies that track and collect information on people's personal lives'.[172] Alongside this inquiry, the CFPB proposed new rules in August 2023 to expand the Fair Credit Reporting Act to cover data brokers.[173] The CFPB's proposed new rules are designed to create more accountability across the industry and provide better recourse to American citizens to correct wrong information.[174]

US federal and state legislation

Several US states have introduced legislation to regulate the data broker industry. California, Vermont, Texas, Oregon and Delaware require data brokers that meet specified criteria to register with the state.[175] Similar legislation is also under consideration in New York and

166 FTC, FTC v. Kochava, Inc., 6 November 2023, accessed 15 March 2024. See also A Toomey McKenna, Data brokers know everything about you – what FTC case against ad tech giant Kochava reveals, *The Conversation*, 13 January 2024, accessed 15 March 2024.

167 FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data, 9 January 2024, accessed 15 March 2024.

168 FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data, 9 January 2024, accessed 15 March 2024.

169 FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data, 9 January 2024, accessed 15 March 2024.

170 FTC, Complaint – In the Matter of X-Mode Social, Inc., a corporation, and Outlogic, LLC, a limited liability company, 212-3038, p 9; FTC, Amended Complaint for permanent injunction and other relief – Federal Trade Commission v Kochava Inc, Case No. 2:22-cv-00377-BLW, 5 June 2023, p 33.

171 ACCC, Digital Platform Services Inquiry – Interim Report No. 5 – Regulatory reform, 11 November 2022, p 4.

172 CFPB, CFPB launches inquiry into the business practices of data brokers, 15 March 2023, accessed 15 March 2024.

173 This legislation governs the US credit reporting industry.

174 CFPB, Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices, 15 August 2023, accessed 15 March 2024.

175 California Civil Code, Title 1.81.48., Privacy: Data brokers [§ 1798.99.80 - 1798.99.88] (2019), accessed 15 March 2024; Vermont General Assembly, Title 9: Commerce and Trade – Chapter 62: Protection of Personal Information, accessed 15 March 2024; Texas Legislature, Texas Data Broker Law: Ch. 509, Data Brokers in Texas Business & Commerce Code (2023), accessed 15 March 2024; Oregon Legislative Assembly, Oregon House Bill 2052: Relating to the registration of business entities that quality as data brokers; and declaring an emergency (2023), accessed 15 March 2024; Delaware House of Representatives, House Bill No. 262 – An Act to amend Title 6 of the Delaware Code Relating to Data Brokers and Consumer Protection (2023), accessed 15 March 2024.

Washington state.[176] Colorado, Connecticut, Indiana, Iowa, Montana, New Jersey, Tennessee, Utah and Virginia have also passed consumer privacy legislation which may affect the data industry more broadly.[177]

The Vermont, Texas and Delaware laws also require registered data brokers to provide information to consumers on opt-out options, the treatment of minors' data, any purchaser credentialing processes (confirming the identity of the broker's clients) and details of past security breaches.[178]

California recently amended its legislation so that consumers will be able to make a single request for the deletion of their personal information held by registered data brokers.[179] This replaces the need to individually request deletion from over 500 registered data brokers.

Several federal Bills relating to data brokers have been introduced into the US Congress but have not passed. The 2 main bills have been the American Data Privacy and Protection Act (ADPA)[180] and the Data Elimination and Limiting Extensive Tracking and Exchange (DELETE Act).[181] The DELETE Act would set up a national registry run by the FTC. This would allow for a centralised opt-out system for people to stop third-party data brokers as defined in the Bill, from using their data.

1.6.2. United Kingdom

Following an investigation into data protection in the direct marketing data broking sector, the UK Information Commissioner's Office (ICO) published a 2020 report which found that Equifax, Experian and TransUnion were unlawfully 'trading, enriching and enhancing people's personal data without their knowledge'.[182] The ICO decided not to take any further action against Equifax or TransUnion. This was because it said they committed to complying voluntarily with UK data protection legislation, by withdrawing what the ICO described as non-compliant products and services.[183]

176 National Conference of State Legislatures, 2023 Consumer Data Privacy Legislation, last updated 28 September 2023, accessed 15 March 2024; Washington State Legislature, Washington House Bill HB1799: An Act Relating to the registration of business entities that qualify as data brokers, accessed 15 March 2024; New York State Senate, Senate Bill S365B – An act to amend the general business law, in relation to the management and oversight of personal data, accessed 15 March 2024.

177 Colorado General Assembly, SB-21-190 – Protect Personal Data Privacy (2021), accessed 15 March 2024; Connecticut General Assembly, Substitute for S.B. No. 6 – An Act Concerning personal data privacy and online monitoring (2022), accessed 15 March 2024; Indiana General Assembly, Senate Enrolled Act No. 5 – An Act to amend the Indiana Code concerning trade regulation (2023), accessed 15 March 2024; Iowa General Assembly, Senate File 262 – An Act Relating to Consumer Data Protection, Providing Civil Penalties, and Including Effective Date Provisions (2023), accessed 15 March 2024; Montana Legislature, Consumer Data Privacy Act (2023), accessed 15 March 2024; New Jersey Legislature, Senate Bill 332 (2024), accessed 15 March 2024; State of Tennessee, House Bill No. 1181 – The Tennessee Information Protection Act (2023), accessed 15 March 2024; Utah State Legislature, SB 227 – Consumer Privacy Act (2022), accessed 15 March 2024; Code of Virginia, Chapter 53 – Consumer Data Protection Act (2023), accessed 15 March 2024.

178 Vermont General Assembly, Title 9: Commerce and Trade – Chapter 62: Protection of Personal Information, §§ 2435, 2446, accessed 15 March 2024; Texas Legislature, Texas Data Broker Law: Ch. 509, Data Brokers in Texas Business & Commerce Code (2023), ss 509.004-509.005, accessed 15 March 2024; Delaware House of Representatives, House Bill No. 262 – An Act to amend Title 6 of the Delaware Code Relating to Data Brokers and Consumer Protection (2023), § 12D-103(3), accessed 15 March 2024.

179 California, Senate Bill No. 362, Chapter 709 (2023), accessed 15 March 2024, also known as the Delete Act.

180 US House of Representatives, Bill No. 8152 - American Data Privacy and Protection Act, 117th Congress, 2022, accessed 15 March 2024.

181 US Senate, Bill No. 3627 – DELETE Act, 117th Congress, 2022, accessed 15 March 2024.

182 ICO, ICO takes enforcement action against Experian after data broking investigation, 27 October 2020, accessed via Wayback Machine 15 March 2024.

183 ICO, Investigation into data protection compliance in the direct marketing data broking sector, October 2020, p 36. Data protection legislation in the UK includes the UK General Data Protection Regulation and Data Protection Act of 2018. See ICO, The UK GDPR, accessed 15 March 2024.

However, the ICO issued an enforcement notice to Experian, saying that while Experian had made progress, the ICO still had fundamental concerns with its processing of personal data.[184] The ICO ordered Experian to change how it processes personal data, including to more clearly set out in its consumer-facing policies how it processes data about consumers for the purpose of direct marketing. It also ordered it to cease processing personal data where there is insufficient evidence it was collected in a compliant manner.[185]

1.6.3. Canada

Canada's Office of the Privacy Commissioner produced a 2014 research report on data brokers. This noted that online and digital platforms had allowed some data brokers to meld the on- and offline worlds to create mature and contextual profiles of individuals.[186] The report highlighted the importance of balancing the legitimate commercial needs of businesses against the privacy rights of Canadians.[187]

1.6.4. Norway

In 2020, the Norwegian Consumer Council (NCC) published a report on data brokers in the digital marketing and ad tech industry.[188] The report stated that data brokers collect data from both the on- and offline world. They compile and combine this data to create detailed profiles about individual consumers, which are then sold or otherwise traded to other companies.[189] The report noted that these profiles are often used in ways consumers cannot control, and that while some companies are open about their practices, others trade data in complex and opaque ways.[190]

Following the NCC's findings about data brokers' data-sharing practices, in 2021 social media and online dating app Grindr was fined NOK65 million (about A$9.4 million) by Norway's Data Protection Authority, for sharing the personal data of users with third parties for advertising purposes.[191]

184 ICO, ICO takes enforcement action against Experian after data broking investigation, 27 October 2020, accessed via Wayback Machine 15 March 2024.
185 ICO, Experian Limited enforcement notice, October 2020, pp 53-55. At the time of writing, the case is ongoing, with the ICO's appeal scheduled to be heard in 2024, after a lower court overturned parts of the ICO's order. See Mlex, UK ICO's appeal of its Experian enforcement rejection will go to higher court in February, 26 July 2023, accessed 15 March 2024.
186 Office of the Privacy Commissioner of Canada, Data Brokers: A Look at the Canadian and American Landscape, September 2014, accessed 15 March 2024.
187 Office of the Privacy Commissioner of Canada, Data Brokers: A Look at the Canadian and American Landscape, September 2014, accessed 15 March 2024.
188 NCC, Out of Control: How Consumers are Exploited by the Online Advertising Industry, 14 January 2020.
189 NCC, Out of Control: How Consumers are Exploited by the Online Advertising Industry, 14 January 2020, p 20.
190 NCC, Out of Control: How Consumers are Exploited by the Online Advertising Industry, 14 January 2020, p 20.
191 European Data Protection Board, Norwegian DPA imposes fine against Grindr LLC, 21 December 2021, accessed 15 March 2024. See also Reuters, Grindr fine cut to $7 mln in Norway data privacy case, 16 December 2021, accessed 15 March 2024.

2. The use and value of data

Key observations

- Data generated through on- and offline activities records consumers' behaviours, interests, habits, and preferences, and can be collected, stored, processed, analysed, sold or shared.
- Organisations collect, use and monetise data for a range of purposes, including predicting behaviour, improving services, and statistics and research. Businesses also sell or share data for monetary or non-monetary gain.
- Government agencies are key collectors and users of data, for a range of public interest purposes.
- It can be challenging for some business customers to access or obtain valuable data, especially when data is collected and held by one service provider or type of service provider.
- There are a range of methods for businesses to acquire data, either from publicly available sources (such as via web scraping or open data schemes) or through purchasing or licensing data from others.

This chapter provides background on the role of data in the digital and broader economy. It explains the variety of ways in which consumers and businesses generate data, the types of entities that collect data, what data is used for, and how business customers can access data. It is structured as follows:

- **Section 2.1** explains how data is consumers and businesses generate data in their day-to-day on- and offline activities.
- **Section 2.2** identifies why organisations collect data and describes the variety of uses for data.
- **Section 2.3** describes a range of challenges that organisations may face when seeking access to data.
- **Section 2.4** provides an overview of the sources from which organisations can obtain data.

2.1. Data generation

Each time we use a search engine or a navigation app, view content on social media, or purchase something from an online marketplace, we generate data. Some of this data is apparent to us: the words of our search terms, the beginning and end of our journey, the audio-visual content of a video we watched, or the product we purchased and its price.

Other data generated by our activity may be less visible, but just as valuable – data also captures whether we searched from a desktop computer, mobile phone, or via voice-assisted search, what mode of transportation we preferred, how long we watched a video or advertisement for, and at what time of day we made the purchase. This data also forms records of our on- and offline behaviours and preferences, and can be collected, stored, processed, analysed, sold, or shared.[192]

[192] T Morey, T Forbath and A Schoop, Customer Data: Designing for Transparency and Trust, *Harvard Business Review,* May 2015, accessed 15 March 2024.

The data that is generated through these kinds of activities is collected by service providers, including retail platforms and online marketplaces,[193] smart device manufacturers,[194] telecommunications companies,[195] financial institutions[196] and card payment providers, transport providers,[197] real estate agencies,[198] news media businesses[199] and other organisations. This type of data collection can be described as 'first-party' data collection, meaning the entity collecting the data has a direct relationship with the consumer providing or generating the data.[200] This collection of data is also usually governed by the collecting entity's terms of service and privacy policies. While this type of data collection is not a new development, technological advances have increased the scale on which it can occur and the value it can bring.

The consumer data such entities collect can fall into a wide range of categories, such as:

- identifying information (e.g. name, address, email address, phone number)
- demographic data (e.g. age, gender, marital status)
- financial and transaction data (e.g. income, debts, purchase history and habits)
- location data (e.g. from mobile phones, transactions, online activities, navigation)
- interests and preferences (either gathered directly, for example through surveys or subscriptions, customer loyalty schemes,[201] or inferred from on- or offline behaviours).

Consumers and businesses also generate data when engaging with government, at the federal, state, and local levels. Governments are significant collectors and users of data for the purpose of governing and to support other public policy objectives. Data collected by government includes:

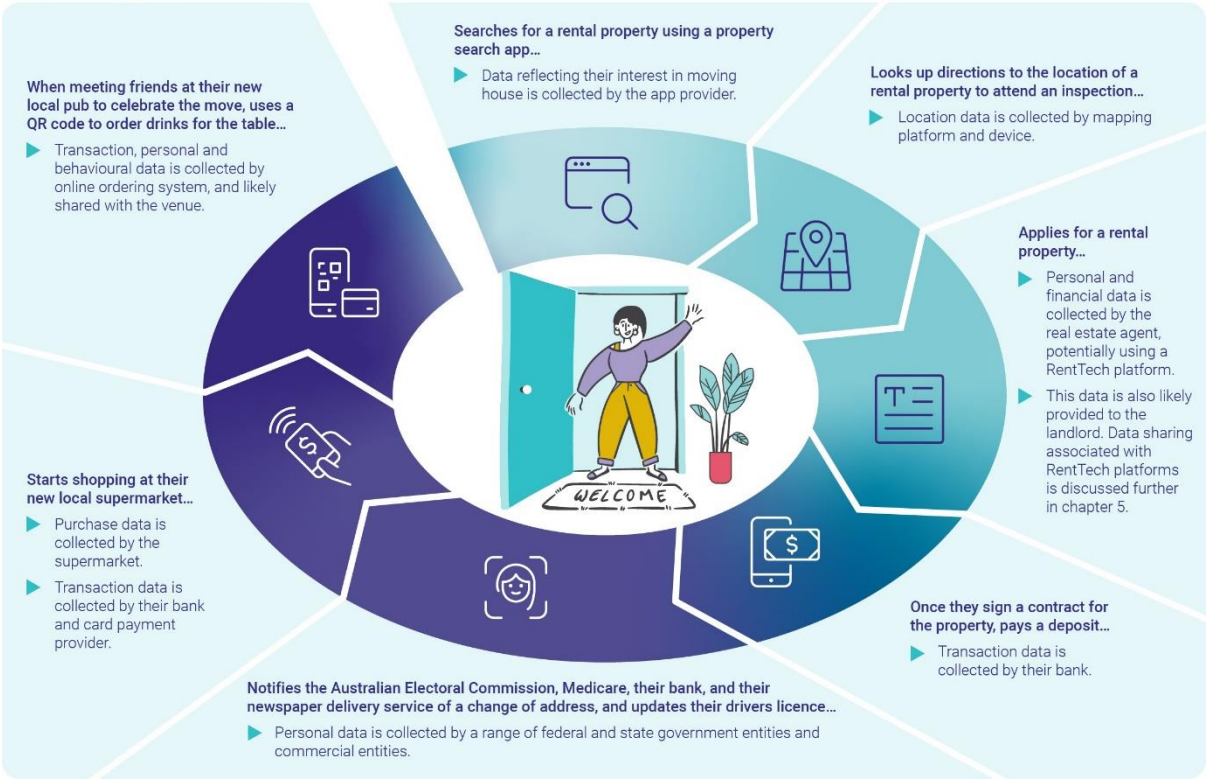
- weather and climate data (e.g. collected by the Bureau of Meteorology and Department of Climate Change, Energy, the Environment and Water)
- business data (e.g. collected by ASIC, IP Australia and the ATO in accordance with legislative roles and responsibilities)
- property data (e.g. collected by state and territory land titles offices)
- transport data (e.g. collected by federal, state and local entities responsible for public transport, roads and aviation)
- information on persons (e.g. collected by government agencies responsible for social services, immigration and law enforcement).

Examples of how a consumer generates data in their day-to-day activities are set out in figure 2.1.

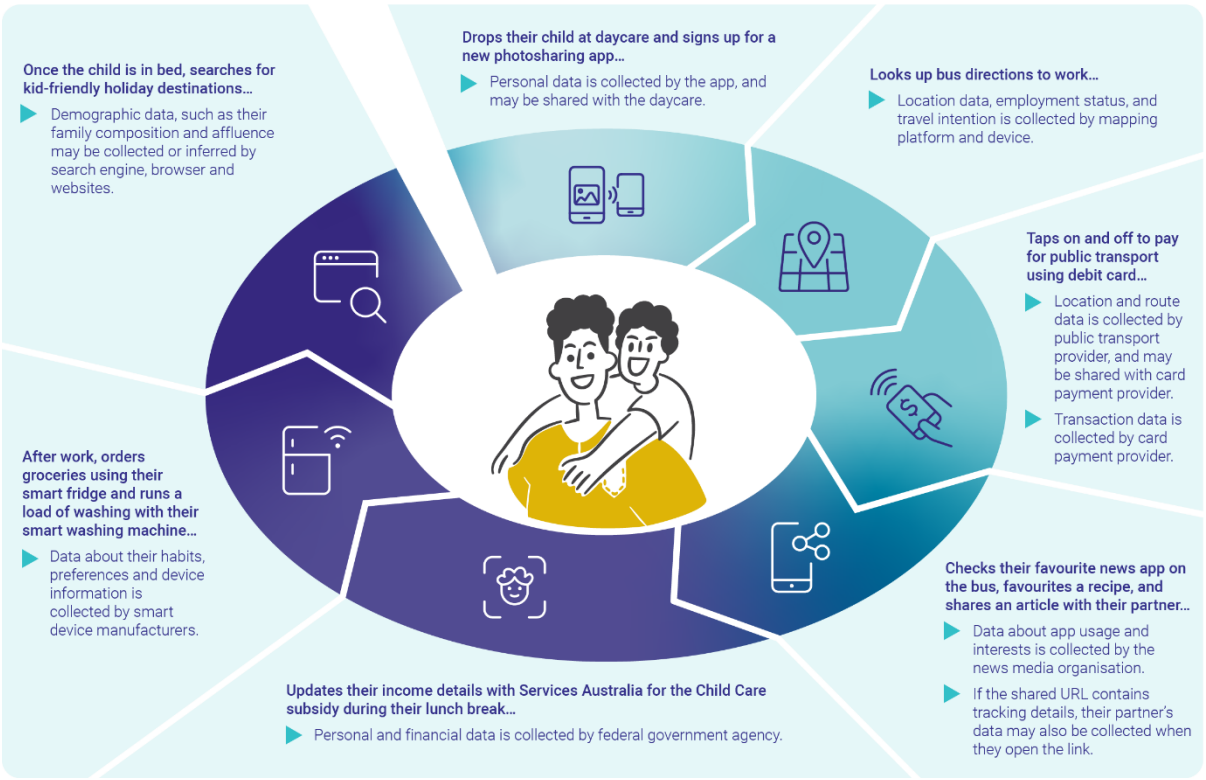
193 ACCC, Digital Platform Services Inquiry – Interim Report No. 4 – General online retail marketplaces, 28 April 2022, p 4.
194 ACCC, Digital Platform Services Inquiry – Interim Report No. 7 - Report on expanding ecosystems of digital platform service providers, 27 November 2023, p 6.
195 OAIC, Telecommunications: data retention scheme, accessed 15 March 2024.
196 World Economic Forum, The Appropriate Use of Customer Data in Financial Services, September 2018, p 6.
197 Uber, How Data Shapes the Uber Rider App, 21 August 2021, accessed 15 March 2024.
198 R Chirgwin, NSW gov wants to cut real estate data collection, *IT News*, 9 November 2022, accessed 15 March 2024.
199 D Wilding, P Fray, S Molitorisz and E McKewon, The Impact of Digital Platforms on News and Journalistic Content, *University of Technology Sydney,* 2018, accessed 15 March 2024, p 51.
200 Discussed further in ACCC, Digital Platform Services Inquiry Eighth Interim Report – Issues Paper, 10 July 2023, p 4.
201 ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019, p 47.

Figure 2.1: Examples of how consumers generate data in their day-to-day activities

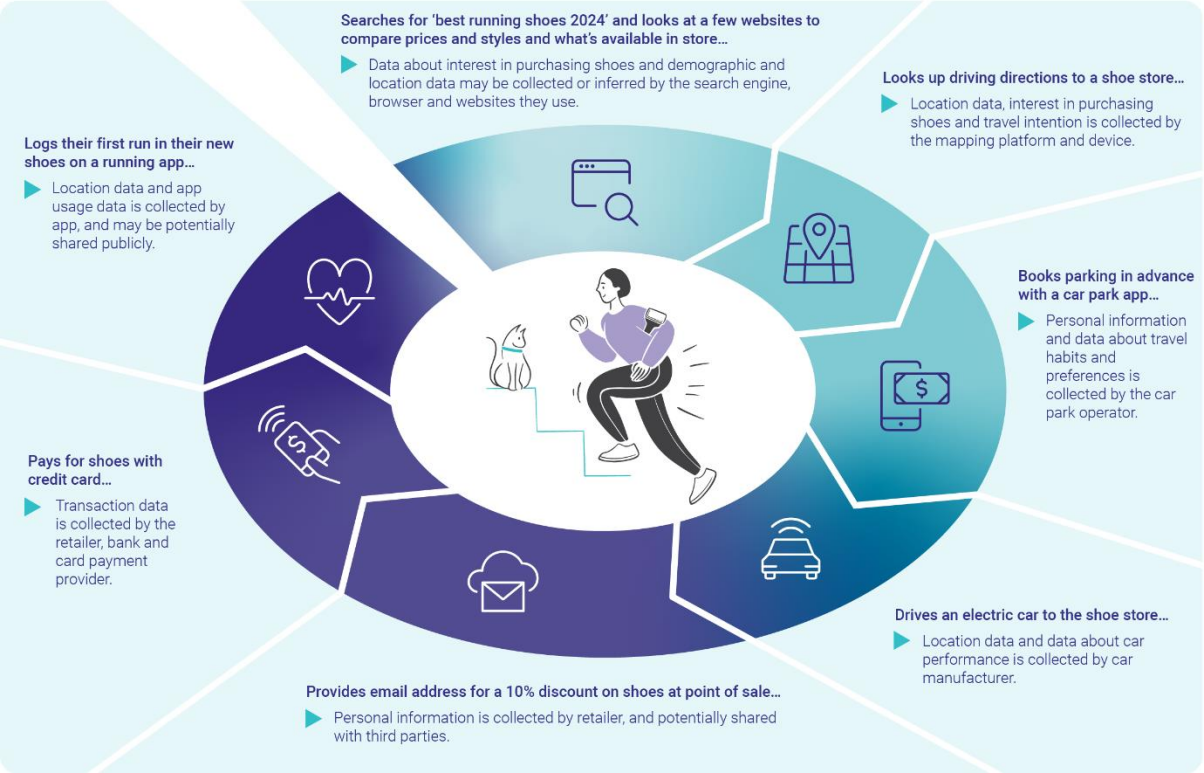
A prospective tenant:



A busy parent:



A future athlete:



2.2. Why organisations collect and use data

For many products and services in today's world, especially in the digital economy, data is considered a key or even essential input. Data can enable public and private entities to innovate and develop better services, tailor and target service offerings and advertising to consumers and prospective consumers, retain existing consumers and set prices that maximise profit. The commercial value of data can be significant for a range of businesses.[202] However, some of these uses and outcomes can also result in potential consumer harms, as discussed in chapter 5.

The value or utility of data is often reflected in how it is used, and by whom. Data can be used for the purpose for which it was collected (e.g. an online store collecting an email address to contact you about your order). However, it can also be valuable for other secondary purposes (e.g. a business contacting you to request a review, for marketing purposes, or combining your information with other data, to better understand its customer base). Even data that appears to be limited in utility may become valuable when combined with other data, shared with a different business, or incorporated into a novel technology or service.

2.2.1. Data analysis

Data is frequently used to draw inferences and make predictions about likely behaviour. Drawing on principles of statistics, data scientists and data analysts create models and develop algorithms to analyse data. This analysis enables data practitioners to observe trends and patterns, understand and predict likely outcomes or behaviour and derive

[202] See, for example, L Baird, How airlines rely on your loyalty to make money, *Australian Financial Review*, 10 March 2023, accessed 15 March 2024. See also Productivity Commission, Data availability and use, 8 May 2017, accessed 15 March 2024; PWC, Putting a value on data, 2019, accessed 15 March 2024.

consumer insights. Importantly, the more data that a business has access to, the greater the potential for sophisticated and accurate data analysis.[203]

Data analysis is undertaken by and for a wide range of organisations. For example:

- Social media platforms use data about users to make decisions about which content to show them.[204]
- Retailers may use inferences and patterns drawn from purchasing or customer loyalty data[205] to decide when or where to open stores, what products to stock, and how to display them to consumers,[206] how to tailor offers to individual consumers and how to develop their own brand products.[207]
- Insurance companies use a wide range of data, including customer data, property data and statistics to make decisions about insurance premiums and coverage.[208]

One of the key uses for data analysis by businesses is for targeted advertising. For example, digital platforms, such as Google and Meta, which operate multi-sided platforms, collect vast amounts of consumer data, which they use to develop and sell sophisticated targeted display advertising services.[209] In general, the larger the user base of a social media platform and the more time users spend on the platform, the more data the platform can collect. This leads to larger platforms being able to offer more detailed targeting to advertisers.[210] Similarly, advertisers and publishers use data about consumers' interests to target advertising. Targeted advertising services offered and facilitated by data firms are discussed in further detail in section 3.2.4 of this Report.

Other ways in which data firms analyse data to develop data products and services are discussed further in chapters 3 and 4.

203 ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, p 76.
204 ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, p 76.
205 ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019, p 47.
206 ACCC, Digital Platform Services Inquiry – Interim Report No. 4 – General online retail marketplaces, 28 April 2022, pp 31–34. This report noted that consumer data is a valuable input for online marketplaces, enabling them to better tailor the products displayed to buyers. It found that online marketplaces collect significant amounts of consumer data, beyond what is necessary to fulfil an order.
207 In its submission on our Issues Paper, the Australian Retailers Association observes 'the increasing reliance of retailers on data-driven insights for enhancing consumer experiences and business strategies'. Australian Retailers Association, Submission to the Report, 28 September 2023.
208 A Arndt, Insurance companies using data collection tools to gain a competitive edge, *Experian,* 15 June 2022, accessed 15 March 2024.
209 ACCC, Digital Platforms Inquiry – Final Report, 28 July 2019, p 7; ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, pp 25–26, 76. ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 37.
210 ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, p 76.

Box 2.1 Data and generative AI

With the recent emergence of novel generative artificial intelligence (AI) technologies and associated product and service offerings, there is a renewed interest in the value of data, especially high-quality and large-scale datasets. We note the Productivity Commission recently stated that AI makes data more valuable.[211]

Data is a key input for training foundation models,[212] which are trained using datasets drawn from a wide range of data often including web scraped or crawled data. Generative AI products and services, such as ChatGPT, function by 'predicting' the correct response to a user prompt based on the model's analysis of the data.

Generative AI products and services present new opportunities for business customers, which can use these data analysis technologies to efficiently process large volumes of data and develop and supply new products and services. For example, real estate agencies could use generative AI technology to draft advertisements for property listings, banks could use generative AI chatbots to engage with customers, and marketing companies or advertisers could use generative AI to develop highly personalised targeted advertising content.

Generative AI datasets that include consumer data have many of the same potential consumer issues discussed in chapter 5.[213] Trust in these technologies may be undermined if consumers do not understand or cannot control how an organisation uses their information. Many organisations have already changed their terms and conditions to provide for the use of consumer data for AI products and services as a condition of using the service.[214]

2.2.2. Service improvement

Data can be a useful input for businesses to enhance their service offerings. Indeed, 'service monitoring and improvement' is often cited as a use for collected data in privacy policies.[215] Peter Leonard's submission in response to the Issues Paper states that the 'use of applications-as-a-service, and associated sharing of data in multiparty data ecosystems, are the norm and an essential incident of the modern Australian economy'.[216] Data can enable organisations to:

- understand how consumers use a product or service, which can then be used to make improvements to the user experience or identify demand for new or existing products or services[217]
- assess the performance of products or services and identify and resolve issues, especially where performance data can be collected in real time

211 Productivity Commission, Making the most of the AI opportunity – Research paper 3: AI raises the stakes for data policy, January 2024, p 4.
212 See, for example, discussion in CMA, AI Foundation Models Initial Report, 18 September 2023, pp 11–12.
213 For example, generative AI services powered by large language models may be used to facilitate scams or misleading and deceptive conduct. See Digital Platform Regulators Forum, Working Paper 2: Examination of technology – Large language models, 25 October 2023, accessed 15 March 2024.
214 For example, see K Hays, A long list of tech companies are rushing to give themselves the right to use people's data to train AI, *Business Insider*, 14 September 2023, accessed 15 March 2024.
215 For example, Google, Privacy Policy, 15 November 2023, accessed 15 March 2024; Microsoft, Privacy Statement, October 2023, accessed 15 March 2024. The effect of provisions such as these in privacy policies, including the extent to which they permit sharing with third parties, is discussed further in chapter 5.
216 P Leonard, Submission to the Report, 28 September 2023, p 4.
217 Data can also be used to design user experiences in a way that targets consumers' vulnerability ('dark patterns'): see CPRC, Unfair Trading Practices in Digital Markets – Evidence and Regulatory Gaps, December 2020, pp 8–10 (discussed further in ACCC, Digital Platform Services Inquiry – Interim Report No. 5 – Regulatory reform, 11 November 2022, p 68).

- innovate by developing new products and services based on user trends or behaviours
- reduce costs, for example by marketing, developing, acquiring, storing and shipping products more efficiently
- set prices in a profit-maximising way, based on a review of publicly available pricing data
- test and monitor the release of new features.

2.2.3. Identification

Data can also be used to effectively and accurately identify individuals. Using data to identify individuals has a range of uses. These include:

- using facial recognition data to identify individuals, e.g. when attending an event at a stadium[218]
- collecting and validating biometric data, e.g. at immigration control[219]
- fraud prevention and identity verification, as discussed in section 3.3 of this Report.

Uses of data in these ways may be for the purposes of security, law enforcement, and prevention of unlawful or criminal behaviour. We note the use of data in these ways is not always without controversy.[220]

2.2.4. Tracking

Data can also be used to track individuals and their activities on- and offline. Online, data-based tracking methods include using identifiers such as log-in details, cookies, and IP addresses to track which websites an individual visits. Offline tracking relies on using location data, often from mobile device or social media use. Location data can also be used in combination with other data, such as transaction records, to identify an individual's movements and activities.

Data-based tracking is key to profiling and targeting advertising to individuals, discussed further in section 3.2.

Concerns related to the potential harms of using data, particularly location data, for on- and offline tracking are discussed further in chapter 5.

2.2.5. Statistics and research

An important and longstanding use of data is for statistics and research. Researchers and academics collect, process, and analyse data to pursue research activities and to develop understanding in a wide variety of fields. Data use in public and private research is often strictly regulated by research ethics processes and considerations, alongside the protections offered by privacy law.

---

218 S Meacham, The major Aussie stadiums using facial recognition technology, *9 News*, 5 July 2023, accessed 15 March 2024.

219 Office of the Victorian Information Commissioner, Biometrics and Privacy – Issues and Challenges, accessed 15 March 2024.

220 For example, see N Geraets, Australian music venues criticised for use of facial recognition technology, *Sydney Morning Herald*, 5 July 2023, accessed 15 March 2024.

2.2.6. Selling and sharing data

Datasets can also be assets in that they can be monetised by selling or licensing them to other organisations. This can provide an additional source of revenue to the organisations that collected the data.

Organisations can also extract value from sharing data, such as by exchanging it for other data or products or services of non-monetary value. Selling and sharing of data often occurs without the knowledge or understanding of consumers, as discussed further in chapter 5.

2.2.7. Government use of data

As set out above, government entities collect data for the purpose of governing and to support other public policy objectives. This includes making decisions, regulating particular sectors, providing services and benefits, and enabling law enforcement activities.

Examples of government use of data include:

- Government departments using census data to understand the population and make decisions about service delivery.
- Services Australia using income data to make decisions about eligibility for certain welfare payments.
- The Australian Taxation Office using data on income and in tax returns to make taxation determinations.
- Law enforcement agencies using data to identify trends and identify and prevent potential criminal behaviour. For example, AUSTRAC collects data from banks on transactions to identify money laundering and terrorism financing activity.
- Regulators, including the ACCC[221], using data to perform their regulatory functions and to inform decisions and policy.

2.3. Challenges to accessing data

As described in section 2.2, data is commercially and competitively important to a range of businesses across industries. However, as much as businesses rely on data in their operations, they may face challenges in obtaining data, especially granular, high-quality consumer data.

Key amongst these challenges is the fact that data generated through online behaviour is often only available to the business whose product or service the consumer was using when data was generated. For example, the personal information that a consumer supplies when subscribing to or using an online service, and which is collected by an online service provider in the course of the consumer's use of the online service, is generally not able to be accessed freely by that online service with others. If another business wanted or needed to use the data, for example to develop a competing product or service, they would need the business that collected the data to sell, license or share it. There would also be legal considerations that govern the sharing of personal information. This situation can result in businesses that operate services that enable them to collect consumer data experiencing a

[221] For example, in the context of the DPSI, the ACCC has purchased data from SensorTower. The ACCC also engages with data firms to obtain data relevant to its market inquiries and investigation and merger review processes. The ACCC uses data that it obtains from parties in connection with its functions and powers under the CCA.

'data advantage' in markets in which they operate.[222] Data as a competitively valuable asset is discussed further in chapter 6.

Further discussion of data access follows below, outlining both legal considerations and practical challenges.

2.3.1. Legal considerations

Legal considerations can sometimes impact the incentive or ability for businesses to share data with others. For example:

- **Intellectual property law:** Some data may be protected by copyright law (such as the data that constitutes an electronic recording of a song) or trade secrets protections. It has been observed that the application of copyright law to restrict access to certain data is particularly relevant in relation to the development of generative AI products and technologies.[223]
- **Contract terms:** Contract law and the terms of contracts for sale or licensing of data may also restrict who can access data and for what purposes. For example, data may be licensed on a non-exclusive or exclusive basis, with the latter meaning that only the licensor and licensee have access to the data. Additionally, data agreements may contain limitations on the purposes for which data can be used, such as limiting use to non-commercial or research purposes.

2.3.2. Practical challenges

Practical challenges can also impact the incentive or ability for businesses to share data with others. For example:

- **Technological capability:** Organisations without technological capability or know-how may struggle to effectively identify what data they need and then obtain that data. Moreover, to the extent that they do have the ability to collect or access data, they may be limited in the extent to which they can effectively store, process or analyse it. A lack of interoperability between data formats or data processing tools and technologies can also restrict an organisation's ability to access and benefit from using data.
- **Infrastructure**: In order to access, store, process and analyse data, organisations need to have the correct infrastructure, including a means to receive data transfers and ensure the security and reliability of data.
- **Cost**: For some businesses, especially small and medium businesses, the cost of purchasing or licensing data, or acquiring the technological or personnel capabilities to process or analyse the data, can be prohibitive. This can intersect with other challenges outlined above, in that hiring capable talent, reformatting data or developing infrastructure can all be costly.
- **Data quality**: Business customers may face difficulties in gaining access to high-quality data, especially more complex datasets that are not easily replicable, which can be significantly more valuable. Timeliness is also an important aspect of data; older data may not be as useful as up-to-the-minute information.

---

222 See ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 77. See also A Hagiu and J Wright, When data creates competitive advantage, Harvard Business Review, January-February 2020, accessed 15 March 2024. As to broader impacts of unequal access to data, see A Fisher and T Streinz, Confronting Data Inequality, 60(3) Columbia Journal of Transnational Law, 829-956 (2022).

223 M Dincer, J Karr, J Schultz and M Weinburg, Generative AI Legal Explainer, 2023, accessed 15 March 2024.

2.4. Sources of data

There is a variety of sources of data available to organisations. These sources may be used by organisations that face challenges in accessing data or organisations that seek to complement and enhance the data they already have. Some key sources of data and how they are accessed are described below.

2.4.1. Publicly available data

A significant amount of data is publicly available, with few limitations on access. For example, data about the movements of planes and ships can be easily collected either from open access websites or by using a radio receiver to receive signals transmitted by vessels.[224] Government records, such as court records, are also largely publicly available sources of data.

Web scraping is a key technique used to collect valuable data from publicly accessible webpages, including personal information from social media platforms, property information, and other commercially valuable information, such as earnings calls, stock price changes, and news reports about corporate developments.

However, the use of web scraping technologies has been challenged by website and copyright owners, particularly in the context of recent developments in generative AI.[225] In particular, web scraping, and other methods of collecting or accessing publicly available data, have been challenged on the basis that they contravene the terms of service of a webpage or service provider. [226] Collecting publicly available data can also be frustrated by technological protections, such as paywalls or inaccessible data formats.

Screen scraping has been considered in government review processes, such as the 2022 Statutory Review of the CDR, which recommended that screen scraping be banned where CDR is a viable alternative.[227] In 2023, in response to the Statutory Review, the Treasury conducted a consultation process on options for regulating screen scraping practices. [228]

As discussed further below, in certain cases, businesses may need to pay a fee to access some publicly available information, especially when requesting data that is detailed, in large quantities or in specified formats. This may require the data supplier to manually collate and provide data.[229]

Data can also be intentionally made publicly available for specific reasons, such as open data schemes that promote access to certain data, and data-sharing schemes designed to promote competition.

---

224 For example, FlightAware, accessed 15 March 2024; MarineTraffic, accessed 15 March 2024. This type of publicly available data can be used to ascertain information about individuals: J Weatherbed, The Elon Musk private jet tracker resurfaces on Threads and immediately goads Mark Zuckerberg, *The Verge*, 10 July 2023, accessed 15 March 2024.

225 For example, LinkedIn and Meta have both sued businesses that sold data products and services developed by processing web scraped data. O Tene, LinkedIn v HiQ and the trans-Atlantic privacy divide, *International Association of Privacy Professionals*, 22 April 2022, accessed 15 March 2024; J Romero, Taking action against scraping for hire, Meta, 5 July 2022, accessed 15 March 2024.

226 King & Wood Mallesons, Screen Scraping: A question of Legality, 9 July 2020, accessed 15 March 2024.

227 The Treasury, Statutory Review of the Consumer Data Right – Report, 29 September 2022, p 12.

228 The Treasury, Screen scraping – policy and regulatory implications, 25 October 2023, p 3.

229 For example while some business register information is available for free on ASIC Connect, access to more detailed information requires payment of a fee: ASIC, Search fees, accessed 15 March 2024. The Australian Bureau of Statistics offers and information consultancy service, operates on a cost recovery basis: Australian Bureau of Statistics, Consultancy Request Form, accessed 15 March 2024.

Open data schemes

Acknowledging that data is a valuable resource, governments in many jurisdictions, national state and local, have developed 'open data' schemes. These make data, usually government data, available either to accredited users or openly for anyone to access. Open data schemes can be distinguished from publicly available data (as described above) in that they represent a deliberate initiative by the data custodian to make data available for wider use.

Open data initiatives are often motivated by a general view of the value of data for a variety of purposes, including non-commercial and research uses. Use of open data may also promote innovation or competition, but unlike the statutory data-sharing schemes described below, these schemes are not specifically intended to enable competition.

Access to 'open data' is often regulated by terms and conditions or rules, which may restrict who can access the data, or for what purposes the data may be used. A feature of many open data schemes is that they only make available de-identified data. However, as discussed in chapter 5, there are risks that de-identified data can be re-identified in certain cases.

Examples of open data schemes include:

- Data.gov.au[230]
- State-based open data schemes, such as data.nsw[231] and Data Vic[232]
- Transport data, such as the Transport for New South Wales Data Hub[233]
- Health data sharing to enable research, such as World Health Organisation data collections and various COVID-19 open data projects.[234]

There are also some examples of privately operated open data schemes. Cloud providers such as Amazon (AWS) and Microsoft (Azure) offer open data access to specific datasets that are stored within and accessible to users of their cloud infrastructure.[235] Meta also provides some open data access to certain users via its platforms Data for Good[236] and CrowdTangle.[237]

We also note the Data Availability and Transparency Act (DATA) Scheme which came into effect in April 2022 and promotes better availability of public sector data.[238]

2.4.2. Statutory data-sharing schemes

Data sharing can be used as a remedy to address competition concerns or a lack of competition in a market.[239] This is in recognition of the value of data and its associated competitive advantages, especially in enabling new entrants to challenge dominant firms. It can also address concerns relating to market participants restricting access to data as a way of exercising market power. This can take the form of statutory schemes to enable

230 Australian Government, data.gov.au, accessed 15 March 2024.
231 NSW Government, Data.nsw, accessed 15 March 2024.
232 Victorian Government, Data Vic, accessed 15 March 2024.
233 Transport for New South Wales, Open Data, accessed 15 March 2024.
234 OECD, Open data in action: initiatives during the initial stage of the COVID-19 pandemic, March 2021.
235 AWS, Open Data on AWS, accessed 15 March 2024; Microsoft, Azure Open Datasets, accessed 15 March 2024.
236 Meta, Data for Good, accessed 15 March 2024.
237 Meta, CrowdTangle, accessed 15 March 2024.
238 Under the Act, Commonwealth bodies are authorised to share their public sector data with other Commonwealth bodies, state and territory government bodies and Australian universities that have become accredited users.
239 OECD, Data portability, interoperability and digital platform competition, 2021; S Besen and P Verveer, Competition and Data: Potential Remedies, Wake Forest Journal of Business and Intellectual Property Law, 2021.

access to data to a wider range of organisations. Compared to open data schemes, mandatory data-sharing schemes set out in legislation often allow access to more granular, and therefore more valuable, data.

Examples of existing or proposed statutory data-sharing schemes in Australia and overseas include:

- The Consumer Data Right (CDR) is an example of a statute-based data-sharing scheme in Australia.[240] The CDR, which includes responsibilities for the ACCC and OAIC, enables consumers to elect to choose to share data about their activities with certain providers. Currently, the CDR supports data sharing in the banking and energy sectors.
- The Australian Motor Vehicle Information Scheme (MVIS), which requires motor vehicle service and repair information (collected by vehicle manufacturers) to be made available to all Australian motor vehicle repairers and registered training organisations to buy at a price that does not exceed its fair market value.[241]
- The data-sharing provisions applicable to certain platforms, such as online search engines, set out in the European Union's Digital Markets Act.[242]
- Proposals overseas for 'right-to-repair' laws, which advocate for a similar approach to the MVIS in other industries, such as consumer electrical goods.[243]

In designing and implementing statutory data-sharing schemes, consideration is often given to the tension between the interests of competition and privacy, given the schemes can involve the sharing of personal information.[244] Further discussion of the intersections of competition and privacy is set out in chapter 6.

240 Consumer Data Right, Giving you choice and control, accessed 15 March 2024.

241 ACCC, Motor vehicle information scheme (MVIS), accessed 15 March 2024. Under the *Competition and Consumer Act 2010 (Cth)* motor vehicle service and repair information must be made available to all Australian motor vehicle repairers (repairers) and registered training organisations (RTOs) to buy at a price that does not exceed the fair market value.

242 Article 6(10) of the EU's Digital Markets Act provides: "The gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users." European Union, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 14 September 2022.

243 AuManufacturing, If you buy it, why can't you fix it? Here's why we still don't have the 'right to repair', 18 April 2023, accessed 15 March 2024.

244 ACCC, Digital Platforms Inquiry Final Report, 26 July 2019, p 5; ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 78–79.

2.4.3. Purchasing and licensing data

As noted in section 2.2.6, organisations may sell or license data they have collected or generated to other organisations.

Data can be purchased or licensed from a range of sources, including:

- Federal and state government entities, including ASIC Connect,[245] state and territory courts authorities,[246] Australia Post[247] and state and territory land titles offices and Valuer-General's offices.[248]
- Businesses in industries such as retail, marketing, technology, real estate, and financial services.[249]

Business customers seeking to use and benefit from data can engage the services of a data firm. Data firms collect data from publicly available sources, and also purchase it from government entities and business, including other data firms.[250]

Using the services of a data firm can help business customers overcome some of the challenges to accessing data identified in section 2.3. For example:

- In many cases, liability for non-compliance with intellectual property or contract law would likely fall on the data firm that supplied a business customer with data products and services.
- Data firms have sophisticated technological capabilities, allowing business customers to effectively 'outsource' the need to have such capabilities in-house. Data firms can identify data requirements and opportunities and ensure that data is made available in appropriate and useable formats, including by tailoring a product or service for the business customer.
- Data firms sometimes promote the fact that they are able to provide data products and services in ways that integrate with a business customer's existing data and operational infrastructures.
- In many cases, the cost to a business customer of acquiring data products and services from a data firm is likely to be less than the cost of the business customer collecting data itself.
- Data firms have knowledge of and access to a range of data sources, as well as tools to clean and validate data, meaning that data products and services supplied by data firms may be more to reflect valuable, complex, and up-to-date data.

Organisations engaging data firms may buy datasets (such as those comprising personal or other information on persons) directly from a data firm, including via a data marketplace provided by a data firm, discussed in box 2.2.

245 ASIC, ASIC Connect and Information brokers, accessed 15 March 2024.
246 For example, Equifax collects court data to develop data products and services. See Equifax, Swiftcheck: What are court actions, accessed 15 March 2024.
247 Australia Post, Access data & insights, accessed 15 March 2024.
248 See, for example, Victoria State Government, Department of Transport and Planning: Victorian Land and property information; NSW Land Registry Services, Access titling information; and Queensland Government, Property sales and valuations products and services, accessed 15 March 2024.
249 Information provided to the ACCC.
250 ACCC, Digital Advertising Services Inquiry – Final Report, 28 September 2021, p 34.

Box 2.2 Data marketplaces

Data marketplaces are online services that facilitate the buying, selling and exchange of (largely) third-party data. The data that is bought, sold and exchanged may be observed or derived data, such as in the form of segments. It may include demographics (age, gender etc.), preferences (such as car types, travel preferences or shopping preferences), family composition (such as 'kids in household' or 'young couples'), and business to business (B2B) data such as industry of employment.

A number of data firms offer data marketplace services in Australia, including Snowflake,[251] wattwatchers,[252] and Lotame.[253] However, as discussed in section 1.3.1 of this Report, some data firms have moved away from offering data marketplaces. For example, LiveRamp has discontinued its Data Marketplace in Australia[254] and, prior to being acquired to IXUP, Data Republic 'evolved from being a data marketplace to an enterprise software [firm]'.[255] We note that privacy laws in Australia may impact the ability of data firms to offer data marketplace services.

An overview of the data products and services supplied by data firms in Australia is discussed in chapter 3. A description of data firms that supply these products and services is set out in chapter 4.

[251] Snowflake, Marketplace, accessed 15 March 2024. CoreLogic has a partnership with Snowflake to use its Data Marketplace. See CoreLogic, Snowflake marketplace, accessed 15 March 2024.
[252] Wattwatchers, Data services, accessed 15 March 2024.
[253] Lotame, homepage; and CMO, New second-party data marketplace debuts, 13 September 2019, accessed 15 March 2024.
[254] LiveRamp, Submission to the Report, 28 September 2023, p 4.
[255] InnovationAus, Data Republic's new global challenge, 17 June 2019, accessed 15 March 2024.

3. Data products and services

Key observations

- Data firms supply a range of data products and services to business customers across many industries for a variety of purposes. These include marketing and advertising, risk management and property management resources.
- Businesses may use data-driven marketing and advertising products and services for enrichment, profiling, segmentation, targeted advertising, and ad measurement and optimisation. Broadly, these products and services are designed to support business customers' marketing activities by improving their data related to their target audiences.
- Some data firms offer 'data clean room' platforms to their business customers. These are often marketed as compliant with privacy law, though the standards of de-identification or anonymisation used across different clean rooms may vary. In some cases, these products may enable the comparison and exchange of datasets in a way that allows consumer data to later be re-identified.
- Risk management products and services include verification services that help to confirm an individual's identity or other information provided by an individual. Some of these products and services also assist with fraud detection and prevention.
- Real estate agents, landlords, renters and buyers use a range of specialised data and analytics services to buy, sell, rent and manage properties.

This chapter explores the main categories of data products and services offered by data firms and the key customers of these products and services. It is structured as follows:

- **Section 3.1** provides an overview of the types and sources of data used to develop the products and services described in this chapter.
- **Section 3.2** describes data-driven marketing and advertising products and services, including data enrichment, profiling, segmentation, targeted advertising, and ad measurement and optimisation.
- **Section 3.3** explores risk management products and services, including verification and fraud detection services.
- **Section 3.4** describes property management services, also known as 'PropTech', including property data platforms, real estate listings websites, 'RentTech' products, and construction and commercial property products.

3.1. What are data products and services and how are they developed?

The main categories of data products and services considered in this Report are:

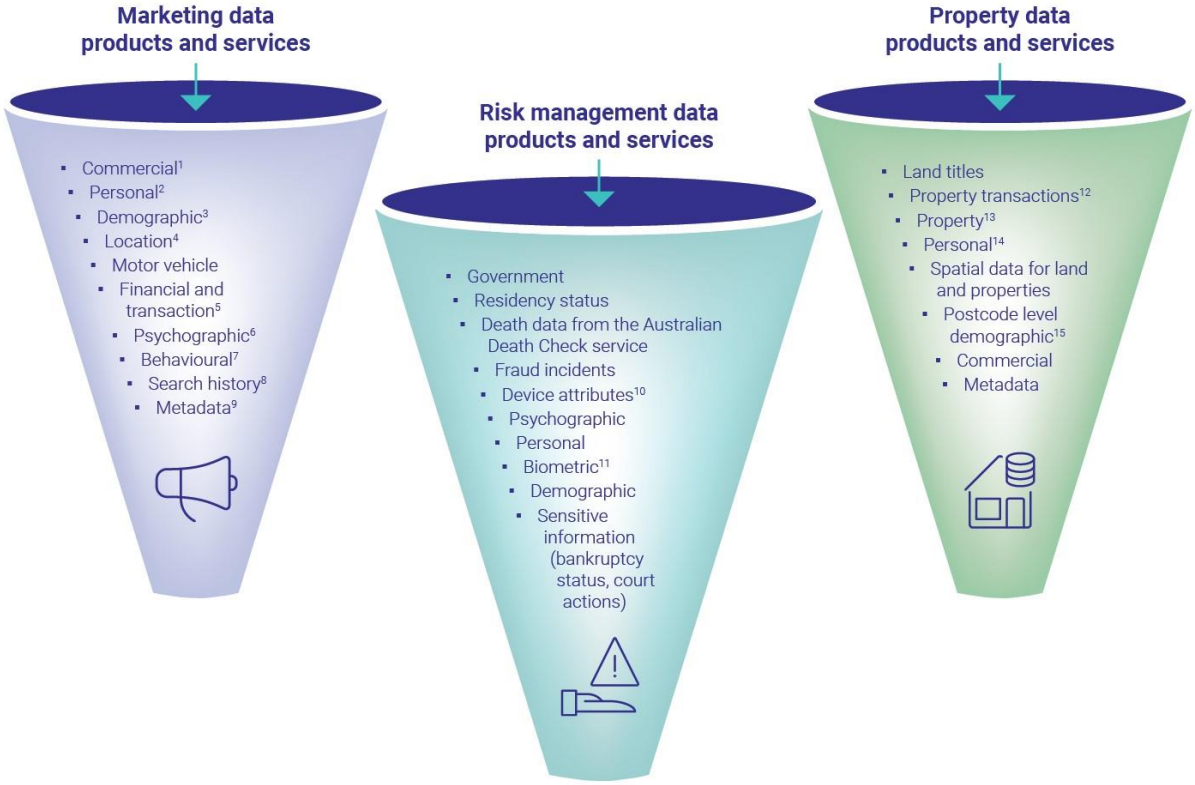
- **Marketing and advertising products and services,** including data enrichment, profiling, segmentation, targeted advertising, and ad measurement and optimisation products and services.

- **Risk management products and services**, including identity verification and fraud detection services.
- **Property products and services**, including property data platforms, real estate listing websites, RentTech products, and construction and commercial property products.

We note that these categories are non-exhaustive, given the wide and ever-increasing variety of data products and services that are developed and supplied in Australia and globally.

As shown in figure 3.1 below, data products and services are developed by data firms using a wide range of collected data as 'inputs'.

Figure 3.1: Types of data that may be used in key data products and services



Note that in figure 3.1 above:

1. Commercial data may include company structure, ownership and directorship details, shareholder data, financial data, business-to-business payment data, and business size and turnover data.
2. Personal data may include names, email addresses, phone numbers and dates of birth.
3. Demographic data may include age, gender, education, occupation, household income, ethnicity and marital status.
4. Location data may include data on consumers' location history and the geographic area they live in.
5. Financial and transaction data may include spending and purchasing behaviour.
6. Psychographic data may include information on consumers' attitudes, interests, activities, lifestyle and values.
7. Behavioural data may include information on social media use and engagement with TV and radio programs or particular advertising campaigns.
8. Search history data may include online search terms, IP addresses, device or advertising IDs and device fingerprints.
9. Metadata in an advertising context may include data on what video and audio a person is watching or listening to and for how long. In a property context, it may include details of when and how they access a property listings website (e.g. browser and device type, IP address and date and time of access).
10. In a risk management context, device attributes data may include whether an individual's device details match those of any devices used in known fraudulent activities.
11. Biometric data may include facial recognition data.
12. Property transactions data may include sales history, past sale prices, property ownership details and lease history.
13. Property data may include property type, year built, latitude and longitude, street address, number of bedrooms, bathrooms and car spaces, floorplan and total land area.
14. Personal data in a property context may include the financial history of prospective tenants or home loan applicants.
15. Postcode-level demographic data may include school, hospital and property zoning information, nearby public transport facilities and data on supply and demand in the suburb where a property is located.

Data firms collect the data they use in data products and services from a variety of the sources discussed in chapter 2, including:

- government entities[256]
- business customers[257]
- publicly available sources, including open data, webpages and social media, and data gathered via web scraping.[258]

Data firms develop their products and services by using a range of processing and analysis techniques. Data processing refers to the conversion of 'raw' data into a usable and understandable format, usually over multiple steps.[259] Data analysis involves a range of methods used to collate and interrogate data, including statistical analysis, processing, and modelling. Data analysis can be used to make predictions, observe trends, draw conclusions, and inform decisions.[260]

Specific methods of data processing and analysis include:

- **Data cleaning and validation**: the detection and removal (or correction) of errors and inconsistencies in a dataset or database due to data corruption or inaccurate entry,[261] which may also involve collating and transforming data into a standard format.[262]
- **Trend analysis**: The use of historical data as well as current datasets to identify behaviour, events, trends or occurrences. Trend analysis is useful in contexts relating to identifying consumer behaviour, or identifying market trends.[263]
- **Deriving and inferring**: processing and analysing data to identify trends or patterns and extrapolate potential options or conclusions. This processing can include cross-referencing of different sources of data. Derived data may, for example, enable attributes to be added to customer data by assigning customer segments or assigning a likelihood a person represented in the data will buy a certain product.[264]

3.2. Data-driven marketing and advertising products and services

Data processing and analysis play a key role in modern marketing and advertising.[265]

Marketing refers to activities that assist in building a business or brand, by identifying and understanding actual or potential customers, and developing tailored communication strategies to both retain existing customers and attract new ones.[266]

---

256 See section 2.4.3 for a discussion of data sources from federal and state government entities.
257 See section 2.4.3 for a discussion of data sources from business customers.
258 See section 2.4.1 for a discussion of data sources from publicly available sources.
259 Smrtr, Top Tips for Data Processing, accessed 15 March 2024.
260 Zapier, What is data analysis? Examples and how to get started, accessed 15 March 2024.
261 Better Evaluation, Data Cleaning, accessed 15 March 2024.
262 O Elgabry, The Ultimate Guide to Data Cleaning, *Medium: Towards Data* Science, 1 March 2019, accessed 15 March 2024.
263 Quantilope, What is Trend Analysis in Research? Types, Methods, and Examples, *Quantilope Blog*, 29 January 2024, accessed 15 March 2024.
264 S O'Regan, Designing Data Products, *Medium: Towards Data Science*, 17 August 2018, accessed 15 March 2024. See also OECD, *Mapping Approaches to Data and data Flows*, 2020, p 16; M Abrams, *The Origins of Personal Data and its Implications for Governance*, 24 November 2014.
265 Prior work by the ACCC has found that 'data about consumers, and their online activity, and in some cases offline activity, is important to the supply of ad tech.' See ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 37.
266 K Snyder, What is Marketing? Definition, Strategies & Best Practices, *Forbes Advisor*, 6 November 2023, accessed 15 March 2024.

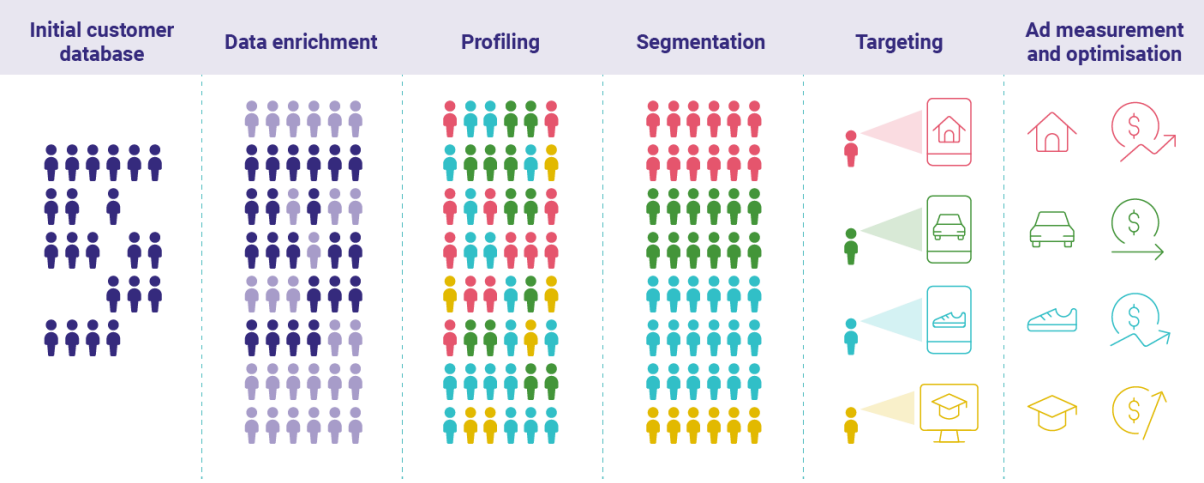
Advertising is the process of actively promoting a business, product or service to audiences through on- and offline channels, including online and mobile advertising, TV, radio, print media, and outdoor advertising (such as billboards).[267]

Data-driven marketing and advertising services include:

- **Data enrichment**: assisting businesses to augment, clean and validate their customer databases (discussed in section 3.2.1).
- **Profiling**: processing and analysing data to understand the characteristics or attributes of customers, individually or collectively (discussed in section 3.2.2).
- **Segmentation**: grouping customer profiles based on shared interests or attributes (discussed in section 3.2.3).
- **Targeted advertising**: using data analysis tools to predict the most effective advertising placement and format for different customer segments (discussed in section 3.2.4).
- **Measurement and optimisation**: analysing data collected about marketing strategies, advertising engagement, sales and brand recognition to assess and improve the performance of each of the above stages (discussed in section 3.2.5).

The relationship between these services is shown in figure 3.2 below.

Figure 3.2: How data-driven marketing and advertising products may be used



Data firms may offer all or many of these services individually or as a package or suite. For example, a business customer may have sophisticated in-house targeted advertising, measurement and optimisation capacity, but require a data firm's assistance to enrich, profile and segment its customer database. Some data firms provide marketing and advertising services through **data management platforms** (also known as customer data platforms), described in box 3.1.[268]

[267] Microsoft, What's the difference between marketing and advertising?, *Microsoft Create*, 9 October 2023, accessed 15 March 2024.
[268] See, for example, Adobe, Adobe Audience Manager, accessed 15 March 2024.

Box 3.1 Data management platforms

Data management platforms provide business customers (such as publishers and advertisers) with a single platform to store, manage and analyse consumer data, as well as to access data-driven marketing and advertising services.[269] For example, a retailer could use a data management platform to upload transaction data on its customers, enrich it with demographic data provided by a brand partner, select segments to further organise the data, and distribute its target audience segments to publishers or digital platforms to serve advertisements.[270]

To the extent that a data firm's data management platform does not provide the entire suite of data-driven marketing and advertising services, it may be compatible with or integrate other ad delivery and ad measurement services.[271]

We note that LiveRamp illustrates the 'collaboration' between companies that its Safe Haven platform can support by describing Ticketmaster and Spotify as examples of 'things that just go together and make sense'.[272]

LiveRamp has also stated that Safe Haven operates as a data clean room.[273] Data clean rooms are discussed further in box 3.2 below.

3.2.1. Data enrichment

Data enrichment is the process of improving or augmenting a business customer's existing data by combining it with other data, often from an external source.[274] For example, a business that has collected data from its customers may purchase, license or collect additional data about those customers in order to develop a more complete or accurate understanding of them.[275] In the Customer Loyalty Schemes Report, the ACCC noted that CoreLogic was able to combine its customer data with property and behavioural information from another firm. It used this to identify Facebook users who were homeowners and may be inclined to sell their home.[276]

Such additional data may help a business customer develop a more comprehensive understanding of consumer behaviour.[277] For example, an airline could enrich its customer data by acquiring purchase history data from a supermarket or online marketplace – this may enable the airline to understand changes in its customers' spending patterns or what their preferred onboard snacks might be.

Data enrichment services can also include data validation and data cleaning, in order to identify and correct errors and inconsistencies in datasets and ensure the data is accurate, consistent, and complete.[278]

---

269 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 33.
270 T Johnson, The Retail Guide to Data Management Platforms, *Tinuiti*, 14 May 2017, accessed 15 March 2024.
271 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, pp 33-34. See also Oracle, Oracle Unity Customer Data Platform, accessed 15 March 2024.
272 LiveRamp, Data Clean Rooms: Everything You Need to Know, accessed 15 March 2024.
273 See LiveRamp, Data Clean Rooms: A Complete Guide, 20 April 2022, accessed 15 March 2024.
274 Data enrichment is also referred to as data enhancement. See Experian, Data Enrichment and Enhancement | Experian Data Quality, accessed 15 March 2024; Alteryx, Data Enrichment | Glossary, accessed 15 March 2024.
275 See, for example, K Kemp, Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful, Research Paper, 27 September 2022; Experian, Single Customer View | Experian Data Quality, accessed 15 March 2024.
276 ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019, p 72.
277 Mparticle, Data enrichment and machine learning: Maximising the value of your data insights, 23 February 2021, accessed 15 March 2024.
278 See, for example, Experian, Data Enrichment | EDQ Platform, accessed 15 March 2024.

Business customers may also use data enrichment services to identify *potential* customers.[279] Business customers can enrich their customer database by purchasing or licensing data on individuals with similar characteristics or attributes to their existing customers, to expand their customer base.

Box 3.2 Data clean rooms

A data clean room is a digital environment designed to facilitate the sharing and use of data between business customers in a way that may be marketed as compliant with privacy laws.[280] Data clean rooms are often used to facilitate data enrichment, audience targeting,[281] optimisation and measurement.

Business customers using data clean rooms upload their consumer data or other data to the clean room platform. The data firm providing the data clean room may process or analyse the data, including by de-identifying or encrypting it.[282] In the data clean room environment, business customers can identify matches between their datasets and other business customers' datasets they work with ('collaboration partners') using a common identifier or key,[283] which enables further analysis and insights to be drawn.[284] In theory, this can occur without businesses sharing any 'raw data' on consumers.[285]

Data clean room providers include specialised data companies like LiveRamp, Habu and Snowflake,[286] as well as companies such as Amazon, Google and Disney.[287] Data clean rooms are used by businesses in the digital advertising supply chain, such as advertisers and publishers,[288] to access and combine anonymised information to assist them in segmenting and targeting consumers.[289]

Data clean rooms are described by industry participants as a 'privacy-safe'[290] or 'privacy-centric'[291] solution for the 'cookie-less future' of digital advertising.[292] However, the standards of anonymisation can vary, meaning data that may have been anonymised while in a data clean room could later be reidentified outside of the clean room by combining it with other data points, such as cookie and device identifiers, or location data.

279 S Smulders, What is Data Enrichment and How to Use It in Your Sales Process, *Expandi.io*, May 2023, accessed 15 March 2024.

280 J Duball, Data clean rooms: An adtech privacy solution?, *International Association of Privacy Professionals*, 24 January 2023, accessed 15 March 2024.

281 IAB Australia, Submission to the Report, 28 September 2023, pp 4, 9.

282 IAB Australia, Data Collaboration Platforms Explainer, 2 May 2023, p 29; Databricks, Data Clean Rooms, accessed 15 March 2024; S Kerner, Definition: Data Clean Room, *TechTarget*, accessed 15 March 2024.

283 N Cameron, Explainer: What you need to know about data clean rooms, *CMO Australia,* 7 February 2023, accessed 15 March 2024, p 1.

284 N Cameron, Explainer: What you need to know about data clean rooms, *CMO Australia,* 7 February 2023, accessed 15 March 2024, p 2.

285 See, for example, Amazon Web Services, AWS Clean Rooms, accessed 15 March 2024.

286 LiveRamp, Data Clean Rooms: A Complete Guide, 20 April 2022, accessed 15 March 2024; Habu, Data Clean Room Platform, accessed 15 March 2024; LiveRamp, Safe Haven, accessed 15 March 2024; Snowflake, Data Clean Rooms, accessed 15 March 2024.

287 J Duball, Data clean rooms: An adtech privacy solution?, *International Association of Privacy Professionals*, 24 January 2023, accessed 15 March 2024. For examples of data clean rooms offered by digital platforms, see Google, Ads Data Hub, accessed 15 March 2024; Amazon, AWS Clean Rooms, accessed 15 March 2024. Meta Business Suite is also sometimes described as a data clean room by others – see N Cameron, Explainer: What you need to know about data clean rooms, *CMO Australia,* 7 February 2023, accessed 15 March 2024. See also Disney, Disney's Proprietary Clean Room Data Solution Sets Its Sights on Measurement & Activation, 2 March 2022, accessed 15 March 2024.

288 IAB Tech Lab, Data Clean Rooms: Guidance and Recommended Practices, 5 July 2023, p 9.

289 S Kerner, Definition: Data Clean Room, *TechTarget*, accessed 15 March 2024.

290 IAB Tech Lab, Data Clean Rooms: Guidance and Recommended Practices, 5 July 2023, p 25.

291 N Gaekwad and A Soares, Secure and privacy-centric sharing with data clean rooms in BigQuery, *Google Cloud Blog*, 30 March 2023, accessed 15 March 2024.

292 Habu, Benefits of data clean rooms in a cookieless future, 27 February 2023, accessed 15 March 2024. See section 1.3.1 of this Report for a discussion of the deprecation of third-party cookies due to changes in the practices of digital platforms.

Issues related to the re-identification of previously de-identified data are discussed in chapter 5.

It is possible that even businesses participating in data clean rooms may not be aware of the data privacy risks that may be associated with them.[293] Most Australian consumers are also unlikely to be aware their data (or other data derived from it) may be shared between parties via a data clean room. Issues relating to consumer awareness and consent are discussed further in chapter 5.

Considerations relating to data sharing and competition in relation to data clean rooms are discussed in chapter 6.

3.2.2. Profiling

Profiling involves combining and analysing data collected about an individual to create a profile of that individual.[294] Profiles may be created or enhanced using some of the services described above.

The data used may include demographic data, such as the individual's age, gender and income, as well as location data and on- and offline purchasing behaviour data. The resulting profile provides detailed information about the individual. Consumer profiles can be updated in real-time,[295] and continuously refined based on updated data.[296]

To create a profile, data firms need to be able to identify the same customer in different datasets, which they do by matching the individual's unique 'identifiers' across datasets. Examples of unique identifiers include internet protocol (IP) addresses, cookie IDs, device IDs, advertising IDs and device fingerprints. These unique identifiers may be present even in purportedly 'de-identified' or 'anonymised' datasets.[297] Issues related to re-identification of previously de-identified data are discussed in chapter 5.

3.2.3. Segmentation

What is segmentation?

Segmentation is the process of grouping together certain individuals within an audience or customer database based on common characteristics.[298]

Audience segments are developed by grouping or categorising individuals based on shared characteristics. There are many potential types of segments, such as those based on:

- **Interests and behaviours** — for example automotive (people who like 'luxury vehicles'), retail ('highflyers' who enjoy fine dining), or entertainment (people who enjoy watching a certain film genre).[299]

293 Ad Exchanger, Fun fact about clean rooms: Data security isn't a given, 22 February 2023, accessed 15 March 2024.
294 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 39. 'In order to provide personalised advertising, ad tech providers will often need to link together the data they have collected over time about a consumer from a range of sources, and combine it to create profiles of consumers (these profiles often do not actually identify a consumer, but use a range of anonymised identifiers associated with a consumer).' See also Experian, How to build a customer profile for effective marketing, *Experian Marketing Insights*, March 2023, accessed 15 March 2024.
295 Oracle, Oracle Unity Customer Data Platform, accessed 15 March 2024.
296 12FasterCapital, Refine Customer Profiles, accessed 15 March 2024.
297 For example, Salinger Privacy submits that 'pseudonyms such as…identifiers…exist to enable links to be drawn between unrelated datasets…'. See Salinger Privacy, Submission to the Report, 28 September 2023, p 11.
298 See, for example, Experian, Submission to the Report, 28 September 2023, p 9; MailChimp, Glossary | Audience Segmentation, accessed 15 March 2024.
299 Oracle, Oracle Audiences | Advertising Products, accessed 15 March 2024. Examples created by the ACCC.

- **Demographics** – such as households with young children or retired couples.[300]
- **Seasonal events** – such as summer travel preferences (those likely to purchase a budget holiday package) or behaviour related to Mother's Day (individuals who have previously purchased or searched for gifts for this day).[301]

Segments can also be further divided based on more granular differences between sub-groups, or combined to create narrower custom segments made up of individuals who share multiple characteristics (for example, single people who own dogs and like watching Netflix).[302]

How are segmentation services developed?

Segmentation services are developed by processing and analysing a range of personal and other information on persons, including:

- demographic data (including age, gender, religion, income level, ethnicity, size of household, education and marital status)
- location data (including postcode, city, state, time zone and language)
- psychographic data (including interests, personality, lifestyle and values)
- behavioural data (including purchasing behaviour, search history, benefits sought and customer loyalty data).[303]

This data is analysed to determine audience segments or groups that have a high probability of sharing similar interests.[304] This may take into account factors such as their past engagement with a brand or likelihood of purchasing particular types of products.[305]

Why are segmentation services used?

Segmentation enables businesses to better understand their audiences. It enables marketing and advertising to be designed and targeted to those individuals most likely to be receptive to particular messages or advertisements.[306]

Business customers of data firms can also use segments to identify trends or preferences among their customers by analysing the behavioural and transaction data collected from certain segments. This analysis can be used to predict the likelihood that others in the segment may also engage in that behaviour. For example, an outdoor supplies retailer using

---

300 See, for example, Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, pp 4–6, 9–10, accessed 15 March 2024.

301 Oracle, Oracle Audiences | Advertising Products, accessed 15 March 2024. Examples created by the ACCC.

302 See, for example, Experian, Custom Segmentation | Experian Marketing Services, accessed 15 March 2024; Oracle, Contextual Intelligence | Advertising Products, accessed 15 March 2024. See also smrtr, Custom Projects, accessed 15 March 2024.

303 Mailchimp, What are Segmentation Variables in Marketing?, 13 February 2023, accessed 15 March 2024. See also Equifax, Audience Enhancement: Variables | Marketing Portal by Equifax, accessed 15 March 2024; ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019, p 47.

304 For example, through lookalike modelling, using taxonomy permission tools for second-party data sharing, or audience discovery reports that highlight categories that are highly correlated to a defined audience. See Lotame, Back to Basics: What is Lookalike Modeling?, 7 December 2023, accessed 15 March 2024; Oracle, Using Taxonomy Permissions to Share Your Data, accessed 15 March 2024; Oracle, Audience Discovery Report, accessed 15 March 2024.

305 Oracle, Customer Data Platform, accessed 15 March 2024. See also Experian, Experian Predict, accessed 15 March 2024. This service includes predictive models about customers in areas relating to Churn (attrition), Pricing (determining optimal price point for an offering), Risk (identifies customers likely unable to repay), Next Best Action (cross-sell opportunities), Lead Scoring/Acquisition (prospective customers) and Store Intelligence (predicting where a new store should be opened or the impact of closing an existing store).

306 In its submission, Experian notes a purpose of segmentation: 'to help our clients define segments for digital marketing, where brands are looking to place relevant advertising and marketing communications with publishers who sell advertising space online.' See Experian, Submission to the Report, 28 September 2023, p 9.

a segmentation service may observe that many of the individuals in its 'over 50s' segment are purchasing caravans, and so may experiment with marketing caravans to individuals in the segment who have not yet purchased a caravan.

Segmentation is also used to identify potential customers, in that a business may notice some of its customers share a common trait (such as owning a pet), and then target advertising to pet owners who are not current customers.

Segmentation services can also be used for 'audience suppression' or to create 'exclusion audiences', which excludes certain groups of consumers from marketing or advertising campaigns.[307] Business customers may use this function to remove individuals who are already customers.[308] They may also be used to comply with codes and statutory obligations, for example by excluding consumers who may be considered vulnerable, such as children, from a product that may be considered inappropriate.[309]

3.2.4. Targeted advertising

Targeted advertising is a method of advertising that uses consumer data to infer or predict which consumers are more likely to engage with an advertisement, and then displays ads to those consumers. It is designed to increase the effectiveness of advertising.

Targeted advertising can be personalised (targeted to individual consumers based on inferences about their personal attributes, also known as behavioural advertising), or contextual (targeted based on the context – where, when or how – in which an ad is displayed, relying less on individual consumer data).[310] Our focus in this Report is personalised targeting, because it relies heavily on the use of personal and other information on persons.

Personalised targeted advertising services are reliant on the processing and analysis of personal and other information on persons. This includes consumer data that is used for segmentation (as set out in section 3.2.3), such as demographic, location, psychographic and behavioural data.

This data is used to predict an individual's preferences, interests or potential interests, so that publishers and advertisers can display advertisements that are likely to be of interest and therefore more effective at encouraging the desired behaviour, such as buying a product or subscribing to a service.[311]

Personalised advertisements can be targeted based on the consumer's individual profile, or more typically, based on the individual having been grouped into an audience segment.[312] For example, an individual who has been categorised into an 'affluent singles' segment may be shown advertisements for a paid dating app.

More precise targeting allows advertisers to potentially earn higher returns on their advertising investment, and ad publishers to earn more revenue from their ad inventory.[313]

---

307 See, for example, LiveRamp, First-Party Data: What It Is, How to Use It, and Why It Matters Now More Than Ever, 12 October 2022, accessed 15 March 2024. See also, Customer Data Platform Institute, 6 Audience Suppression Tactics to Reduce Ad Spend and Increase ROI, 19 April 2021, accessed 15 March 2024.

308 See, for example, LiveRamp, First-Party Data: What It Is, How to Use It, and Why It Matters Now More Than Ever, 12 October 2022, accessed 15 March 2024.

309 For example, see The Australian Association of National Advertisers, Children's Advertising Code, accessed 15 March 2024.

310 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 37.

311 AIContentfy, The role of targeted advertising in customer acquisition, 15 February 2024, accessed 15 March 2024.

312 Bannerflow, A guide to audience targeting for personalised advertising, accessed 15 March 2024.

313 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 37.

Potential consumer issues relating to segmentation and personalised targeting of vulnerable consumers are discussed in section 5.2.2.

3.2.5. Measurement and optimisation

Measurement and optimisation services provide business customers with information about the performance and effectiveness of specific advertising or marketing campaigns.[314]

Measurement services involve measuring and analysing how the campaign reaches and impacts audiences.[315] This can include feedback to advertisers to verify whether their advertising has been targeted effectively. Based on the feedback received from measurement, optimisation involves tweaking or adjusting the approach to marketing and advertising for current or future campaigns. Measurement and optimisation can be performed throughout a marketing campaign.[316]

Measurement and optimisation services are developed by processing and analysing a range of data, including:

- demographic data[317]
- location data[318]
- data on media consumption or engagement[319]
- online behavioural data reflecting what content has been viewed (such as the ad campaign that was viewed) and where the content was viewed (such as through a website or app).[320]

This data may be collected and matched using identifiers such as IP addresses, mobile advertising identifiers, and cookie IDs.[321]

Metrics for measurement and optimisation include verification (whether an ad is shown in the way it was intended, such as on appropriate websites), validity (whether an ad is viewed by a real person), viewability (how long an ad is viewed) and completion quality (whether customers view entire ads).[322] Metrics also indicate how audiences engage with ads across channels and devices.[323]

3.3. Risk management products and services

Risk management products and services include those designed for identity verification, verification of other metrics (such as income) and fraud detection. While credit reporting services are a key type of risk management product, these services are not addressed in this Report.[324]

---

314 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 147. See, for example, IAB Australia, Submission to the Report, 28 September 2023, p 7.
315 See, for example, Nielsen, Audience Measurement | Digital Ad Ratings, accessed 15 March 2024.
316 Marketing Evolution, A Guide to Measuring and Analysing Your Campaign Performance, accessed 15 March 2024.
317 Nielsen, Submission to the Report, 28 September 2023, p 1.
318 B Brookes, What is Location Data and Why is it Important for Marketers?, 5 October 2022, accessed 15 March 2024.
319 Nielsen, Solutions | Audience measurement, accessed 15 March 2024.
320 Nielsen, Digital measurement privacy statement, September 2023, accessed 15 March 2024; Nielsen, Our Privacy Principles | C. The data Nielsen collects, May 2023, accessed 15 March 2024.
321 Nielsen, Privacy Statement, September 2023, accessed 15 March 2024.
322 See Oracle, Customers | Spotify rocks advertisers with measurement by Oracle, 7 January 2022, accessed 15 March 2024; Oracle, Advertising Products | Viewability and Attention, accessed 15 March 2024.
323 See Oracle, Customers | Spotify rocks advertisers with measurement by Oracle, 7 January 2022, accessed 15 March 2024; Oracle, Advertising Products | Viewability and Attention, accessed 15 March 2024.
324 See discussion in section 1.1.1.

Risk management products and services often involve matching data which cannot be independently verified by the requesting party with additional data available to the data firm offering these services. Automated decision-making is often used in the provision of these services. This involves the use of algorithms or artificial intelligence (AI) to analyse relevant data and action final decisions.[325]

These services can sometimes be provided on a standalone basis or as a packaged service accessed through a single channel or platform.[326]

These services typically draw on a range of datasets. The specific data that is used will depend on the type and nature of the risk management service. Data types that may be used to match or verify the information provided by a requesting party include:

- **Personal and other information on persons** – such as name, address, consumer demographics, bankruptcy status and participation in court actions
- **Commercial data** – such as business registration documents, professional and trade licences, company financial reports, credit applications, court actions, defaults and financial information.
- **Fraud and identity verification data** – such as fraud incident data, and data confirming an individual's identity such as biometrics or document-based verification.

This data may come from a range of sources, including government data and databases,[327] shared fraud databases,[328] and proprietary data sources.[329]

Business customers of data firms may choose to use such services if they do not have the resources, including access to the data, expertise, and technology to manage the verification processes themselves, or if they find it more efficient to outsource such functions.

3.3.1. Verification services

Verification services help to confirm an individual's identity, or other information they have provided.[330] For example, an employer may use verification services to screen candidates based on whether they are an Australian citizen or have a criminal record, while a bank may use customer identification and verification services to comply with its obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).[331]

Verification processes may involve:

- **Records matching** – where the identity of the customer or information they have provided is verified against other databases, such as the Australian Government's Document Verification Service (DVS) which allows for matching key document data with

325 S O'Regan, Designing Data Products, *Medium: Towards Data Science*, 17 August 2018, accessed 15 March 2024.
326 For instance, customers can access various fraud and risk services through Equifax IDMatrix. See Equifax, IDMatrix, accessed 15 March 2024.
327 Some examples of government data and databases are death data from the Australian Death Check service, residency status data from the Department of Home Affairs Visa Entitlement Verification Online service, and the Australian Government's Document Verification Service (DVS). See Australian Death Check, accessed 15 March 2024; Equifax, Australian Death Check, accessed 15 March 2024; Department of Home Affairs, Check visa details and conditions, accessed 15 March 2024; Equifax, Visa checks via VEVO, accessed 15 March 2024.
328 See, for example, Equifax, Fraud Lookup | IDMatrix, accessed 15 March 2024; Equifax, Fraudcheck | Business Enterprise Products, accessed 15 March 2024.
329 Such as Equifax's Tenancy Database and Consumer Credit Bureau. See Equifax, Multiple Verification Sources | IDMatrix, accessed 15 March 2024.
330 See, for example, illion, GreenID, accessed 15 March 2024; Equifax, Identity Verification | IDMatrix, accessed 15 March 2024.
331 See, for example, Equifax, Employee Screening | Business Enterprise Solutions, accessed 15 March 2024; AUSTRAC, Customer Identification and Verification, accessed 15 March 2024.

government records.[332] The information may relate to property, finances, education, employment, or residency status.[333]

- **Biometric data matching** – which may involve a form of identification, such as a driver's licence, being uploaded, assessed for 'liveness' (i.e. the likelihood it was not AI-generated), matched with a current, authentic photo of the individual, and verified against other data sources, such as the DVS.[334]
- **Multifactor authentication** – which confirms the identity of the customer by generating a one-time use unique code sent to their phone ('multifactor authentication'), or through knowledge-based authentication which requires the customer to provide specific information, such as answers to a series of questions only they are likely to know.[335]
- **Insurance assessment** – which verify applicants' or policyholders' applications against their claim history, assist insurers to validate data and assess risk, identify fraudulent claims, and streamline investigative processes.[336]
- **Employment data matching** – employment income and payroll information can be used as a form of identity and information verification, providing access to an individual's income records to verify their employment income.[337] When the individual applies for a loan, lease or credit card, the business using the data matching service receives an employment or income report, which is based on data the individual's employer has provided.[338]

Data-driven human resources services are a category of data services that involve verification functions. These services are discussed in box 3.3, along with further discussion of employment data matching.

Box 3.3 Data-driven human resources services

Data-driven human resources services assist employers in managing employees and employment processes. These include recruitment, onboarding, payroll, performance management and 'offboarding' (i.e. employee separation) processes.

Data-driven human resources services include verification platforms that enable employers to conduct background checks and verify a prospective employee's identity and other information.

These services use data from a range of sources, such as government data and databases,[339] and shared fraud databases.[340] This data may include personal

[332] Organisations must be approved as a 'gateway service provider' in order to have a direct connection to the DVS. See Australian Government, idmatch.gov.au and Gateway Service Provider, accessed 15 March 2024. See also Equifax, Document Verification Service (DVS) | IDMatrix, accessed 15 March 2024.

[333] For instance, Equifax Identity Verification and IDMatrix is an identity verification service that works by matching the information provided by the customer against various data source. See Equifax, Identity Verification | IDMatrix, accessed 15 March 2024.

[334] See, for example, Equifax, Equifax Biometrics | Business & Enterprise Solutions, accessed 15 March 2024; illion, GreenID, accessed 15 March 2024. See chapter 4 for further discussion.

[335] For instance, Experian offers multifactor authentication products, including Knowledge IQ (knowledge-based authentication) and One-time passcode (multifactor authentication). Experian, Multifactor Authentication Solutions | Experian Identity Solutions, accessed 15 March 2024.

[336] See, for example, illion, Insurance | Commercial Risk Solutions, accessed 15 March 2024.

[337] See, for example, Equifax, Verification Exchange for Verifiers, accessed 15 March 2024.

[338] Equifax, Human Resource Solutions, accessed 15 March 2024.

[339] Some examples of government data and databases are residency status data from the Department of Home Affairs' Visa Entitlement Verification Online (VEVO) service, and the Australian Government's Document Verification Service (DVS). See Equifax, Customer Visa Checks | IDMatrix, accessed 15 March 2024; Department of Home Affairs, Check visa details and conditions, accessed 15 March 2024.

[340] See, for example, Equifax, Fraud Lookup | IDMatrix, accessed 15 March 2024; Equifax, Fraudcheck | Business & Enterprise Products, accessed 15 March 2024.

information (such as name, address, and contact information), education and employment history, bankruptcy status, court appearances and medical history.[341]

Firms supplying identity verification services may seek to become accredited service providers under the Australian Government's Digital ID program. This accreditation allows these firms to demonstrate their suitability to provide digital ID services to government and private sector – services that enable individuals to verify their identities online. Digital ID is described in more detail in box 3.4.

Box 3.4 Digital ID services

A digital ID provider allows users to create a Digital ID by verifying existing ID documents with the issuing body (such as the relevant state or territory for a driver's licence) or checking features of the document to confirm that the document is authentic and belongs to that user.[342] A user will only need to share their document once, and in subsequent uses will only need to provide their name, email address and date of birth to the provider.[343]

Since 2018, the Australian Government has been piloting an accreditation program for digital ID providers. Digital ID providers can voluntarily apply to be accredited under the Trusted Digital Identity Framework.[344] The pilot program has tested the Framework and provided feedback that allows it to be expanded to a legislative scheme.[345] The current accreditation framework ensures all digital ID providers meet strict rules and standards for usability, accessibility, privacy protection, security, risk management, and fraud control.[346]

The Government intends for the Trusted Digital Identity Framework to shortly be replaced by Digital ID legislation and related rules which will provide the foundation for creating a voluntary, secure, convenient and inclusive way for individuals to verify their identity online.[347] The legislation will establish an economy-wide accreditation scheme which will set a benchmark for privacy and information security for entities involved in digital identity services, and an independent regulator to provide accreditation and to ensure accredited entities are complying with their obligations.

The Digital ID Bill builds on the existing framework, by, among other things, enabling the Australian Government Digital ID System to be used by private sector organisations in the future (subject to phasing and approval by the Digital ID Regulator).[348]

The Bill, if passed, will require accredited Digital ID service providers to comply with specified privacy, cyber security and fraud control requirements, with penalties applying for non-compliance.[349] Once an entity becomes an accredited provider, it will be able to choose to join the Australian Government Digital ID system and/or hold out that it has

341 See, for example, Equifax, fit2work Privacy Collection Statement, 11 April 2023, accessed 15 March 2024; Equifax, eCredential | HR Solutions, accessed 15 March 2024; Oracle, Human Capital Management, accessed 15 March 2024.
342 Australian Government, How Digital ID works, accessed 15 March 2024.
343 Australian Government, How Digital ID works, accessed 15 March 2024.
344 Australian Government, Trusted Digital Identity Framework, accessed 15 March 2024.
345 Australian Government, Trusted Digital Identity Framework, accessed 15 March 2024.
346 Australian Government, Trusted Digital Identity Framework, accessed 15 March 2024.
347 See Australian Government, Digital ID Bill, accessed 15 March 2024; Digital ID Rules 2024, accessed 15 March 2024.
348 Australian Government, Digital ID Legislation, accessed 15 March 2024. The ACCC will be the interim Digital ID regulator responsible for accrediting Digital ID services, approving which services can participate in the Digital ID System, and ensuring that Digital ID providers comply with the requirements.
349 See Australian Government, Digital ID Bill, accessed 15 March 2024.

met the accreditation requirements when providing its services outside of this system.[350]

3.3.2. Fraud detection and prevention services

Fraud detection and prevention services ('fraud services') are designed to detect fraudulent activity and to assess and reduce the risk of fraud occurring, such as by identifying and mitigating specific risks.[351] There is some overlap between verification services and fraud services, as verification services also determine if information provided is correct or authentic.

Fraud services include:

- **Fraud screening assessments** – which enable users of the service to verify the information provided by an individual (such as name, phone number, email or physical address, passport, or visa details), and assess the likelihood the individual is linked to fraud by comparing the information to other data, such as databases of proven fraudulent activity and data points and email address metadata.[352]
- Other fraud screening services use artificial intelligence technologies that crosscheck data provided by the customer with consumer identity data drawn from proprietary or shared databases (such as device IDs, purchasing behaviours, phone numbers and IP addresses).[353] These technologies then check for data that indicates a connection to previously detected fraud (such as device location, multiple credit cards associated with the same device, and numerous requests coming from the same IP address).[354] A risk score can then be assigned to an individual when they interact with a firm, such as when making a payment or creating an account.
- **Device intelligence services** – which profile 'device attributes' to recognise returning customers and identify potential fraudulent transactions or activity,[355] such as by detecting the use of a stolen device, or a device used in known fraudulent activities.[356]
- **Identity monitoring services** – which alert customers if their personal information is found on the dark web (such as in forums where stolen information is illegally traded).[357]

3.4. Property data and analytics services

Property data and analytics services are designed to assist with property-related decisions. They are used by real estate agents, landlords, buyers, sellers and renters to research, buy,

350 Australian Government, Digital ID Bill, accessed 15 March 2024.
351 For a more detailed definition and discussion of fraud, see Attorney General's Department Commonwealth Fraud Prevention Centre, Explore the Fraud Problem, accessed 15 March 2024.
352 Equifax supplies at least 4 fraud screening assessment services in Australia: Kount, FraudCheck, Phone Number Validation (through IDMatrix) and Email Risk Search (through IDMatrix). See Equifax, Kount in Australia | Business & Enterprise Products, FraudCheck | Business & Enterprise Products, Phone Number Validation | IDMatrix and Email Risk Search | IDMatrix, accessed 15 March 2024. Some of these data validation services, such as phone number and email validation, which ensure contact details are real and active, may also be used for marketing purposes.
353 For instance, Equifax Kount fraud-screening service uses data from its Identity Trust Global Network, through which hundreds of global companies share data they have collected. See Payment Consulting Network, Q&A with Adam Gunther and Brad Wiskirchen (of the Digital Solutions team) at Equifax, accessed 15 March 2024.
354 See Equifax, Kount in Australia | Business & Enterprise Products, accessed 15 March 2024.
355 For an example of a device intelligence service, see Equifax, Device Intelligence, *IDMatrix*, accessed 15 March 2024.
356 Such services can also be used as verification services. For instance, device intelligence is commonly used for online payments, creating new accounts and logins, and applications.
357 See Equifax, Equifax Identity Protect, accessed 15 March 2024.

sell, rent and manage properties. Collectively, these services are sometimes described as 'PropTech'. Some provide information on a specific property,[358] while others provide market-level information.[359]

Property data and analytics services are usually based on detailed residential, developer and/or commercial property datasets. The types of data used include specifics about a property, such as address, floorplan, number of rooms, sale price, and ownership details.[360]

Property services also use more general data such as the number of clicks on an online listing and neighbourhood demographic information.[361] The data may also relate to property market trends and conditions (e.g. local market values and capital growth), property histories, valuations, and expected sales or rental performance.

State and territory land titles offices are a key source of detailed property data.[362] This data may be supplemented with data made available by the Australian Bureau of Statistics (such as postcode-level demographic information), data collected from real estate companies and financial institutions, and data collected from real estate listings sites (discussed in box 3.5).

Property products and services can be accessed in various ways, such as through property reports, application programming interfaces (API), data extract files and customisable property datasets.[363]

A business customer's specific needs will dictate the format in which they choose to access the product or service. For instance, property reports provide derived data and insights on a specific property, often in an interactive form, to help business customers to present the information to their own customers in a simplified and engaging format.[364] The derived data in property reports can also be fed through APIs. An API enables clients to instantly access real-time data for use in their own apps, or websites.[365]

Alternatively, data extract files may be used, which are pre-generated files containing a fixed set of raw property data (such as market trends or housing statistics across a geographical region[366]). These are intended for clients who wish to perform specific analysis tasks.[367]

While the data from a data extract file may not be as current as data available through APIs, more data can be accessed at a given time.[368]

Another common way to access property data is through real estate listing websites. These also serve the broader role of providing certain property data and analytics services, as described in box 3.5.

---

358 For example, CoreLogic offers reports for both buyers and sellers which provide a 'comprehensive view' of a single property, including current estimated value, suburb insights (such as number of sales, median value and gross rental yield), property sales listings, rental history and development permit applications, to help them understand an individual property. See CoreLogic, Property Report | News & Research, accessed 15 March 2024.

359 See, for example, CoreLogic, Market Trends, accessed 15 March 2024.

360 See, for example, PropTrack, Property Data and Insights, accessed 15 March 2024; PropTrack, Submission to the Report, 28 September 2023, p 6.

361 PropTrack, Submission to the Report, 28 September 2023, p 6.

362 PropTrack, Submission to the Report, 28 September 2023, pp 1, 6.

363 See, for example, CoreLogic, Market Trends | Our Data, accessed 15 March 2024; PropTrack, Products, accessed 15 March 2024.

364 See, for example, PropTrack, Digital Property Reports: cut through the market noise, accessed 15 March 2024.

365 See PropTrack, Property Data APIs | Property Data, accessed 15 March 2024. See also CoreLogic, CoreLogic APIs | Our Data, accessed 15 March 2024.

366 CoreLogic, Market Trends | Our Data, accessed 15 March 2024.

367 PropTrack, API vs Data Extracts, accessed 15 March 2024.

368 PropTrack, API vs Data Extracts, accessed 15 March 2024.

Box 3.5 Real estate listing websites

Real estate listing websites display residential property sale and rental listings. They also provide information on off-market properties and property market trends.

REA Group's realestate.com.au and CoreLogic's OnTheHouse.com.au are marketed as being among the most popular listing websites and property resources in Australia.[369] OnTheHouse and the Track Your Property (realEstimate) service on realestate.com.au both provide instant estimated property values, information on the property market such as market trends, recently sold and currently listed properties in the area, and loan comparisons.[370]

Real estate listing websites may receive data from a data firm, such as through an API, to retrieve and display market data from the data firm. For example, PropTrack's property API may be linked to a real estate listing website to provide rental and sale history, property attributes, valuation, listings history and transaction data.[371]

These websites can also be a valuable source of data in themselves for firms that supply property data. For example, listings created by real estate agencies provide data on supply and demand statistics in particular regions, which can be incorporated into other property products.[372]

3.4.1. Property data platforms

Property data platforms typically integrate a range of data sources and may be used to generate property reports or valuations.

Examples of property data platforms include CoreLogic's RP Data platform and the IQ Connect platform (a partnership between Equifax and CoreLogic).[373] These platforms enable business customers to research properties (through property attributes, imagery and market trends), order valuations, automate valuation requests (using automated valuation models), and track changes in value.

Property reports typically focus on a specific property and provide details such as current estimated value, suburb insights (number of sales, median value and gross rental yield), property sales listings, rental history and development permit applications.[374] These may be supplied in static (e.g. PDF) or interactive formats via a platform.

---

369 REA Group's realestate.com.au claims to be 'the leading property resource in Australia', with an average of 12 million visitors per month. See Nielsen Digital Media Ratings (Monthly Tagged), Jul-2021 to Jun-2022 (average), P2+, Digital (C/M), text, realestate.com.au, Average Monthly Unique Audience, cited on realestate.com.au, About us, accessed 15 March 2024. This is a primary source of property data for PropTrack (also owned by REA Group). CoreLogic's OnTheHouse.com.au listings website portal is a research tool for consumers and real estate agents, which leverages CoreLogic's data ecosystem, that according to the website covers 'approx[imately] 98% of Australia's property market' and 'attracts 2.6 million visits each month'. See CoreLogic, OnTheHouse Residential Real Estate | Software & Solutions, accessed 15 March 2024.

370 See realestate.com.au, realEstimate, accessed 15 March 2024; CoreLogic, OnTheHouse for Residential Real Estate, accessed 15 March 2024.

371 See PropTrack, Property Data APIs | Property Data and Insights, accessed 15 March 2024; PropTrack, PropTrack Market API Brochure, accessed 15 March 2024; PropTrack, Automated Valuation Models (AVMs), accessed 15 March 2024.

372 See PropTrack, Property Data APIs | Property Data, accessed 15 March 2024; PropTrack, PropTrack Market API Brochure, accessed 15 March 2024.

373 See CoreLogic, RP Data | Software & Solutions, accessed 15 March 2024; Equifax, Property Valuation | Business Enterprise Products, accessed 15 March 2024.

374 See, for example, CoreLogic, Property Report | News & Research, accessed 15 March 2024.

Valuation products help brokers, lenders and other property professionals determine the value of a property. The Australian Property Institute describes accurate property valuation, facilitated by property services, as 'an essential element of a healthy housing market'.[375]

Automated Valuation Models (AVM) provide an automated statistical calculation of the value of a property, using machine learning to perform this function by analysing data such as property details (size, number of rooms), area demographics (presence of local schools, supermarkets, public transit and so on), property transaction history and market trends and activity (e.g. sales price of similar properties).[376] AVMs can be used for rental valuations as well as sales.[377] Platforms that provide property valuations can remove the need for properties to be physically inspected, potentially saving valuers and lenders time and money.[378]

These valuation products are marketed to lenders or mortgage brokers (e.g. for determining risk in lending against a property), insurers (e.g. for determining the appropriate level of cover) and government (e.g. to determine charges, such as council rates and land tax).[379] Consumers may also use AVM functions to receive an indication of a property's value.[380]

3.4.2. RentTech platforms

RentTech platforms are online platforms used by real estate agents, landlords and tenants to manage the rental application process and ongoing rental needs, such as paying rent. Their use has grown rapidly in recent years, and they are now widely used across Australia.[381] RentTech platforms concentrate the tenancy application process to a single self-service platform, and are used to streamline identification and income validation processes. These platforms include functions used for searching and applying for a rental property, making rent payments, reporting maintenance issues, and requesting repairs.[382]

A common source of data for some RentTech platforms are tenancy databases, which collect and store data about tenants' rental history.[383] For instance, Equifax's National Tenancy Database is marketed as providing Australia's most comprehensive tenancy screening service, using data such as bankruptcy data, court records, and data relating to an applicant's commercial history from the Australian Securities and Investments Commission (ASIC) and Equifax's commercial credit bureau.[384] Real estate agents and other property professionals can use this database to validate applicants' identities and conduct background checks.[385]

Consumer issues associated with the use of RentTech platforms are discussed further in box 5.2.

---

375 Australian Property Institute, Submission to the Report, 28 September 2023, p 1.

376 N Kok, Everything You Need To Know About Automated Valuation Models In Real Estate, *Forbes*, 2 March 2020, accessed 15 March 2024. See also A Valier, Who performs better? AVMs vs hedonic models, *Journal of Property Investment & Finance*, 38(3), 2020, pp 213–225.

377 See PropTrack, Submission to the Report, 28 September 2023, p 2. See also REA's property research website property.com.au, accessed 15 March 2024.

378 See CoreLogic, Data-powered-digital-solution-a-game-changer for faster property valuations, *News & Research,* 8 June 2023, accessed 15 March 2024.

379 PropTrack, Submission to the Report, 28 September 2023, pp 3–5.

380 PropTrack, Submission to the Report, 28 September 2023, p 2. See realestate.com.au, realEstimate, accessed 15 March 2024.

381 A Kollmorgen and K Bower, RentTech platforms making renting that much harder, *CHOICE*, 18 April 2023, accessed 15 March 2024.

382 CHOICE, At what cost? The price renters pay to use RentTech, April 2023, p 7.

383 See, for example, Equifax, National Tenancy Database, accessed 15 March 2024. RentTech platforms that use this database include, among others, RentBetter's Tenant Check, and InspectRealEstate's 2Apply, accessed 15 March 2024.

384 Equifax, National Tenancy Database, accessed 15 March 2024.

385 Equifax, National Tenancy Database, accessed 15 March 2024; Equifax, Case Study: A tech and data partnership is getting quality tenancy into rental properties up to 50% faster, 1 November 2021, accessed 15 March 2024.

3.4.3. Construction and commercial property products

Data products and services for the construction industry include platforms that provide data on construction products, and online models or calculators.[386]

Online construction product calculators provide customers with an estimate of building replacement costs, to help them select an appropriate level of insurance cover based on their property's insured value.[387]

Construction management platforms enable business customers to view and track planned, ongoing and past construction projects, and to view related details such as the companies and contacts (e.g. architects, builders and developers) associated with specific projects.[388] A construction company may use this data to, for example, discover new development or building opportunities, or a property developer may use it to connect with a construction company.[389]

The data may also be drawn from commercial property databases covering office, retail and industrial properties, which business customers may use to identify investment opportunities, or to promote their services to commercial property owners, tenants, and property managers.[390]

Property data and analytics services can also be valuable to other business customers. For example, Equifax supplies a land titles search service which enables business customers, including lenders, insolvency firms and financial planners, to verify and assess ownership data on Australian properties by searching land titles registries to confirm the existence of any deeds, caveats, or easements.[391] This information can be used for processing mortgage applications, investigating ownership, and assessing credit.[392]

386 See, for example, CoreLogic, Cordell Connect and Cordell Sum Sure, accessed 15 March 2024.
387 See, for example, CoreLogic, Cordell Sum Sure, accessed 15 March 2024.
388 CoreLogic, Cordell Connect, accessed 15 March 2024.
389 CoreLogic, Cordell Connect for Trades and Services, accessed 15 March 2024.
390 See CoreLogic, CityScope | Software & Solutions, accessed 15 March 2024. CoreLogic states that CityScope contains data on over 27,000 owners and 85,000 tenants.
391 Equifax, Land Titles | Business & Enterprise Products, accessed 15 March 2024.
392 Equifax, Land Titles: Features and Benefits | Business & Enterprise Products, accessed 15 March 2024.

4. Supply of data products and services in Australia

Key observations

- This chapter describes the data products and services supplied by an illustrative sample of data firms operating in Australia.
- The supply of data products and services in Australia is a dynamic and evolving industry. Analysis of the firms described in this chapter demonstrates an industry trend of evolving or expanding beyond offering data marketplace services and customer lists, and towards providing sophisticated, and often proprietary, data analytics services and data management platforms.
- Almost every industry in Australia uses data products and services from data firms.
- Data products and services are provided to business customers and other data firms on varying terms, including through pay-per-use, subscription and licensing models and monetary reciprocal supply agreements.

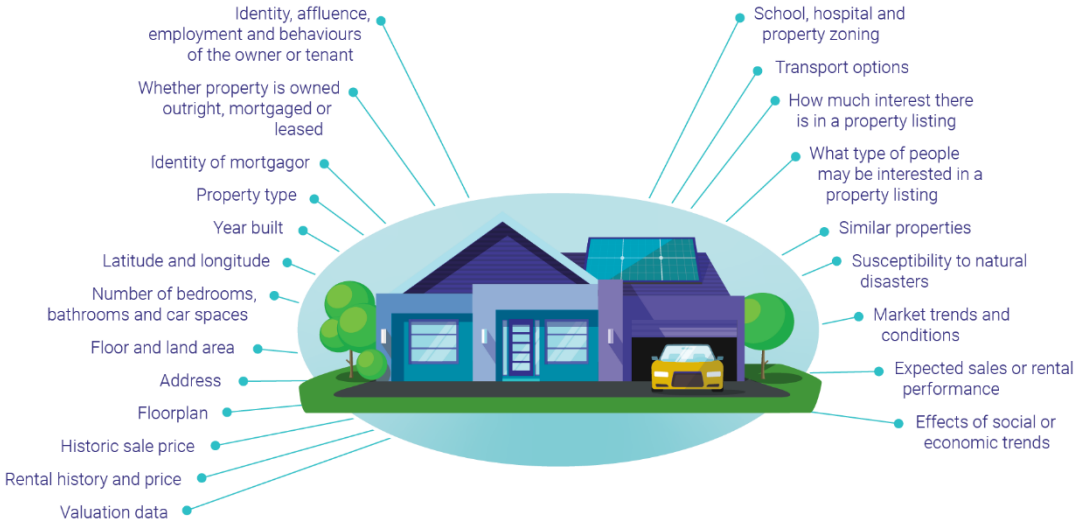
This chapter provides a snapshot of the business models of firms that supply the data products and services set out in chapter 3. The data firms described in this chapter do not represent an exhaustive list or description of all suppliers of data products and services in Australia.

This chapter is structured as follows:

- **Section 4.1** describes how each of the 9 sample firms identified in the Issues Paper collect data and supply data products and services in Australia.
- **Section 4.2** provides a list of 15 additional data firms we have identified in our Inquiry as further examples of data firms that supply data products and services in Australia.
- **Section 4.3** sets out some of the main industries of business customers that acquire data products and services from data firms.
- **Section 4.4** explains some of the key terms of supply for data products and services.

In order to develop data products and services, data firms collect a range of data about individual consumers and properties. Figure 4.1 shows some examples of the depth and breadth of information that data firms hold on Australian consumers and properties.

Figure 4.1: Examples of data that data firms may hold on properties and consumers



4.1. How the sample firms collect data and supply data products and services

In the Issues Paper, the ACCC identified 9 firms that supply the types of data products and services that are the focus of the Report. This section of the Report describes, in relation to each of the 9 firms:

- how the firm collects data and from where
- what data products and services the firm supplies in Australia
- what types of business customers acquire data products or services from the firm.

For the purposes of this section, the 9 firms are categorised as:

- Credit reporting agencies (Equifax, illion and Experian), discussed in section 4.1.1

- Property data firms (CoreLogic and PropTrack), discussed in section 4.1.2
- Data analytics and other data firms that supply data products and services (Oracle, Quantium, LiveRamp and Nielsen), discussed in section 4.1.3.

Figure 4.2 provides a summary of which of the 9 sample firms provide each category of data product and service described in chapter 3.

Figure 4.2: Types of data products and services supplied by the 9 sample firms

4.1.1. Credit reporting agencies

As noted in section 1.1.1, credit reporting is outside the scope of this Report. However, the 3 major credit reporting agencies in Australia – Equifax, illion and Experian – are also suppliers of a diverse range of data products and services in Australia which are relevant to this Report.

Equifax

Equifax is a global data firm that operates in Australia. It collects and uses a wide range of consumer data, including:

- personal information (such as name, address, and date of birth)
- certain demographic information
- biometric information
- employment information
- sensitive information, including criminal and medical history (when consented to)

- property information.[393]

It collects this from sources ranging from federal and state government agencies, other data firms, direct from consumers and third-party suppliers.[394]

Equifax supplies a wide variety of data products and services in Australia, including:

- Data-driven marketing services, including its data management platform Marketing Portal.[395] Through this platform, business customers can validate, verify and enhance their customer data.[396] Equifax's data-driven marketing services are advertised as helping to:
  - deliver advertising campaigns, including through audience segmentation, based on value to the business customer, propensity to buy and media preferences[397]
  - measure and optimise the performance of these campaigns.[398]
- Risk management products, including several fraud detection products, such as Kount, Device Intelligence, FraudCheck, and Email Risk Search.[399] They also include identity verification products, such as Equifax Biometrics and Verification Exchange.[400] Some of Equifax's fraud and identity products can be accessed through its IDMatrix service.[401]
- Property services, such as a land titles search service which is designed for business customers in financial and property services, to verify and assess ownership of Australian properties using land titles, deeds, caveats and easements.[402] This information can be used for mortgage application processing, ownership investigations and for credit assessments.[403]
- The Human Resources platform, which provides recruitment, onboarding, performance management and offboarding services.[404]
- The 'fit2work' employment screening product line.[405]

Equifax supplies data products and services to a broad customer base, including Australian banks and other financial services entities and 'businesses seeking data solutions across their business landscape'.[406] According to Equifax, customers may use these data products and services to refine human resources processes, manage risk within commercial markets, verify identities, and manage matters pertaining to tenancy arrangements.[407]

393 See Equifax, Submission to the Report, 28 September 2023, pp 8–9.
394 See Equifax, Submission to the Report, 28 September 2023, pp 8–9.
395 See Equifax, About Us | Data-Driven Marketing, accessed 15 March 2024; Equifax, Marketing Portal | Data-Driven Marketing, accessed 15 March 2024; Equifax, Our Capabilities | Data-Driven Marketing, accessed 15 March 2024; and Equifax, Equifax Engage, accessed 15 March 2024.
396 Equifax, Data Management | Data-Driven Marketing, accessed 15 March 2024.
397 Equifax, Analysis and Segmentation | Data-Driven Marketing, accessed 15 March 2024; Equifax, Audience Enhancement: Variables | Marketing Portal by Equifax, accessed 15 March 2024; Equifax, Campaign and Channel Management | Data-Driven Marketing, accessed 15 March 2024.
398 Equifax, Marketing Effectiveness | Data-Driven Marketing, accessed 15 March 2024.
399 See Equifax, KOUNT Australia: A Leading Fraud Solution, accessed 15 March 2024; Equifax, Device Intelligence, accessed 15 March 2024; Equifax, FraudCheck, accessed 15 March 2024; Equifax, Email Risk Search, accessed 15 March 2024; Equifax, Phone Number Validation | IDMatrix, accessed 15 March 2024.
400 Equifax, Equifax Biometrics, accessed 15 March 2024; Equifax, Verification Exchange, accessed 15 March 2024.
401 Equifax, ID Matrix: Device Intelligence, accessed 15 March 2024; Equifax, Packages | IDMatrix, accessed 15 March 2024.
402 Equifax, Land Titles | Business & Enterprise Products, accessed 15 March 2024.
403 Equifax, Land Titles: Features & Benefits, accessed 15 March 2024.
404 Equifax, Human Resource Platform | HR Solutions, accessed 15 March 2024.
405 Equifax, Fraud and Identity | Business & Enterprise Solutions, accessed 15 March 2024; Equifax, fit2work, accessed 15 March 2024.
406 Equifax, Submission to the Report, 28 September 2023, p 2.
407 Equifax, Submission to the Report, 28 September 2023, p 2.

illion

illion, owned by the Australian company Credit Data Solutions, collects data on consumers and businesses from public and private data sources.[408] illion submits that it may obtain data direct from illion customers themselves, from data suppliers (or directly from a data source) or from proprietary-built sources.[409]

illion uses combined information from its commercial and consumer bureau databases and other databases to generate insights for use in some of its data products.[410]

For its consumer marketing services, illion says it collects personal information from unspecified 'first party data brokers'.[411] illion provides a consumer marketing product called 'Geo Attributes,' based on credit demand or geographic risk, which business customers can use to verify and/or segment consumer data. One attribute uses transaction data to provide consumer behavioural insights, while another uses Centrelink customer income data at an aggregate level.[412] Some of illion's risk management products rely on personal information (for example, its identity verification service GreenID compares an individual's name, address and date of birth against a range of government, public and proprietary data sources).[413]

illion says it supplies a range of data products and services in Australia, including:

- marketing and advertising services, such as:
  - commercial marketing products, including Company360, Hoovers and Prospector.[414] These services provide data on companies for illion's business customers to market their own services to other businesses.[415]
  - consumer marketing services, including providing analysis for marketing campaigns and targeted advertising.[416] illion says its Consumer Marketing product contains 5.6 million phone numbers and 11 million email addresses, and 'appends' more than 100 attributes on consumers.[417]
- risk management products and services, specifically credit risk products for commercial, consumer and anti-money laundering (AML) risk, as well as ID and income verification. illion says the GreenID product is an ID verification and AML product, which verifies a customer's name, address and date of birth against a range of data sources (including government, public and proprietary data sources).[418]

illion's data products and services may be used by businesses seeking to improve their marketing activities or better understand their supply chain.[419] illion's business customer

408 Illion, Submission to the Report, 28 September 2023, p 4.
409 illion, Submission to the Report, 28 September 2023, p 4.
410 'Value-added insights…are generated by illion using the combined information that is available in the commercial bureau service database and other illion databases to create 'Products' that deliver subsets of the data to clients to solve specific problems.' illion, Submission to the Report, 28 September 2023, p 4. On its website, illion indicates these databases may be used in various products. For instance, see illion, Unlock the power of geo attributes, accessed 15 March 2024; illion, Consumer Risk | Evaluation, accessed 15 March 2024.
411 illion, Submission to the Report, 28 September 2023, p 3.
412 illion, Unlock the Power of Geo Attributes, accessed 15 March 2024; illion, How illion data can help increase customer retention, accessed 15 March 2024.
413 Illion, Consumer Risk | ID, Fraud & AML, accessed 15 March 2024.
414 illion, Lead Portals | Marketing Solutions, accessed 15 March 2024.
415 illion, Company 360, accessed 15 March 2024.
416 illion Batch Solutions | Marketing Solutions, accessed 15 March 2024.
417 illion, Case studies: Consumer Marketing empowering customer reach for an Australian, tier one, utility company, accessed 15 March 2024.
418 illion, Submission to the Report, 28 September 2023, p 3; illion, Consumer Risk | ID, Fraud & AML, accessed 15 March 2024.
419 illion, Submission to the Report, 28 September 2023, p 3.

base includes banks and financial services, utility companies, telecommunications providers, government agencies,[420] and other commercial enterprises.[421]

Experian

Experian Australia, owned by Experian US, collects a range of personal and other information on persons that it processes and analyses to develop data products and services. In its submission, Experian notes that it collects data from sources such as the Australian Bureau of Statistics (ABS), other data firms, and self-reported data from consumers who voluntarily participate in surveys or studies. This data includes property information, geospatial points of interest data and what Experian calls 'consumer permissioned data'.[422] Experian claims its Australian data holdings include 'contact channels' of over 15 million email addresses, 8 million mobile numbers and 10 million residential addresses.[423]

Experian supplies a range of data products and services.[424] These include:

- risk management products and services, including identity verification and fraud detection products, and data validation services.[425] For example, Experian Hunter is an identity verification and fraud prevention product.[426] Experian Hunter aims to prevent application fraud, which can occur when fraudsters apply for a service such as utilities, telecommunications, a loan or a credit card.[427]
- data-driven marketing and advertising products and services (Experian Marketing Services):[428]
  - ConsumerView is a detailed database of Australian consumers, which contains household-level information, including data on income, assets, education, and other household members, which Experian says it holds on 100% of Australian households.[429] Business customers can use this product for data enrichment when conducting or planning marketing campaigns. ConsumerView provides information on over 18 million Australian consumers (73% of the adult population).[430]
  - A key offering of Experian Marketing Services is Mosaic, a segmentation system that classifies consumers by lifestyle into one of 14 overarching Groups and 51 Types.[431] Groups include 'Hardship and Perseverance', described as unemployed and blue-collar workers living in units and flats on low incomes, and 'First Class Life', described as the 'wealthiest group in Australia'.[432] Types within these groups include 'Central Prosperity', 'Successful Spending', 'Power Couples', 'Determined Suburbans', 'Spirit Questers', 'Selfless and Hardworking', 'Mature Modernites', and 'Farming Reliance'.[433] Business customers may use the service to enhance their marketing strategies and campaigns.[434]

---

420 See illion, Case Studies, accessed 15 March 2024; illion, Submission to the Report, 28 September 2023, p 2.
421 illion, Submission to the Report, 28 September 2023, p 2.
422 Experian, Submission to the Report, 28 September 2023, p 8.
423 Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, pp 1–3, accessed 15 March 2024.
424 Experian, Submission to the Report, 28 September 2023, p 3.
425 Experian, Fraud Management, accessed 15 March 2024; Experian, Identity Verification and Fraud Solutions, accessed 15 March 2024; Experian, Risk Management, accessed 15 March 2024.
426 Experian, Experian works with FMT Worldwide to further enhance Hunter fraud prevention service, Media Release, April 2010, accessed 15 March 2024.
427 Experian, Experian Hunter, accessed 15 March 2024.
428 Experian, Submission to the Report, 28 September 2023, pp 3–4.
429 Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, p 1, accessed 15 March 2024.
430 Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, p 1, accessed 15 March 2024.
431 Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, p 4, accessed 15 March 2024.
432 Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, p 4, accessed 15 March 2024.
433 Experian, Marketing Services | Mosaic, accessed 15 March 2024.
434 Experian, Fact Sheet – ConsumerView: The ultimate database of the Australian consumer, pp 4–6, accessed 15 March 2024.

- Aperture Data Studio is a data management platform, that includes data validation and enrichment options, enriching client data with data from a number of sources.[435] These sources include Mosaic, ConsumerView, public records and geographic data.[436]
- Experian also offers data validation services — including address, email, and phone number validation — that enable business customers to check and correct their customer databases.[437]

Experian has a broad customer base, including banks and financial services businesses, insurance companies, utilities companies, and telecommunications providers.[438] Experian notes that its marketing services are used by brands in nearly every industry – including financial services, media, automotive, travel and leisure, healthcare, retail and non-profits.[439]

4.1.2. Property data firms

Some data firms primarily provide property-related data products and services. CoreLogic and PropTrack are examples of data firms that supply the property services identified in section 3.4 of this Report.

CoreLogic

CoreLogic is a global data firm that operates in Australia. It specialises in property services, ranging from property data platforms to construction and valuation products. CoreLogic holds information on over 14 million properties – covering 98% of the Australian housing market.[440]

CoreLogic advertises that it uses 'hundreds of diverse property sets' in its property data products.[441] As an example, CoreLogic's Home Value Index uses datasets on sales and listings. CoreLogic notes that 'the majority of sales are reported through an agents' advice pipeline, which in the 12 months to August 2023 recorded 68.3% of sales prior to official notification of sales by the relevant Valuer General.'[442] For its Automated Valuation Model, CoreLogic uses data on a property's full address, property attributes such as bedrooms and land size, historical and recent sales information and local market trends.[443]

CoreLogic's data products and services include:

- RP Data, a platform that provides data and reports about individual properties, suburbs and market trends.[444] It also provides application programming interfaces (API), to connect RP Data with business customer websites and software,[445] and custom datasets for customers with particular needs.[446]
- valuation products, including:

435 Experian, Aperture Data Studio Product Sheet, accessed 15 March 2024.
436 Experian, Aperture Data Studio – Aperture Overview (video), accessed 15 March 2024.
437 Experian, Customer Data Validation, accessed 15 March 2024.
438 Experian, Submission to the Report, 28 September 2023, pp 10–11.
439 Experian, Submission to the Report, 28 September 2023, p 4.
440 CoreLogic, Our Data | What We Do, accessed 15 March 2024.
441 CoreLogic, Our Data | What We Do, accessed 15 March 2024.
442 CoreLogic, CoreLogic Australia Residential Property Index Series, October 2023, accessed 15 March 2024.
443 CoreLogic, What data is used to derive an Estimated Value?, accessed 15 March 2024.
444 CoreLogic, RP Data | Software & Solutions, accessed 15 March 2024.
445 CoreLogic, RP Data | Software & Solutions, accessed 15 March 2024. CoreLogic, Real-time data when you want it, where you need it, accessed 15 March 2024.
446 CoreLogic, What we do: Comprehensive property data solutions, accessed 15 March 2024.

  - an Automated Valuation Model (AVM)[447]
  - SMARTval, accessed through the Valex platform,[448] which facilitates the ordering and delivery of digital valuation reports
  - PropertyHub, a research platform for lenders and brokers, through which they can also order and track valuations[449]
  - ValConnect, a multi-purpose valuation platform that allows clients to research, access, combine and store property data from CoreLogic and other third-party sources for desktop and onsite valuations and assessments.[450]
- construction products, such as the Cordell Connect platform which provides a range of data on construction projects via APIs or reports.[451] It also provides Cordell SumSure, an online calculator for property rebuild cost estimates.[452]
- CoreLogic also provides 2 data-driven marketing products for use in the real estate sector:
  - RiTA, which enhances real estate agent client data with CoreLogic property and market data to generate potential clients.[453]
  - Plezzel, which is a targeted advertising product for real estate agents and agencies to advertise properties on social media platforms.[454]

CoreLogic also provides a free listings website (onthehouse.com.au)[455] for real estate agents and consumers, and a paid consumer research website (propertyvalue.com.au) providing information on, among other things, sale and rental values and history.[456]

CoreLogic's customers include banks,[457] insurance providers[458] and property professionals[459]. Banks, other lenders and mortgage brokers are key customers of CoreLogic's valuation and property market research tools.[460]

CoreLogic also supplies products and services to state and federal government clients, which CoreLogic indicates are used to inform economic policy, infrastructure decision-making and law enforcement initiatives.[461] For example, CoreLogic data has been cited in reports by the ABS and the NSW Treasury.[462]

---

447 CoreLogic, Our Data | Automated Valuation Model, accessed 15 March 2024.

448 CoreLogic, smartval | Software & Solutions, accessed 15 March 2024; CoreLogic, Data-powered digital solution a 'game changer' for faster property valuations, *News & Research,* 8 June 2023, accessed 15 March 2024; CoreLogic, Active Allocation: a power boost for CoreLogic Desktops, *News & Research,* 7 March 2022, accessed 15 March 2024.

449 CoreLogic, PropertyHub, accessed 15 March 2024.

450 CoreLogic, ValConnect, accessed 15 March 2024.

451 CoreLogic, Cordell Connect, accessed 15 March 2024.

452 CoreLogic, Cordell Sum Sure, accessed 15 March 2024.

453 CoreLogic, RiTA, accessed 15 March 2024.

454 CoreLogic, Plezzel, accessed 15 March 2024.

455 CoreLogic, Onthehouse.com.au, accessed 15 March 2024.

456 CoreLogic, Propertyvalue.com.au, accessed 15 March 2024.

457 CoreLogic, Industries | Banking and Lending, accessed 15 March 2024; CoreLogic, Our Data | Automated Valuation Model, accessed 15 March 2024.

458 CoreLogic, Industries | Insurance, accessed 15 March 2024.

459 CoreLogic serves a wide range of businesses in the property sector, as listed on its website. See CoreLogic, Industries, accessed 15 March 2024. See also CoreLogic, Time Savings for the Ray White Park Coast East Sales Team, *News & Research*, 26 February 2023, accessed 15 March 2024; CoreLogic, Enhanced Buyer Experiences, Increased Appraisals, and Brand Growth, *News & Research*, 26 October 2022, accessed 15 March 2024; CoreLogic, Helping OBrien Real Estate Berwick Attract Buyers & Homeowners, *News & Research*, 23 November 2023, accessed 15 March 2024.

460 See CoreLogic, Industries | Banking & Lending, accessed 15 March 2024; CoreLogic, Industries | Valuers, accessed 15 March 2024; CoreLogic, Industries | Mortgage Brokers, accessed 15 March 2024.

461 CoreLogic, Industries | Government, accessed 15 March 2024.

462 See, for example, Australian Bureau of Statistics, Total Value of Dwellings: Concepts, Sources and Methods, December 2022, accessed 15 March 2024; NSW Treasury, Housing, home ownership and household savings, 2021–22, accessed 15 March 2024.

PropTrack

PropTrack is a data firm owned by REA Group, which owns real estate websites, mortgage brokers and other property-adjacent companies in Australia.[463] PropTrack states it has the most 'comprehensive data and analytics available', including Australia's largest listings portal, with '1 trillion data points covering more than 12 million properties'.[464] PropTrack also uses insights generated from visitors to REA group websites, listings details and imagery from realestate.com.au, and real estate sales data in its products and services.[465] The PropTrack Home Price Index uses both sales price data from realestate.com.au and sales data from State and Territory Valuer Generals.[466] PropTrack's property data services use raw data from land titles offices, Valuer General offices, Geoscape Australia and realestate.com.au.[467]

PropTrack supplies 2 main categories of property products:[468]

- **Mortgage solutions products**, including:
  - an AVM, used to perform property valuations.[469] This model is made available by PropTrack in the following ways:
    - through property.com.au, where consumers can access a version for residential rental properties[470]
    - in the PropTrack Portfolio Manager, where it is used to perform batch property valuations across a property portfolio[471]
    - through realEstimate, a consumer version available on realestate.com.au[472]
  - PropTrack's valuation platform PropTrack Desktop, which is a web-based valuation tool for valuers to digitally conduct valuation assessments.[473]
- **Property data products**, (which may be supplied via PropTrack's APIs), data extracts and property reports related to residential property.[474] These products can be combined or used separately. Specific examples include:
  - Residential and commercial property data, using current and historical property data, which can also be incorporated through APIs into business customers' own websites and products, or downloaded as data extracts[475]
  - Property reports, which are specific to one property and automatically updated with recent data on address, key property details, property history, estimated value, comparable sales, median price guides and photo galleries.[476]

463 REA Group's network in Australia includes: realestate.com.au, realcommercial.com.au, flatmates.com.au, Mortgage Choice, PropTrack, Property, Campaign Agent, Simpology and Realtair. See REA Group, About us | Business and Brands, accessed 15 March 2024.
464 See PropTrack, Property Data and Insights, accessed 15 March 2024.
465 See PropTrack, Desktop, accessed 15 March 2024.
466 PropTrack, Home Price Index White Paper, accessed 15 March 2024.
467 PropTrack, Submission to the Report, 28 September 2023, p 7.
468 PropTrack, Submission to the Report, 28 September 2023, pp 1–2.
469 PropTrack, Submission to the Report, 28 September 2023, p 3.
470 PropTrack, Submission to the Report, 28 September 2023, p 3.
471 PropTrack, Portfolio Manager, accessed 15 March 2024.
472 See PropTrack, Submission to the Report, 28 September 2023, p 2.
473 See PropTrack, Submission to the Report, 28 September 2023, p 2.
474 See PropTrack, Submission to the Report, 28 September 2023, pp 2–3.
475 PropTrack, Submission to the Report, 28 September 2023, p 4; PropTrack, Property Data APIs: Instant access to property data, accessed 15 March 2024.
476 PropTrack, Submission to the Report, 28 September 2023, p 4; PropTrack, Digital Property Reports: cut through the market noise, accessed 15 March 2024.

– PropTrack Home Price Index is a more aggregated report provided monthly and annually on median property values. This is provided by region and property type.[477]

Both categories of PropTrack's products are marketed to banks, property valuers and local and state governments.[478] PropTrack claims that its data products and services assist banks, property valuers and local and state governments to '…increase property price transparency, enhance productivity and reduce operating costs and carbon emissions (by reducing the need for physical inspections)'.[479]

4.1.3. Data analytics and other data firms

The 4 data firms described in this section also supply a range of data products and services in Australia. Although each has a varying business model and data product and service portfolio, they can be roughly grouped together as offering data analytics services in relation to business customers' consumer or audience data. While the credit-reporting and property data firms described in sections 4.1.1 and 4.1.2 also offer data analytics services, the audience or consumer experience seems to be a greater focus for the firms described below.

Oracle

Oracle Australia, owned by Oracle (US), offers some of the types of data products and services identified in chapter 3. These include:

- Oracle Unity Customer Data Platform,[480] which provides data enrichment services by combining different sources of customer data, including second- and third-party data attributes. This enriches the customer's first-party data with Oracle's third-party data. Oracle Australia states that business customers can automate profile data enrichment within the Unity Customer Data Platform, with access to 'the world's largest third-party data marketplace'.[481]
- Moat Analytics, an ad measurement service assisting advertisers, ad publishers and digital platforms to measure advertising viewing and performance across channels and devices and in turn to assess the efficacy of their ads.[482]
- Responsys[483] and Eloqua Marketing Automation,[484] marketing campaign management platforms. Responsys can also be integrated with Oracle CrowdTwist Loyalty and Engagement to enrich customer profiles and segmentation.[485]

Globally, Oracle supplies its marketing products to business customers in a wide range of industries, including retail, aviation, financial services, banking, payments and insurance.[486] In Australia, business customers of Oracle's Eloqua Marketing Automation have included

477 PropTrack, Submission to the Report, 28 September 2023, p 4; PropTrack, PropTrack Home Price Index, accessed 15 March 2024.
478 See PropTrack, Industries, accessed 15 March 2024.
479 PropTrack, Submission to the Report, 28 September 2023, p 1.
480 Oracle, CX | Oracle Unity Customer Data Platform, accessed 15 March 2024.
481 Oracle, Profile enrichment | Oracle Unity Customer Data Platform, accessed 15 March 2024.
482 Oracle, Advertising | Oracle Moat Measurement and Customers | Spotify rocks advertisers with measurement by Oracle, 7 January 2022, accessed 15 March 2024.
483 Oracle, CX | Oracle Responsys Campaign Management, accessed 15 March 2024.
484 Oracle, CX | Oracle Eloqua Marketing Automation, accessed 15 March 2024.
485 Oracle, Oracle CrowdTwist Loyalty and Engagement, accessed 15 March 2024.
486 Oracle, CX | Oracle Marketing, accessed 15 March 2024; Oracle, Oracle Customer Successes, accessed 15 March 2024; Oracle, Industries | Financial Services Customer Acquisition and Experience, accessed 15 March 2024; Oracle, Oracle is a Leader in customer data platforms (CDPs) focused on the financial services industry, accessed 15 March 2024.

universities seeking to advertise to prospective students.[487] Flybuys has used Oracle's Responsys application to deliver targeted emails to its 8.6 million active members.[488]

Quantium

Quantium is 75% owned by supermarket chain Woolworths[489] and it uses Woolworths sales and transaction data from Woolworths, specifically transactional point-of-sale data capturing the volume of product sales and the products' price points to derive insights used in some products.[490] Quantium submits that it uses its business customers' own datasets, primarily within the customers' own IT systems, to supply client-specific data consulting services in Australia.[491]

Quantium supplies data products and services to particular business customers in the retail, fast-moving consumer goods and banking industries.[492] Such products and services include:

- Q.Refinery, used by clients in the banking industry,[493] which Quantium states can turn 'unstructured transaction data' into '[m]ore complete, higher quality customer data'.[494] More specifically, Quantium states that Q.Refinery transforms transaction data into thousands of customer attributes, giving an '[u]nparalleled understanding of each unique customer.'[495]
- Retail analysis services, such as:
  - Q.Checkout, which provides information such as likely consumer segment purchasing behaviours, likely product switching and product loyalty.[496] This information may, in turn, be used to inform pricing, promotional strategy or likely product substitutes.[497]
  - Q.Scan, which provides insights from transactional data capturing what products are purchased, how many, and at what price. Q.Scan helps retailers and suppliers[498] to understand the volume of products sold and to identify product sales trends, and primarily helps suppliers set their pricing and promotional strategies.[499]
  - Q.Shelf, which is used to inform product range and space decisions,[500] and to help clients understand likely substitutes and customer segments that might be interested in a product.[501]

487 See, for example, Oracle, Customers | ANU boosts student enrolment with Oracle, 4 February 2022, accessed 15 March 2024; Oracle, Customers | Victoria University engages Oracle Eloqua to market Open Day, 12 November 2021, accessed 15 March 2024.
488 Oracle, Customers | Flybuys delivers targeted emails at huge scale with Oracle Cloud, 18 November 2020, accessed 15 March 2024.
489 See Woolworths Group, Woolworths Group deepens partnership with Quantium, ASX Market Announcement, 20 April 2021, accessed 15 March 2024; S Mitchell, Woolworths doubles down on data, takes control of Quantium, *Australian Financial* Review, 20 April 2021, accessed 15 March 2024.
490 Quantium, Submission to the Report, 28 September 2023, p 2. See also Quantium, Q.Checkout, accessed 15 March 2024; Quantium, Q.Shelf, accessed 15 March 2024; Quantium, Q.Supply, accessed 15 March 2024.
491 Quantium submits that in many cases, it does not receive this business customer data in its own systems. See Quantium, Submission to the Report, 28 September 2023, p 2; Quantium, Privacy Policy, accessed 15 March 2024.
492 Quantium, Submission to the Report, 28 September 2023, p 2.
493 Quantium, Submission to the Report, 28 September 2023, p 3.
494 Quantium, Q.Refinery, accessed 15 March 2024.
495 Quantium, Q Refinery – Not all transaction data solutions are the same (video), accessed 15 March 2024.
496 Quantium, Submission to the Report, 28 September 2023, p 2.
497 Q.Checkout, accessed 15 March 2024. Quantium submits that it makes Q.Checkout available to Woolworths and its suppliers, as well as one other Australian client.
498 Quantium submits that it makes Q.Scan available to Woolworths and its suppliers. See Quantium, Submission to the Report, 28 September 2023, p 2.
499 Quantium, Submission to the Report, 28 September 2023, p 2.
500 Quantium, Q.Shelf, accessed 15 March 2024.
501 Quantium, Submission to the Report, 28 September 2023, pp 2–3. Quantium submits that it makes Q.Shelf available to Woolworths and its suppliers.

- Marketing measurement and optimisation tools, such as Q.Promotions, which uses transaction data and predictive modelling to measure the impact of sales promotions,[502] and Q.Supply, which provides business customers with a report on how to improve their sales performance using better product availability.[503] Quantium submits that Q.Supply is used to help Woolworths suppliers reduce waste in the supply chain.[504]

Box 4.1 CommBank iQ

Quantium has a joint venture partnership with the Commonwealth Bank, called CommBank iQ. This combines the Commonwealth Bank's transaction datasets from approximately 7 million customers[505] with Quantium's data analytics capability to develop data-driven products and services.[506] One example is Centre iQ, a platform which monitors 'real customer behaviour' and the competitive landscape to allow shopping centre owners to measure the impact of their 'development, marketing and leasing decisions' on customers' engagement with their centre.[507] CommBank iQ's key customer sectors include property, retail, government and financial services and insurance.[508]

LiveRamp

LiveRamp is a global data firm that provides a data collaboration platform in Australia.[509] LiveRamp's Australian business offers a service that allows its business customers to upload, collaborate on, segment and analyse their own datasets.[510]

LiveRamp's data products and services include:

- Safe Haven, a data management platform and data clean room used for data collaboration. It allows participating business customers to create their own segments and enrich the customer data they already hold with aggregated insights from other brands or businesses that they choose to partner with.[511] Once a business customer uploads its consumer data, LiveRamp removes directly identifiable personal data,[512] and converts it into pseudonymous RampIDs.[513] The platform's 'Lookalike-Modelled Audience' feature allows a businesses to target expanded audiences that share certain characteristics with their existing customer bases, such as age, gender, income, family status, and likes or dislikes.[514]
- LiveRamp's Authenticated Traffic Solution lets publishers capture hashed email addresses[515] of their website users and convert them to RampIDs which advertisers can

502 Quantium, Submission to the Report, 28 September 2023, p 2.
503 Quantium, Q.Supply, accessed 15 March 2024.
504 Quantium, Submission to the Report, 28 September 2023, p 3.
505 CommBank, CommBankiQ intelligence, accessed 15 March 2024.
506 Quantium, Commonwealth Bank and data science leader Quantium launch CommBank iQ to help customers build Australia's future economy, 10 May 2021, accessed 15 March 2024.
507 Commonwealth Bank, CommBank iQ, accessed 15 March 2024.
508 CommBank, CommBankiQ, accessed 15 March 2024.
509 LiveRamp, Submission to the Report, 28 September 2023, p 3.
510 LiveRamp, Submission to the Report, 28 September 2023, p 3.
511 LiveRamp, Safe Haven | Audiences, accessed 15 March 2024; LiveRamp, Safe Haven | Analytics Environment, accessed 15 March 2024; V Sharma, Data Clean Rooms: A Complete Guide, *LiveRamp Blog*, 20 April 2022, accessed 15 March 2024; LiveRamp, Data Collaboration, accessed 15 March 2024.
512 LiveRamp, Understanding Safe Haven: Safe Haven Features, accessed 15 March 2024.
513 LiveRamp, Understanding LiveRamp: Interpreting RampID, LiveRamp's People-Based Identifier, accessed 15 March 2024. As discussed in box 1.2, the use of pseudonymous identifiers does not necessarily prevent businesses from individually targeting consumers.
514 LiveRamp, Safe Haven | Overview of LiveRamp's Lookalike Modeling, accessed 15 March 2024.
515 Hashing is a data pseudonymisation technique described in the Glossary of this Report.

bid on.[516] This product allows business customers to measure advertising reach and effectiveness using what LiveRamp calls a 'privacy-first' solution.[517]

We note that LiveRamp has discontinued its Data Marketplace product in Australia.[518] Previously, this product allowed business customers to purchase third-party data from sellers to use for their own advertising and marketing purposes.[519]

Nielsen

Nielsen primarily offers data-driven marketing, media and audience products and services in Australia, with a particular focus on audience and media measurement and media planning.[520] A key source of data for Nielsen's data products are its 'panels', which are groups of people that Nielsen recruits to represent larger groups of people.[521] Nielsen monitors panel members' media consumption behaviour, with their permission.[522] For instance, this may involve a recruit attaching a box to their home TV to capture their TV viewing.[523] Nielsen also relies on various audio and video metadata, which captures how audiences engage with various media.[524]

Nielsen's products and services include:

- audience measurement products, such as TV Audience Measurement, Digital Audience Measurement, and digital ad ratings.[525] These services help business customers to understand their audiences by measuring the number of people who engage with media and advertising. They are provided across various content formats, including television (i.e. broadcast television and streaming services), digital (i.e. media content viewed on computer and mobile devices) and digital advertising (advertising campaigns on computer and mobile devices).[526] Nielsen states that audience measurement services provide an independent benchmark for advertisers and content creators, owners and distributers to measure and compare the performance of their ads or content against those of competitors[527]
- data-driven marketing services, such as segmentation and data enrichment services, including:
  - Nielsen Marketing Cloud, a data management platform that allows clients to collect, organise and use data to segment and target consumers with ads, and measure and optimise these ads[528]
  - Audience Segments, which provides custom and syndicated customer segments based on 'demographic, psychographic, behavioural, purchase-based and media consumption information'[529]

516 LiveRamp, Identity | Authenticated Traffic Solution, accessed 15 March 2024.
517 LiveRamp, Reach authenticated audiences across browsers, apps, and CTV—at scale, accessed 15 March 2024.
518 LiveRamp, Submission to the Report, 28 September 2023, p 3.
519 LiveRamp, Submission to the Report, 28 September 2023, p 3.
520 Nielsen, Marketing optimization, accessed 15 March 2024.
521 Nielsen, Nielsen Panels, accessed 15 March 2024.
522 Nielsen, How do panels and surveys work?, accessed 15 March 2024.
523 Nielsen, Nielsen Television Audience Measurement, accessed 15 March 2024.
524 Nielsen, Solutions | Gracenote Content Metadata, accessed 15 March 2024.
525 Nielsen, Audience Measurement: TV Measurement, accessed 15 March 2024; Nielsen, Audience Measurement: Digital Measurement, accessed 15 March 2024; Nielsen, Audience Measurement: Cross-Media Measurement, accessed 15 March 2024.
526 Nielsen, Submission to the Report, 28 September 2023, p 1.
527 Nielsen, Submission to the Report, 28 September 2023, p 2.
528 Nielsen, Media Planning | Marketing Cloud, accessed 15 March 2024.
529 Nielsen, Media Planning | Audience Segments, accessed 15 March 2024.

- media planning products, such as Gracenote.[530] These products are used to assist business customers to determine when, where and how to deliver content. For instance, audience measurement data may be applied and analysed to determine content strategies for streaming platforms and other media distributors and creators.[531]

Nielsen's products are marketed to potential business customers such as television broadcasters, pay television companies and other media audience measurement companies.[532] They are also marketed towards advertisers and publishers,[533] other data firms,[534] and digital platforms.[535]

4.2. Additional firms supplying data products and services in Australia

The ACCC has identified a number of other data firms that supply some of the types of data products and services described in chapter 3.[536] These are in addition to the 9 sample firms discussed above and other data firms that made submissions to the Inquiry, such as NielsenIQ.

We note that there are many other data firms not listed below that also supply products and services discussed in this Report, and the additional firms referenced below should not be considered an exhaustive list.

The other data firms we have identified include:

- **smrtr**[537] – smrtr is an Australian company that offers data enrichment, insights, segmentation, audience targeting and data activation services.[538] The data smrtr collects includes 11 million mobile advertising IDs and 50 billion 'location pings' per year, as well as 8 million residential properties with information on their location, size and value, and 5 million automotive purchase transactions.[539]
- **Thryv Data**[540] – Thryv Data Australia was formerly Australian company Sensis, which provided TrueLocal and the White and Yellow Pages, and is now owned by US company Thryv. Thryv supplies data services including data rental, validation and cleaning, data enhancement, customer profiling and segmenting, and access to targeted consumer lists from a database of over 19 million consumer records.[541]
- **Datametric**[542] – Datametric is an Australian company offering data collection, analysis and visualisation services. Datametric claims to be able to aggregate data from 'any online or offline source', through methods including web scraping and matching. It can

530 Nielsen, Gracenote Content Metadata | Global Sports Services, accessed 15 March 2024.
531 See Nielsen, Gracenote Content Metadata | Content Analytics Suite, accessed 15 March 2024.
532 Nielsen, Audience Measurement | National TV Measurement, accessed 15 March 2024. Foxtel is an example of Nielsen's pay television company customers – see Foxtel, Privacy Opt-Outs, accessed 15 March 2024.
533 Nielsen, Audience Measurement | Digital Ad Ratings, accessed 15 March 2024.
534 Nielsen, Nielsen partners with RDA and Eyeota in big win for ad reach, marketing analytics and campaign performance, Press Release, 18 September 2023, accessed 15 March 2024.
535 Nielsen, Nielsen ONE launches globally, press release, 18 October 2023, accessed 15 March 2024.
536 This is based on a review of the products and services advertised on these firms' Australian websites.
537 Smrtr, Home, accessed 15 March 2024.
538 Smrtr, Home, accessed 15 March 2024; smrtr, Audience Summary, accessed 15 March 2024.
539 Smrtr, smrtr Data Universe, accessed 15 March 2024.
540 Thryv Data, Home, accessed 15 March 2024.
541 Thryv Data, Home, accessed 15 March 2024.
542 Datametric, We Know Big Data, accessed 15 March 2024.

supply this to clients in a raw format, provide statistical or sentiment analysis, or build data visualisation models.[543]

- **Conexum**[544] – Conexum is an Australian-owned business offering a variety of data products and services including data rental, profiling and segmentation, and data cleaning. Conexum says it offers access to a variety of databases, including information on charity donors as part of the Insight Data Co-operative, multi-channel retailer transaction data from 120 contributors, and 1.6 million email data points on pre-mover homeowners and renters.[545]
- **Eight Dragons Digital**[546] – Eight Dragons Digital is a global supplier of consumer data, based in Australia, offering data on consumers that match the business customer's desired profile. It offers 'extensively profiled' consumer contacts across market segments including travel and tourism, retail, charities, and financial services.[547] It obtains data from a variety of sources, including government and publicly available data, consumer and market research surveys, marketing campaign partnerships and other data partners.[548]
- **Data Solutions**[549] – Data Solutions Australia provides access to comprehensive consumer and business databases and data cleaning services.[550] Data Solutions says its consumer database has information on 1.6 million households, while its business database contains 800,000 records.[551]
- **Eyeota**[552] – Eyeota, a Dun & Bradstreet company[553], is a 'global provider of audience data for marketing and advertising', offering data enrichment, segmentation, targeted advertising and data marketplace products in Australia.[554] Eyeota combines information such as demographic, behavioural and psychographic attributes from its data partners to create segments, which can be used to enrich first-party data.[555]
- **Circana**[556] – Circana is a global provider of data-driven services relating to consumer behaviour, including market insights, product insights and decision-making analytics, which serves the Australian market.[557] Circana Marketplace additionally offers data collaboration through access to partner data providers (including Experian).[558] Circana provides data on global consumer spend covering over 30 million products, 23 countries, 26 industries and over 500,000 stores.[559]
- **WINR Data**[560] – WINR Data is an Australian company that offers identity verification and data driven-marketing services. Its profiling services allow companies to build customer segments based on first and third-party data. Clients can connect identifiers from

543 Datametric, We Know Big Data, accessed 15 March 2024.
544 Conexum, Conexum – Data management services, accessed 15 March 2024.
545 Conexum, Data Rental Products, accessed 15 March 2024; Conexum, Data Insights, accessed 15 March 2024.
546 Eight Dragons Digital, Eight Dragons Digital, accessed 15 March 2024.
547 Eight Dragons Digital, About, accessed 15 March 2024.
548 Eight Dragons Digital, Data Collection, accessed 15 March 2024.
549 Data Solutions Australia, Data Solutions – Email, SMS, Telemarketing Lists, accessed 15 March 2024.
550 Data Solutions, Data Acquisition, accessed 15 March 2024.
551 Data Solutions, Consumer Data - Email, SMS, Telemarketing Lists, accessed 15 March 2024; Data Solutions, Business Data - Email, SMS, Telemarketing Lists, accessed 15 March 2024.
552 Eyeota, Global Quality Audience Targeting Data for Advertisers and Marketers, accessed 15 March 2024.
553 Eyeota, Eyeota is now a Dun & Bradstreet Company!, accessed 15 March 2024.
554 Eyeota, Addressable & Globally Available Audience Data for Digital Advertising, accessed 15 March 2024.
555 Eyeota, Audience Marketplace, accessed 15 March 2024.
556 Circana, Unlock Growth with Complete Consumer Insights, accessed 15 March 2024.
557 Circana, About Us, accessed 15 March 2024. MediaWeek, The Trade Desk and Circana partner to strengthen retail data in Australia, 8 November 2023, accessed 15 March 2024.
558 Circana, Circana Marketplace, accessed 15 March 2024.
559 Circana, Home, accessed 15 March 2024.
560 WINR Data, Global Identity Data Solutions, accessed 15 March 2024.

various platforms and WINR can also enrich their data with additional attributes such as age, gender, and affluence.[561]

- **Xandr**[562] – Xandr (owned by Microsoft) operates globally and in Australia as a digital advertising platform and data marketplace that allows buyers to obtain third-party data to target specific audiences.[563]
- **iD4me**[564] – iD4me is an Australian company that offers a 'comprehensive database', including data enrichment and validation, and platforms to search for data on individuals and to download segmented consumer marketing lists. Its database contains over 14 million phone numbers and 12 million email addresses across Australia and New Zealand.[565]
- **Lexer**[566] – Lexer is a global company, headquartered in Australia, that offers a customer data platform which provides data enrichment, audience segmentation, data analytics and targeted advertising services. Customers can connect data from various sources to create a singular view of each customer, and enrich their data with third-party segments from Experian's Mosaic.[567]
- **Adobe**[568] – Adobe is a global company that supplies various data-driven marketing products and services in Australia, such as a data management platform which includes data enrichment, segmentation and data marketplace services.[569] Adobe's Audience Marketplace allows users of the platform to source, sell and exchange audience and customer data, including datasets from firms such as Acxiom, Eyeota and Experian.[570]
- **Domain Group**[571] – Domain Group is an Australian entity that supplies property data products and services through various brands, including property data platforms, automated valuation models, property marketing, lead generation and targeted advertising products.[572] Domain says its data networks capture 14.7 million properties, an average of 7.9 million online users and over 100 engagement signals monitored by its platforms.[573]
- **Azira**[574] – Azira (formerly Near Intelligence) is a global company that supplies a data platform which uses consumers' home location and behavioural data to offer marketing products and services in Australia, such as segmentation, targeted advertising, and measurement and optimisation services.[575] It also offers location-based analysis and information for analytics and decisioning services.[576]

---

561 WINR Data, About Us, accessed 15 March 2024; WINR Data, Identity Resolution Providers, accessed 15 March 2024.
562 Microsoft Advertising, Xandr - Reach audiences across screens with premium advertising, accessed 15 March 2024.
563 Microsoft Advertising, Xandr - Reach audiences across screens with premium advertising, accessed 15 March 2024; Microsoft Advertising, Xandr - Xandr Marketplace, accessed 15 March 2024.
564 iD4me, Home, accessed 15 March 2024.
565 iD4me, Home, accessed 15 March 2024.
566 Lexer, Lexer | The Leading Customer Data Platform for Retailers, accessed 15 March 2024.
567 Lexer, The Customer Data Platform for retail brands, accessed 15 March 2024; Lexer, Create Actionable Segments, accessed 15 March 2024.
568 Adobe, Adobe: Creative, marketing and document management solutions, accessed 15 March 2024.
569 Adobe, Audience Marketplace, accessed 15 March 2024; Adobe, Real-Time CDP features, accessed 15 March 2024.
570 Rich Phillips, Source, Sell, and Swap Audiences with Ease using Adobe Audience Manager Audience Marketplace, *Adobe Blog,* 10 November 2015, accessed 15 March 2024.
571 Domain Group, About Us – Domain Group, accessed 15 March 2024.
572 Domain Group, Portfolio - Domain Group, accessed 15 March 2024. See also Domain Insight, Market Intelligence, accessed 15 March 2024; Domain Insight, Valuations, accessed 15 March 2024; Pricefinder, Pricefinder Property Data Solutions, accessed 15 March 2024; Domain Media, Home, accessed 15 March 2024; Realbase, Realbase.io, accessed 15 March 2024.
573 Domain Insight, Home, accessed 15 March 2024.
574 Azira, Know your Market. Reach your customer., accessed 15 March 2024.
575 Near, Affinity Audiences and Location-Based Marketing Solution, accessed 15 March 2024.
576 Near, Foot Traffic Insights and Operational Intelligence Solution, accessed 15 March 2024.

4.3. Customers of data products and services

A wide range of entities use data products and services in Australia, including business customers in financial services, retailing, media and telecommunications, marketing and advertising, property, and digital platforms, as well as government.

Many firms that supply data products and services are also customers of other firms that supply these services. As discussed in chapter 6, the relationships that different suppliers of data products and services have with each other, as both competitors and customers, may have implications for the nature and complexity of competitive dynamics in the supply of these services.

4.3.1. Financial services

Customers in the financial services sector include banks, fintech companies, Buy Now Pay Later (BNPL) providers, private equity firms and superannuation funds.[577] Businesses in this sector access a range of different data products and services from data firms. For example, a bank may use risk management services to verify the identity or income of customers seeking a loan, to streamline its credit assessments and reduce the risk of fraud,[578] or it may use marketing products to learn more about spending behaviours, preferences or wider trends.[579] A bank or other lender may also use property data services, such as an Automatic Valuation Model, in assessing an applicant for a residential or commercial property loan.[580]

4.3.2. Retail and consumer goods

The retail industry covers supermarkets, department stores, large retail stores, and restaurants. The fast-moving consumer goods (FMCG) sector includes food and beverage, home and personal care businesses. Some companies in these industries use third-party data and data products and services to learn about their customers and potential customers to improve their data-driven marketing and advertising projects.[581] For example, FMCG and retail businesses use LiveRamp's Safe Haven data clean room environment to compare and match their own first-party data, including transactional data, to generate new audience insights, and optimise their audience reach.[582] Similarly, Quantium markets many of its services to FMCG brands.[583]

As mentioned in chapter 2, the ACCC's Customer Loyalty Schemes Report found that operators of customer loyalty programs, including in the FMCG and retail sectors, may enrich their customer data by acquiring additional data or insights from third-party data firms – largely for the purpose of segmentation and personalised advertising.[584] As also

577 See illion, Case Studies, accessed 15 March 2024; Experian, Submission to the Report, 28 September 2023, p 10; Oracle, Customer Successes, accessed 15 March 2024.
578 See, for example, illion, Case studies: Bank Australia dramatically reduces assessment timeframes and achieves faster, more responsible decisions leveraging illion's frictionless bank data, accessed 15 March 2024.
579 See, for example, Experian, Who Uses Our Services, accessed 15 March 2024. See also Quantium, Submission to the Report, 28 September 2023, p 3.
580 See, for example, PropTrack, Industries: Banking, accessed 15 March 2024; CoreLogic, Industries: Banking & Lending, accessed 15 March 2024; CoreLogic, Automated Valuation Model, accessed 15 March 2024.
581 LiveRamp, Submission to the Report, 28 September 2023, p 2.
582 LiveRamp, Danone Boosts Customer Intelligence and Addressable Reach Using LiveRamp's Safe Haven, accessed 15 March 2024.
583 Quantium, Homepage, accessed 15 March 2024.
584 ACCC, Customer Loyalty Schemes Final Report, 3 December 2019, p 47.

noted in chapters 2 and 3, customer loyalty schemes are also a source of data for some data firms' products and services.[585]

4.3.3. Media and telecommunications

Businesses in Australia's media and telecommunications sector are customers of a wide range of marketing, audience measurement and risk management products and services supplied by data firms. For example, media organisations are among Equifax's customers for its Consumer Audience product.[586] Free TV Australia submits that its members, comprising all of Australia's commercial free-to-air television broadcasters, rely on data enrichment services provided by data firms to offer segment-based digital advertising.[587]

4.3.4. Marketing and advertising

Marketing, advertising and media agencies are key business customers of data firms. In particular, Nielsen submits that data-driven audience measurement products and services are often used by advertising agencies to confirm audience exposure to their products.[588] Experian notes it works with 'carefully selected partners and advertising, marketing and media agencies', who use its marketing data to serve their own customers.[589] Several submissions to the Issues Paper noted that data products and services play an important role in the digital advertising ecosystem.[590]

4.3.5. Property

Businesses in Australia's property sector, including real estate agents, property investors, and adjacent industries like mortgage brokers and property insurers, may use property data products and services.[591] The Australian Property Institute (comprising 4,000 Australian property companies) notes that the property data and analytics products provided by data firms such as CoreLogic and PropTrack allow property valuation professionals to perform their functions accurately and efficiently.[592] The sector also uses various marketing products, for example, to identify potential customers and target them with advertising.[593]

4.3.6. Digital platforms

As discussed in section 1.4, prior ACCC work has demonstrated that data collection is central to the business models of most advertiser-funded digital platforms.

Digital platforms such as Meta, X (formerly Twitter), Amazon and eBay may acquire data for the purpose of enriching their own first-party data, segmenting audiences and delivering

585 ACCC, Customer Loyalty Schemes – Final Report, 3 December 2019, pp 47, 72.
586 Equifax, Submission to the Report, 28 September 2023, p 15.
587 Free TV Australia, Submission to the Report, 28 September 2023, pp 2–5.
588 Nielsen, Submission to the Report, 28 September 2023, p 1.
589 Experian, Submission to the Report, 28 September 2023, p 11.
590 See, for example, Free TV Australia, Submission to the Report, 28 September 2023, pp 3–5; IAB Australia, Submission to the Report, 28 September 2023, pp 6-7.
591 PropTrack, Submission to the Report, 28 September 2023, p 5; CoreLogic, Industries – Residential Real Estate, Industries – Property Investors, Industries – Banking & Lending, Industries – Valuers, Industries – Insurance and Industries – Mortgage Brokers, accessed 15 March 2024.
592 Australian Property Institute, Submission to the Report, 28 September 2023, p 1.
593 See CoreLogic, Time Savings for the Ray White Park Coast East Sales Team, *News & Research*, 26 February 2023, accessed 15 March 2024; CoreLogic, Enhanced Buyer Experiences, Increased Appraisals, and Brand Growth, *News & Research*, 26 October 2022, accessed 15 March 2024; CoreLogic, Helping OBrien Real Estate Berwick Attract Buyers & Homeowners, *News & Research*, 23 November 2023, accessed 15 March 2024.

targeted advertising.[594] Digital platforms may also integrate media measurement products and services to assess the performance of advertising campaigns and connect advertisers to their desired target audiences.[595] IAB Australia submits that many smaller platforms regard these services as fundamental to their ability to compete with larger platforms for advertising spend and to deliver relevant content.[596]

4.3.7. Data firms

As discussed in chapter 3, data firms utilise many different types of data to develop their products and services. Accordingly, data firms often have arrangements with other data firms to acquire or exchange information or services.

Data firms may choose to acquire specific types of data from more specialised data firms, to use as inputs to their own products. For example, Equifax has a partnership with CoreLogic to deliver national sales and valuation data. Using CoreLogic's Automated Valuation Model, information is drawn from multiple data sources to calculate property values.[597] smrtr connects with CoreLogic property data, including listing activity, values, tenure and property characteristics, for use in its own products.[598]

In some cases, a data firm may choose to integrate another data firm's product or service within one of its own product offerings, to enhance its capabilities. For example, Experian offers partnership opportunities where other data firms can integrate Experian's solutions into their own platforms or resell Experian data, services or solutions directly to their end customers.[599] In particular, Experian's Mosaic and ConsumerView dataset and segmentation tools are licensed by Lexer, and Mosaic by Circana, who make this available to their own customers by incorporating it into their own services.[600] Similarly, Nielsen's Consumer and Media View dataset and audience segments are made available to Eyeota's customers though Eyeota's audience marketplace.[601]

Chapter 6 further considers competitive dynamics relating to the exchange and sale of information and partnerships or joint ventures between data firms.

4.3.8. Government and public sector

Marketing, risk management and property data products and services are widely used by the public sector, across a range of federal and state government bodies.

Experian's consumer marketing services are used by several public sector organisations, including national and local government, public health bodies, emergency services such as police, fire and ambulance, and other public service initiatives.[602]

---

594 This practice is stated in the privacy policies of many major digital platforms. See, for example, Meta, Privacy Policy; X, Privacy Policy; Amazon, Interest-Based Ads; eBay, User Privacy Notice, accessed 15 March 2024.

595 See, for example, Oracle, Customer references | Spotify rocks advertisers with measurement by Oracle, accessed 15 March 2024.

596 IAB Australia, Submission to the Report, 28 September 2023, p 4.

597 Equifax, Property Valuation | Business & Enterprise and Property Valuation: Features - Benefits | Business & Enterprise, accessed 15 March 2024.

598 Smrtr, Data Universe, accessed 15 March 2024. See also Salinger Privacy, Submission to the Report, 28 September 2023, p 5.

599 Experian, Why Partner with Us, accessed 15 March 2024; Nielsen, Nielsen and Experian expand agreement to enhance identity demographics, Press Release, 28 February 2022, accessed 15 March 2024; Eyeota, Experian Overview & Buyer's Snapshot, accessed 15 March 2024.

600 Lexer, Partner data – Experian, accessed 15 March 2024; Circana, Circana Marketplace, accessed 15 March 2024.

601 Nielsen, Nielsen partners with RDA and Eyeota in big win for ad reach, marketing analytics and campaign performance, Press Release, 18 September 2023, accessed 15 March 2024.

602 Experian, Who Uses Our Services, accessed 15 March 2024.

illion's risk management data and analytics services have been used by federal, state and local government agencies to improve operations and reduce fraud, waste and abuse by suppliers.[603]

Government bodies may also seek data products and services to assist in their recruitment processes. For example, Equifax's fit2work background checks may be used by government departments around Australia to verify applicants' criminal history, employment history, referees and more.[604]

Property data services may be used by government bodies for a number of purposes, including infrastructure planning, and statutory valuation assessments and administration, such as for determining council rates and land tax.[605] Property data from data firms is also cited in government reports.[606] This data may be used to analyse housing trends, measure housing demand and affordability and inform government policy decisions.[607]

4.4. Terms on which data products and services are supplied

4.4.1. Pricing

As data firms' products and services are highly customisable, they often apply highly varied and tailored pricing. However, some common pricing models include:

- **Pay per use/per transaction:** Pay per use is a common method of payment for data products and services, whereby customers are charged per instance they access or use the product. This allows customers to avoid paying for services they may not need or use regularly.[608] OECD research indicates that data firms that sell personal data, for example for advertisement purposes, mostly use the pay-per-dataset model.[609]
- **Subscription models:** Data firms also commonly provide access to data products or services via subscriptions. Subscriptions are often annual but may be for shorter periods in some cases.[610]
- **Licensing models:** Data firms may grant customers a licence to use their data assets, such as access to processed data or data analysis tools. For example, Experian notes that its EMS product will license data attributes to its business customers. [611]
- **No-monetary-cost or reciprocal agreements**: Some data firms may offer certain services to some types of users at zero monetary cost. For example, PropTrack makes available various products and services via its website realestate.com.au[612] (where data is also generated by the website's users). Other zero monetary cost arrangements include

603 illion, Government Best Practices for Mitigating Supplier Risk, *2017 Finance Industry Interviews: Summary Report*, 2017, accessed 15 March 2024.
604 Equifax, Fit2work, accessed 15 March 2024.
605 See, for example, DomainInsight, Government, accessed 15 March 2024. See also PropTrack, PropTrack Valuations Platform, accessed 15 March 2024.
606 See, for example, Australian Bureau of Statistics, Total Value of Dwellings: Concepts, Sources and Methods, December 2022, accessed 15 March 2024. See also NSW Treasury, Housing, home ownership and household savings, 2021-22, accessed 15 March 2024.
607 CoreLogic, Industries | Government, accessed 15 March 2024; PropTrack, Public Sector - PropTrack, accessed 15 March 2024.
608 V Wauters, What is Pay-Per-Use (PPU) and how can it benefit your business, *Bundl*, accessed 15 March 2024.
609 OECD, Data Driven Innovation: Big Data for Growth and Well-Being, October 2015, p 82.
610 For example, Equifax offers a subscription model for its Credit and Identity Protect products. See Equifax, Credit and Identity Products | Equifax Personal, accessed 15 March 2024.
611 Experian, Submission to the Report, 28 September 2023, p 9.
612 For example, PropTrack states that its rental AVM is available to consumers on property.com.au, REA's property research website. See PropTrack, Submission to the Report, 28 September 2023, p 3.

reciprocal agreements, where data firms may acquire data assets from a customer, in exchange for providing them with access to a product or service.

Other pricing arrangements may include a 'one-off' fee (e.g. for supplying static reports or undertaking agreed statements of work), or a price per 1,000 customer ad impressions (cost per mille or CPM) for digital advertising products.[613]

Data firms typically offer several different pricing options, depending on the product or service. For example, PropTrack licenses its mortgage solutions as a suite of products, or as standalone products, in most cases for a monthly subscription fee or a pay-by-consumption basis, which may also be tiered with lower charges per use as consumption increases.[614] PropTrack also offers customers using its Property Data APIs a charge per extract for a static file, based on the parameters of the data request.[615]

Similarly, Equifax applies various pricing models depending on the type of data product or service, including pricing on a per-transaction or per-purchase basis (such as for its commercial data products), subscription-based models, one-off fees, licensing fees, or tiered pricing based on the amount of data used.[616] Through Experian Marketing Services, Experian licenses data attributes and provides analytical services, based on an agreed statement of work.[617] It also offers digital marketing services on a CPM basis.[618]

4.4.2. Restrictions on use

Data firms sometimes provide products and services with certain restrictions, relating to conditions of use, data security and protection of intellectual property. These may include:

- **Permitted use cases**: Data assets will often be provided for the purpose of a defined permitted use, which is usually negotiated with the customer on a case-by-case basis. For example, according to Equifax's terms of supply for its HR-Workforce products, reports and information may only be used for internal business use, and for the purpose they were supplied for.[619]
- **Restricted use cases**: Data may be provided with certain restricted uses. For example, Equifax submits that it imposes specific conditions on the use of data it provides, and that prior to contracting, it investigates the context(s) in which any dataset is to be used.[620]

613 CoreLogic, Insights for confident property decisions, accessed 15 March 2024.
614 PropTrack, Submission to the Report, 28 September 2023, pp 2, 4–5.
615 PropTrack, Submission to the Report, 28 September 2023, p 5.
616 Equifax, Submission to the Report, 28 September 2023, pp 10, 12.
617 Experian, Submission to the Report, 28 September 2023, p 9.
618 Experian, Submission to the Report, 28 September 2023, p 9.
619 See Equifax, Fit2Work Terms of Supply, accessed 15 March 2024.
620 Equifax, Submission to the Report, 28 September 2023, p 11. Likewise, illion submits it may restrict the use of some of its product outputs based on the type of data being supplied or the purpose for which the data was obtained, particularly in relation to identity verification services. See illion, Submission to the Report, 28 September 2023, p 6.

5. Potential consumer issues

Key observations

- Many consumers are not aware that a range of data firms may collect their data from a variety of sources, or how this data may be used. 74% of Australians are uncomfortable with the idea of their personal information being shared or sold with other companies. The collection, sharing and use of consumer data between firms is often facilitated by the inclusion of broad terms in lengthy consumer-facing privacy policies for a wide range of digital and physical products and services.
- These policies may use ambiguous language, referring to the sharing of information with 'partners', 'suppliers' or 'affiliates', making it difficult for a consumer to identify and understand who their data may be shared with, and for what purposes. This limits a consumer's ability to identify who holds their data and exercise their rights to inspect or correct that data or opt out of its collection and use.
- While de-identified data has important beneficial uses, there is a risk that individuals may be identified within a previously de-identified dataset when it is combined with additional data points from other sources.
- Data products and services may be misused by bad actors, resulting in the risk of consumer harm. Such harms may include the targeting of vulnerable consumers with inappropriate advertising, discrimination and the exclusion of individuals or groups from certain opportunities, and the identification of potential scam and fraud victims. While many data firms have in place various controls to protect data, including terms and conditions in their supply agreements, once data is out of the hands of one party, generally that party has little or no way to guarantee that the data will remain subject to appropriate protection and controls.
- The collection and storage of large amounts of consumer data by data firms may make them a target for data breaches and other data security incidents. Where such incidents occur, there is the potential for consumer harm.
- The increasing prevalence and use of RentTech platforms in Australia can lead to streamlined application processes for landlords and prospective tenants. However, it may also create or exacerbate a range of data security and privacy risks for consumers. The mandatory use of these platforms to apply for a rental property forces consumers to contribute additional data, which may be used in ways that consumers do not expect. One service identified advertises a personality assessment product that can be embedded into online application process. Once an applicant completes the questionnaire, the service provides a report on tenant safety and risk which are then indexed against a proprietary database of tenancy risk indicators that the service advertises can be used to 'predict future tenant behaviour.'

This chapter examines potential consumer issues arising from the collection and use of consumer data in a range of data products and services offered by data firms in Australia. It is structured as follows:

- **Section 5.1** considers consumers' general lack of awareness and understanding of how their data may be collected, shared and used. It discusses current barriers to consumers being able to exercise meaningful choice and control over their data, often arising from

the inclusion of "take-it-or-leave-it" terms in some privacy policies which a consumer must accept in order to access a service. Finally, it considers how consumer consent is obtained, noting this often involves long and complex privacy policies which may permit the sharing of consumer data with unidentified third parties. This makes it difficult for consumers to identify who may collect and use their data, and for what purposes.

- **Section 5.2** considers a range of potential harms that consumers may experience from the misuse of their data. This includes a discussion of the risks of data re-identification, the identification and targeting of vulnerable consumers, the potential for discrimination and exclusion, reliance on incorrect or incomplete data, the use of data to facilitate scams and fraud, misuse of location data, and data security breaches.

Box 5.1 Measures proposed to address the issues discussed in this chapter

As discussed in chapter 1, in September 2023 the Australian Government released its response to the recommendations set out in the Privacy Act Review Report. This response indicated agreement, or in-principle agreement, with a majority of the 116 recommendations of the report.[621]

The ACCC considers that the privacy-related issues discussed in this chapter are best addressed in the first instance through strengthened privacy laws, coupled with the allocation of further resources to the Office of the Australian Information Commissioner (OAIC). However, we note that certain practices that give rise to potential consumer harms may not necessarily be addressed by strengthened privacy laws, such as those that use only de-identified data.

Throughout this chapter, the ACCC will note specific proposals from the Privacy Act Review Report that are relevant to the issues identified.

In addition, some issues around data use and misuse may be covered by existing provisions of the Australian Consumer Law (ACL), such as where a firm makes a potentially false or misleading statement in its privacy policy about how it uses consumer data or who it shares consumer data with. The unfair contract provisions of the ACL may also be relevant when assessing terms in data firms' standard-form contracts that govern what data may be collected from consumers, and how data firms may use it (including sharing with third parties). The ACCC will continue to consider such issues, and potential actions to address them, under our Compliance and Enforcement Policy.[622]

The ACCC also continues to support the introduction of a prohibition on unfair trading practices in the ACL.[623] Such a prohibition could better capture instances of harmful conduct that may currently fall outside the scope of the existing provisions of the ACL. For example, such conduct may include the use of click-wrap agreements containing "take-it-or-leave-it" terms and seeking bundled consents to policies that are long, complex, and unclear, in order to obtain unreasonable rights to use data or share it with others.

621 Australian Government, Government Response – Privacy Act Review Report, 28 September 2023. The government agreed to 38 recommendations, agreed in-principle to 68 and noted 10. Those agreed to in-principle will be subject to further engagement with regulated entities and an impact analysis to be led by the Attorney-General's Department.

622 ACCC, Compliance and enforcement policy and priorities, accessed 15 March 2024.

623 The Government is currently consulting on options to address unfair trading practices. See The Treasury, Unfair trading practices – Consultation Regulation Impact Statement, accessed 15 March 2024.

5.1. Consumer awareness, choice, control and consent regarding how their data is used

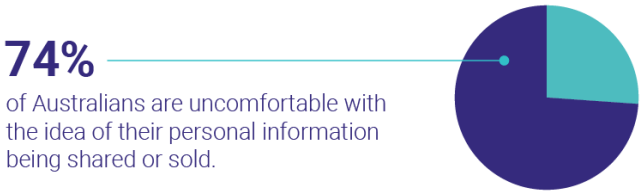
5.1.1. Consumer awareness

Many consumers are not aware that a range of data firms collect their data from a variety of sources, including other firms, or how this data may be used.[624] This raises the question of whether consumers are able to understand and knowingly consent to, or control, how their data is collected and used.

This problem is not unique to data firms. For example, the ACCC's original Digital Platforms Inquiry found consumers are generally not aware of how much data is collected, nor of how it is collected, shared and used, by digital platforms.[625] This is influenced by the length, complexity and ambiguity of online terms of service and privacy policies. Digital platforms also tend to understate to consumers the extent of the platforms' data collection practices, while overstating the level of consumer control over their data.[626]

Similar consumer sentiments are echoed in relation to the data practices of firms across the economy more broadly. A 2023 survey by the OAIC found only 21% of Australians 'always or often' read an organisation's privacy policy before providing their personal information,[627] while a similar survey by the Consumer Policy Research Centre (CPRC) found 74% of Australians were uncomfortable with the idea of their personal information being shared or sold (see figure 5.1 below).

Figure 5.1: CPRC 2023 survey of consumer views on how businesses use their data[628]



Consumer understanding of what is meant by 'de-identified' data

The ACCC considers most consumers are unlikely to understand what is meant by the term 'de-identified' data or how this term may be used by data firms to describe consumer data. As discussed in chapter 1, recent research by the CPRC found that most consumers report having no knowledge of, or familiarity with the term 'de-identified information', nor with related terms such as 'pseudonymised information', 'hashed email addresses', 'aggregated

624 UNSW Allens Hub (K Kemp and G Greenleaf), Submission to the Report, 28 September 2023, p 8; Salinger Privacy, Submission to the Report, 28 September 2023, p 12; CPRC, Submission to the Report, 28 September 2023, p 3. Consumer surveys reviewed by the ACCC in preparing the Customer Loyalty Schemes Report suggested that many consumers are concerned about the sharing of their data with unknown third parties, targeted advertising, and whether their data is being used responsibly. See ACCC, Customer Loyalty Schemes: Final Report, 3 December 2019, p 55.
625 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 23.
626 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 23.
627 OAIC, Australian Community Attitudes to Privacy Survey, August 2023, pp 21–22.
628 CPRC, Not a fair trade: Consumer views on how businesses use their data, March 2023, p 9.

information', or 'advertising ID'.[629] Businesses may use these terms in their consumer-facing privacy policies when describing the information they collect.[630]

5.1.2. Consumer choice and control

In the original Digital Platforms Inquiry, the ACCC found that Australian consumers are better off when they are both sufficiently informed and have sufficient control over the collection and use of their data.[631] It noted that transparency over the collection of data is important, so that consumers can understand what data they are providing and how it is used.[632] However, the Digital Platforms Inquiry also noted that transparency alone is not enough and that consumers, once they understand what data is being collected and how it will be used, must be able to exercise choice and meaningful control.[633]

The OAIC submits that 'even where individuals do read privacy policies and collection notices, they may feel resigned to consent to the use of their information to access online services as they do not feel there is any alternative.'[634] The ACCC considers that this could particularly be the case when consumers are required to use a data product in order to access an essential service. One example is the growing requirement to use RentTech platforms to apply for a rental property, discussed in a case study below at box 5.2.

A recent CPRC study on Data Privacy Perspectives (conducted in September 2023) reveals that the majority of Australians do not feel in control of their personal information, with more than 70% of consumers believing they have very little or no control over what personal information online businesses share with other businesses.[635] Figure 5.2 demonstrates that most consumers feel it is unacceptable for businesses they are not in direct contact with to use their data. In a similar vein, another study conducted by the CPRC in 2020 found 94% of consumers are uncomfortable with how their personal information is collected and shared online. Equally significantly, 94% of Australian consumers reported not reading all of the privacy policies or terms and conditions that applied to them in the previous 12 months.[636]

629 K Kemp, C Gupta and M Campbell, Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them, CPRC and UNSW Sydney, February 2024, p 13.

630 For example, Flybuys' Privacy Policy notes they *'collect from [Flybuys] Participants information about your purchases when you haven't presented your Flybuys card, but where we were able to identify from your payment card information that you have made the purchase. We use this information on an anonymised, aggregated basis for modelling and research purposes.'* The Privacy Policy also notes Flybuys may collect personal information from third parties, including from *'Flybuys media and advertising partners, to enable us to provide them with aggregated and de-identified data and services for targeted advertising purposes.'* FlyBuys, Privacy Policy, 1 December 2021, accessed 15 March 2024.

631 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 22.

632 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 22.

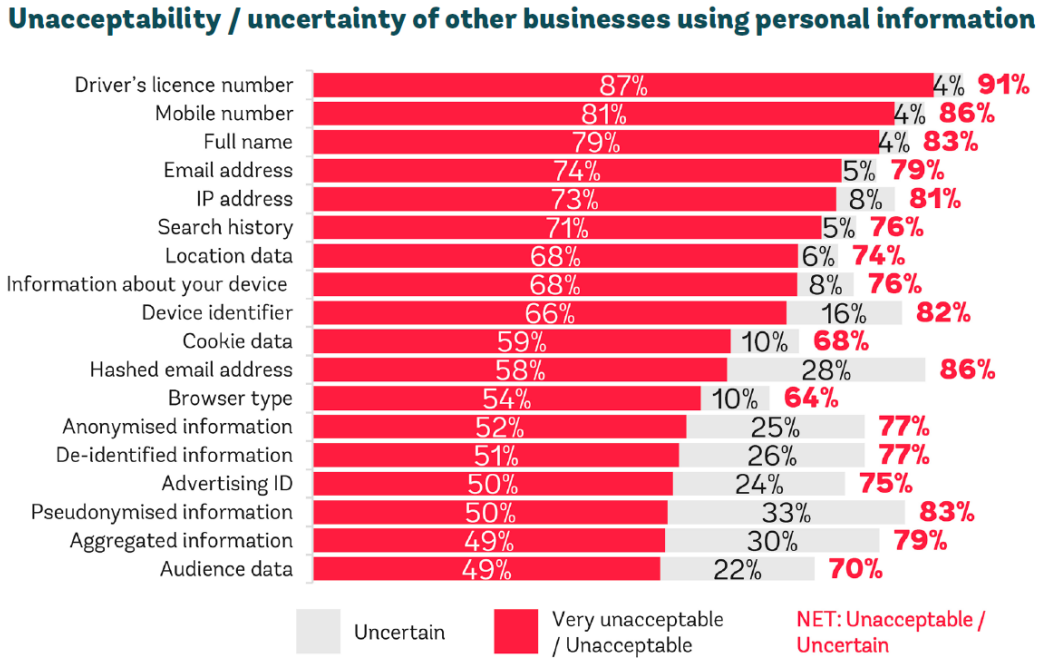
633 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 9.

634 OAIC, Submission to the Report, 28 September 2023, p 14.

635 K Kemp, C Gupta and M Campbell, Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them, CPRC and UNSW Sydney, February 2024, p 13.

636 CPRC, CPRC 2020 Data and Technology Consumer Survey, 7 December 2020, accessed 15 March 2024.

Figure 5.2: CPRC 2023 study of consumer views regarding the use of their data by businesses they are not in direct contact with[637]



Dr Katharine Kemp and Professor Graham Greenleaf submit that "take-it-or-leave-it" terms contained in some privacy policies do not constitute choice or consent by the individual.[638] Salinger Privacy argues consent must be truly voluntary, informed, specific, current, and granted actively and willingly by a person with both the capacity to understand and, in circumstances where they had the option to make a choice between granting or refusing their consent, without being denied access to goods or services.[639]

Box 5.2 Case study – the growing use of RentTech platforms in Australia

As discussed in chapter 3, RentTech platforms are online platforms used by real estate agents, landlords and tenants to more easily manage the rental application process.[640] The use of RentTech platforms has grown rapidly in recent years and they are now widely used across Australia.[641] They can centralise the tenancy application process via a single, self-service platform capable of saving previously inputted information, avoid time-consuming paper-based processes, and streamline the identification and income validation processes.

Lack of consumer choice

637 K Kemp, C Gupta and M Campbell, Singled Out – Consumer understanding – and misunderstanding – of data broking, data privacy, and what it means for them, CPRC and UNSW Sydney, February 2024, p 13.
638 UNSW Allens Hub (K Kemp and G Greenleaf), Submission to the Report, 28 September 2023, p 4.
639 Salinger Privacy, Submission to the Report, 28 September 2023, p 3.
640 RentTech platforms can also be used for purposes beyond just the rental application process, including property management and payment processing. See Victorian Government, The rental and housing affordability crisis in Victoria Inquiry, November 2023, p 144.
641 A Kollmorgen and K Bower, RentTech platforms making renting that much harder, *CHOICE*, 18 April 2023, accessed 15 March 2024.

Despite these efficiencies, Digital Rights Watch notes many renters feel they have no choice but to comply with whatever is asked of them, out of fear of being passed up for another applicant.[642] In an April 2023 survey by CHOICE, 41% of renters noted they had been pressured to use a RentTech platform.[643] This is likely exacerbated by the recent demand and increased competition for finite rental properties in many parts of Australia.

CHOICE's study also raised concerns relating to data insecurity, noting RentTech platforms can collect and store more data than traditional methods such as paper forms and online forms hosted by real estate agencies.[644]

The ACCC is aware that some rental application processes may also require prospective tenants to undertake a personality assessment. For example, 10antprofiles advertises a personality assessment product that can be embedded via a link or code directly into the online application process. Applicants then complete the questionnaire, and 10antprofiles provides a report on tenant safety and risk.[645] The 10antprofiles website notes that 'applicant responses are indexed against our proprietary database of tenancy risk indicators' and responses can be used to 'predict future tenant behaviour'.[646]

It is not clear to the ACCC how the collection of this type of consumer data is necessary for the purpose of considering a rental application. However, the ACCC notes that if requested as part of the application process, many consumers may feel they may have little choice but to comply in order to be considered for a property.[647]

Sharing of consumer data with unidentified third parties

The ACCC has observed that the privacy policies of some RentTech platforms facilitate the collection, use and sharing of consumer data with unidentified third parties. For example, analysis of the privacy policies of 2 RentTech platforms used in Australia identified that both facilitate the sharing of consumer data with unidentified third parties. One privacy policy examined states *'You acknowledge and agree that your use of our products and services and your provision of your personal information to us, constitutes your consent, and 'opting-in', to us,* ***or any third parties to whom we provide your personal information****…* [emphasis added] and '***we may share your personal information with other third parties*** [emphasis added] *(including any third parties you may interact with using our services) so that they can contact you directly about their goods or services, or other offers or promotions.*[648]

Similarly, the second privacy policy examined states: [The platform] ***'will discloses [sic] personal information collected by it to organisations such as real estate agents, property owners, utility providers, utility brokers, insurers and insurance brokers, other providers of goods and services, banks and commercial agents*** [emphasis added]. *Personal Information may be disclosed to persons outside Australia.*[649] Issues relating to a lack of meaningful consumer consent, choice and control over who their data may be shared with are discussed further below at section 5.1.3.

Lack of clarity over how data may be used

642 Digital Rights Watch, Submission: Inquiry into the worsening rental crisis, July 2023, accessed 15 March 2024.
643 A Kollmorgen and K Bower, RentTech platforms making renting that much harder, *CHOICE*, 18 April 2023, accessed 15 March 2024.
644 CHOICE, At what cost? The price renters pay to use RentTech, April 2023, p 4.
645 10antprofiles, Introducing objective personality assessments for tenant selection, accessed 15 March 2024.
646 10antprofiles, Introducing objective personality assessments for tenant selection, accessed 15 March 2024.
647 See, for example, CHOICE, At what cost? The price renters pay to use RentTech, April 2023, pp 11–12.
648 Inspect Real Estate, Privacy policy, updated March 2023, accessed 15 March 2024.
649 tApp, Privacy policy, accessed 15 March 2024. The privacy policy notes tAPP [the platform] is a division of Trading Reference Australia Pty Limited (TRA) [the platform's parent company].

The ACCC has observed a lack of clarity over how some of the consumer data provided as part of the rental application process may be used. For example, a 2022 investigation by The Guardian Australia alleged some RentTech platforms use opaque algorithms to make recommendations as to the suitability of a prospective tenant. The Guardian analysed RentTech provider Snug's Match Score, which rates a renter's compatibility with a property as a value out of 100.[650] The Guardian notes that Snug's FAQs disclose a person's Match Score is based on 'property owner preferences, property data, rental application attributes, renter profile completion and market conditions', and that how the score is calculated is mostly invisible to the renter.[651]

University of Technology Sydney researcher Linda Przhedetsky similarly identified a patent application filed by Snug in 2018, which she notes is still active, suggesting that the company's intention was to collect information from users that included friend lists, social media networks and ratings on third-party platforms such as Airbnb and Uber, and to develop a kind of 'rental credit system'.[652] The ACCC considers that the average consumer is likely unaware that this type of information may be collected and used by a RentTech platform for the purpose of assessing a rental application.

Measures to address concerns about data use in the RentTech sector

The ACCC notes that concerns about data use in this sector, including how data is collected, shared and used, may at least be partially addressed through reforms to state and territory residential tenancies legislation.[653]

As discussed in box 2.1, the ACCC considers the collection and use of consumer data in generative AI to be a growing potential source of consumer harm. Many AI technologies rely on enormous amounts of data to train and test algorithms, however it is often unclear whether informed consumer consent was obtained to collect consumer data for these purposes.

The Productivity Commission recently found that while consent frameworks can play an important role in providing consumers a degree of control over their data, the threshold for consent is low and there are questions about its effectiveness – particularly when consumers have few alternatives to accessing services.[654] The Productivity Commission also noted that AI is challenging consent frameworks by incentivising riskier data collection

650 S Convery, Imperfect match: Australian renters in the dark over use of data by tech company Snug, *The Guardian Australia*, 17 November 2022, accessed 15 March 2024.

651 S Convery, Imperfect match: Australian renters in the dark over use of data by tech company Snug, *The Guardian Australia*, 17 November 2022, accessed 15 March 2024.

652 L Przhedetsky, Submission to the Senate Standing Committee on Community Affairs Inquiry into the worsening rental crisis in Australia, 4 September 2023.

653 For example, in September 2023, the Victorian Government announced it would look to reform various aspects of the residential tenancies laws and framework in Victoria, including standardising rental applications, saving renters time and giving them a clear idea of what they can expect to be asked for during the application process, and also limiting the kind of information agents or landlords can keep on file, and how long they can keep it for, better protecting renters' privacy and data. See Victorian Government, Protecting renters' rights, 20 September 2023, accessed 15 March 2024.
The 28 November 2023 report of the Victorian Parliamentary Inquiry into the rental and housing affordability crisis in Victoria also recommended the Victorian Government 'urgently implement' this policy announcement, finding that 'the lack of a standard rental application process has resulted in disparate practices from real estate agencies and third-party RentTech platforms. For some renters, this has meant the over collection of personal information, risking their privacy and data security' (see finding 11). Victorian Legislative Council Legal and Social Issues Committee, The rental and housing affordability crisis in Victoria Inquiry, November 2023, p xxv.

654 Productivity Commission, Making the most of the AI opportunity – Research Paper 3: AI raises the stakes for data policy, January 2024, p 6.

practices and increasing the use of higher-risk data, including instances of sensitive data being web scraped without consumer consent.[655]

5.1.3. Consumer consent

The ACCC remains concerned about the inclusion of vague terms within privacy policies for a wide range of digital and physical products and services which facilitate the provision of, in some cases, arguably 'uninformed' consent for consumer data to be on-sold or provided to other firms for a broad range of uses. Often, the identity of these third parties is not disclosed – instead, they may be referred to in consumer-facing privacy policies using general terms such as 'partners', 'suppliers' or 'affiliates'.[656] This adds an additional layer of complexity for any consumer seeking to understand what data may be shared, who it may be shared with, and how it may be used.

Salinger Privacy provided a case study of an Australian consumer who claimed she received targeted marketing to her home address from a business she had not previously heard of or interacted with. Over a period of 6 months, the consumer claimed she discovered that at least 2 data firms she had also never heard of had collected and shared personal information about her, including her:

- title and full name
- gender
- date of birth
- home street address and phone number
- personal email addresses (one current and one no longer in use)
- 2 pages of 'modelled data' about her, including details about her financial status, employment status, family status and living arrangements.

When she questioned how they had obtained this information, the data firms reportedly responded that she had supplied these details (and consented to their use for direct marketing purposes) when she entered an online competition in 2019.[657]

The ACCC understands that often, the standard terms and conditions provided and agreed to at the time a consumer enters an online competition may broadly refer to the sharing and use of a consumer's data with third parties. However, as discussed below, the ACCC considers consumers are unlikely to either engage with such privacy policies, or fully understand what they are consenting to due to the policies' length and complexity.

Figure 5.3 below indicates the results of a study examining the average time required to read the privacy policies of the most visited websites in the US and globally. The results highlight that the length and complexity of most typical privacy policies would prohibit the average consumer from meaningfully engaging with them.

655 Productivity Commission, Making the most of the AI opportunity – Research Paper 3: AI raises the stakes for data policy, January 2024, p 6.

656 For example, Woolworths' Everyday Rewards privacy policy notes *'we may share some personal information with our Everyday Rewards Partners, suppliers and other third parties'.* While Woolworths' Everyday Rewards website notes the identity of its Everyday Rewards Partners, the identity of 'suppliers and other third parties' appears unclear to the ACCC. See Woolworths, Everyday Rewards and your privacy, accessed 15 March 2024.

657 Salinger Privacy, Submission to the Report, 28 September 2023, pp 14–15.

Figure 5.3: The approximate length and time taken to read an average privacy policy in Australia per month[658]

The above case study provided by Salinger Privacy demonstrates how consumers may find it challenging to identify who holds data on them, as they often do not have a direct relationship with the third-party firms which may have received their data from other sources. Consumers often do not have ready means to identify who these third-party firms receiving their data may be. For example, in 2018 an ABC journalist downloaded her data from Facebook, in an effort to understand how brands targeted her with personalised advertising. She described seeking to understand 'who knows what about you online' as a 'Sisyphean undertaking', which in her case took dozens of emails and almost a month.[659]

The ACCC's Customer Loyalty Schemes Report found an imbalance of bargaining power and significant information asymmetries between consumers and major loyalty schemes examined in the report. These were primarily seen through the broad consents loyalty schemes sought from consumers about the collection and use of their data, and the vague disclosures they made to consumers about how their data could be used, and with which entities it could be shared.[660]

Box 5.3 Measures proposed to address a lack of meaningful consent and control

Privacy Act Review Proposal 12.1 - Collection, use and disclosure of personal information should be fair and reasonable in the circumstances

As discussed in chapter 1, the Privacy Act Review Report proposed amendments to the Privacy Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances, regardless of whether consent has been obtained.[661] This may have future implications for some of the practices discussed in this chapter, including the use of broad terms and conditions contained in some privacy policies that facilitate the collection, sharing and use of consumer data with others for broad purposes not connected with the original purpose the information was provided for.

Prohibition on unfair trading practices

We also note a future prohibition on unfair trading practices may require some firms to ensure their privacy policies are more accessible to consumers, including the use of more straightforward and clear options for obtaining consumer consent for the collection, use and sharing of data, as well as more clearly identifying the identities of other parties who their data may be shared with, and for what purpose.

658 Mi3, Aussies face 10-hour privacy policy marathon, finds study, 6 November 2023, accessed 15 March 2024.
659 A Bogle, I asked everyone from Facebook to data brokers to Stan for my information. It got messy, *ABC News*, 28 April 2018, accessed 15 March 2024.
660 ACCC, Customer Loyalty Schemes – Final Report, December 2019, p vii.
661 Whether something is fair and reasonable should be assessed from the perspective of a reasonable person: Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 8.

5.1.4. Consumers' ability to access or correct data

The ACCC's analysis of some data firms' public-facing privacy policies found they generally include details on how consumers can apply to inspect and correct personal information held about them, as required by the Privacy Act.[662] However, as discussed above, consumer 'consent' for the sharing of their data, often with unidentified third parties, is generally obtained at the point data is provided to the first party, often without the proper understanding of consumers, and without consumers having any means of identifying the additional firms their data may be shared with.

Given these issues, the ACCC considers it unlikely a consumer could meaningfully exercise their existing rights to access and correct any personal information held by some third-party businesses using the contact method(s) set out in these businesses' privacy policies. This is on the basis they are unlikely to be aware that their data was provided to those third parties in the first place.

Additionally, the ACCC notes the right of individuals to inspect and correct data only applies to personal information within the meaning of the Privacy Act, rather than to all categories of consumer data that may be held by a data firm.[663] This means there may be significant amounts of consumer data held and used by data firms that consumers are not entitled to request to access in order to correct any errors that it may contain.

The ACCC understands that the ability of data firms to facilitate and action requests to access or correct data that has been de-identified or pseudonymised may vary, depending on how the data is processed and held. There may be practical and technical reasons why firms are unable to action consumer requests.[664] Nonetheless, there may still be harms arising from the use of such data. For example, harms may still occur from the use of de-identified consumer data used to create certain consumer segments for targeting advertising to a consumer or particular group of consumers.

The serving of targeted ads to a consumer based on this type of profiling may result in general annoyance (such as a person feeling uncomfortable with the level of specific targeting occurring), through to instances of potential greater harm (such as ads for alcohol and tobacco being served to minors or those affected by substance abuse who may be more susceptible to such messaging).

Some examples of potential measures that could be considered to improve consumers' understanding and control over the future use of their data are outlined in box 5.4.

---

662 CoreLogic, CoreLogic Privacy Policy, last updated 2 December 2022, accessed 15 March 2024; Equifax, Privacy Policy (Australia), last updated 30 September 2021, accessed 15 March 2024; Experian, Experian Australia Privacy Policy 2022, last updated December 2022, accessed 15 March 2024; illion, Risk & Marketing Solutions Privacy Policy, last updated March 2023, accessed 15 March 2024; LiveRamp Australia, Privacy Policy, accessed 15 March 2024; Nielsen, Our Privacy Principles, last updated May 2023, accessed 15 March 2024; Oracle Australia, Privacy @ Oracle – Oracle General Privacy Policy, last updated 7 July 2023, accessed 15 March 2024; PropTrack, Privacy policy, accessed 15 March 2024; Quantium, Privacy policy – The Quantium Group, last updated July 2021, accessed 15 March 2024.

663 *Privacy Act 1988* (Cth), s 6; Schedule 1, Part 5 (APPs 12 and 13).

664 For example, in order to allow access and correction or to delete data, a firm may be required to first re-identify previously de-identified information in order to identify the individual. Some submissions to the Privacy Act Review discussed the technical difficulties associated with compliance with consumer access requests – see Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 168.

Box 5.4 Measures proposed to improve consumers' control over future use of their data

Privacy Act Review Proposal 18.3 - Future right to erasure

The Privacy Act Review Report proposed the introduction of a right for an individual to have any of their personal information erased.[665] The government's response indicated in-principle agreement for a requirement that an entity be required to delete (or de-identify) personal information (subject to specific exceptions) following a request from an individual.[666]

This would be supported by Proposal 4.1 of the Privacy Act Review Report, which would clarify the definition of personal information. This proposal is discussed further at section 1.5.2.

Further consideration of an Australian data broker registry

As discussed in chapter 1, several US states have introduced requirements for data brokers meeting specified criteria to register with the state.[667] Californian law goes further, providing a means for consumers to make a single request for the deletion of their data held by all registered data brokers.[668]

The ACCC notes the government could give further consideration to the introduction of a similar registry in Australia, which could provide consumers with a way to:

- submit a 'do not collect' request to all registered entities
- request the deletion of data held about them.[669]

This further consideration could occur alongside consultation on a future right to erasure under the Privacy Act. While additional work would be required to determine the kinds of data firms that would be required to register, such a registry may better enable consumers to exercise their future right of erasure by identifying which firms hold their data and centralising their request.

5.2. Potential harms arising from the use of consumer data

In chapter 3, we discuss the important role that data products and services can play, including their potential benefits for business customers and consumers. However, the ACCC has identified several areas of potential consumer harm stemming from how data firms and their business customers may use consumer data or data products and services.

This section outlines the specific potential harms we have identified. However, we note that survey evidence indicates that consumers view loss of privacy, arising from the sharing or

665 See Proposal 18.3. Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 11.
666 Attorney-General's Department, Government response to the Privacy Act Review Report, 28 September 2023, p 18.
667 See California Civil Code, Title 1.81.48., Privacy: Data brokers [§ 1798.99.80 - 1798.99.88] (2019), accessed 15 March 2024; Vermont General Assembly, Title 9: Commerce and Trade – Chapter 62: Protection of Personal Information, accessed 15 March 2024; Texas Legislature, Texas Data Broker Law: Ch. 509, Data Brokers in Texas Business & Commerce Code (2023), accessed 15 March 2024; Oregon Legislative Assembly, Oregon House Bill 2052: Relating to the registration of business entities that quality as data brokers; and declaring an emergency (2023), accessed 15 March 2024; Delaware House of Representatives, House Bill No. 262 – An Act to amend Title 6 of the Delaware Code Relating to Data Brokers and Consumer Protection (2023), accessed 15 March 2024.
668 California, Senate Bill No. 362, Chapter 709, accessed 15 March 2024, also known as the Delete Act.
669 This suggestion was also made by The App Association. See The App Association, Submission to the Report, 28 September 2023, pp 3–4.

sale of their personal information, *as a harm in and of itself*. As discussed in section 5.1, 74% of consumers feel uncomfortable with the idea of their personal information being shared or sold, and a majority of consumers feel it is unacceptable for businesses they are not in direct contact with to use their data.

The ACCC acknowledges that the likelihood a data product or service may give rise to the specific consumer harms discussed in this section will differ depending on the particular data product or service. This may depend on the form in which the data product or service is provided to a business customer. For example, data products in the form of reports that provide high-level insights about a business' customer base may pose a lower risk of consumer harm than products that can identify or target an individual or groups of consumers.

As previously highlighted in boxes 5.1, 5.3 and 5.4, the ACCC notes some of the potential harms identified in this section may be mitigated by changes to the Privacy Act following the Privacy Act Review. We also note some issues around data use and misuse may be covered by existing provisions of the Australian Consumer Law, or may be capable of being better addressed by a future prohibition on unfair trading practices.

5.2.1. Risks arising from data re-identification

De-identified information has several beneficial uses, including in research and to inform public policy. For example, the OAIC notes that appropriately de-identified information may be made available by a government agency for use by researchers and others outside of the agency to:

- enable better public participation in government processes
- inform policy and program development and design, or
- drive innovation and economic growth by creating new opportunities for commercial enterprise.[670]

However, the ACCC remains concerned about the growing risk of re-identification as datasets are combined and data analytics technologies become more advanced.[671] Multiple studies have identified the relative ease with which some de-identified datasets can be re-identified.[672] One way an individual could be identified within a de-identified dataset is through the combination of that data with additional data points. For example, this could occur as a result of data enrichment (discussed in section 3.2.1), where the data is augmented with additional data from an external source.[673] Examples of data re-identification are discussed in Box 5.5 below. Generally, a greater number of data points on an individual will increase the chances of identifying that person within a dataset.[674]

Data is a non-rivalrous resource, which means it can be collected multiple times by different data firms, increasing the likelihood that de-identified data might be re-identified in the future as a result of its combination with other data sources.

670 OAIC, De-identification and the Privacy Act, 21 March 2023, accessed 15 March 2024.
671 ACCC, Digital Platforms Inquiry Final Report, June 2019, p 36.
672 J Sherman, Big data may not know your name. But it knows everything else, 19 December 2021, accessed 15 March 2024.
673 The OAIC notes that once a customer dataset is returned to a data product or service user following a data enrichment process, any newly created inferences in relation to a particular individual's characteristics, behaviours or preferences, or information that has been appended to a customer profile, will likely constitute a new collection of personal information for the purposes of APP 3. See OAIC, Submission to the Report, 28 September 2023, p 10.
674 This is because the likelihood of multiple individuals all having the exact same preferences or demographic characteristics now expressed in that dataset declines as additional data points are introduced.

Box 5.5 Examples of data re-identification

The below examples illustrate instances where datasets previously considered to be de-identified were re-identified when combined with additional data from other sources.

- In August 2016, the federal Department of Health published the de-identified longitudinal medical billing records of a sample of 10% of Australians. For each selected patient, all medical and pharmaceutical bills reimbursed under Medicare for the years 1984 to 2014 were included. Despite supplier and patient IDs, patients' years of birth and genders being encrypted, researchers from the University of Melbourne were able to decrypt the IDs of Medicare service providers and discovered patients could be re-identified by linking this unencrypted data with known information about those individuals obtained from public sources.[675] The researchers found linking public information with other information about individuals, such as dates of childbirth, could lead to easy re-identification of individuals.
- In 2018, Public Transport Victoria released what it considered to be de-identified data from Melbourne's contactless smart card ticketing system, known as Myki, as part of the 2018 Melbourne Datathon. The dataset consisted of nearly 2 billion rows of 'touch on' and 'touch off' events for Myki smart cards used on public transport between mid-2015 and mid-2018.[676] Shortly after this dataset's release, researchers from the University of Melbourne raised concerns of re-identification risks after it emerged that anyone with access to the dataset could re-identify themselves and others by linking entries in the dataset with publicly available information about people's travel patterns.[677] Most people in the dataset could be identified from just a handful of 'touch on' or 'touch off' events. Further information like people's home and work locations, regular patterns and times of travel could be revealed by further analysing the dataset.[678]
- In 2006, Netflix released over 100 million movie ratings from almost 500,000 randomly selected customers as part of a competition to improve its recommendation system.[679] Netflix claimed that all personally identifiable information had been removed from the dataset. However, researchers from the Massachusetts Institute of Technology compared the Netflix dataset against public reviews on Amazon's Internet Movie Database (IMDb) website, to test whether reidentification of Netflix users in the dataset was possible.[680] Researchers found they could uncover the identity of the Netflix reviewers using their corresponding Amazon accounts.[681]

675 C Culnane, B Rubinstein and V Teague, Health Data in an open world, a Report on Re-Identifying Patients in the MBS/PBS Dataset and the Implications for future releases of Australian Government Data, *The University of Melbourne*, 18 December 2017, p 9; OAIC, MBS/PBS Data Publication, 23 March 2018, accessed 15 March 2024.

676 C Culnane, B Rubinstein and V Teague, Two data points enough to spot you in open transport records, *University of Melbourne,* 15 August 2019, accessed 15 March 2024.

677 Office of the Victorian Information Commissioner, Disclosure of myki travel information, Investigation under s 8C(2)(e) Myki of the *Privacy and Data Protection Act 2014* (Vic), 15 August 2019, p 13, accessed 15 March 2024.

678 C Culnane, B Rubinstein and V Teague, Two data points enough to spot you in open transport records, *University of Melbourne*, 15 August 2019, accessed 15 March 2024.

679 M Archie, S Gershon, A Katcoff and A Zeng, Who's watching? De-anonymisation of Netflix Reviews using Amazon Reviews, Massachusetts Institute of Technology Project, 2018, p 1.

680 M Archie, S Gershon, A Katcoff and A Zeng, Who's watching? De-anonymisation of Netflix Reviews using Amazon Reviews, Massachusetts Institute of Technology Project, 2018, p 2. The researchers compared reviews submitted to Netflix and Amazon that were an exact match (the same review submitted on the same date for the same movie), as well as matching similar reviews (analysed using a similarity score) to identify matches and link Netflix accounts with Amazon accounts.

681 M Archie, S Gershon, A Katcoff and A Zeng, Who's watching? De-anonymisation of Netflix Reviews using Amazon Reviews, Massachusetts Institute of Technology Project, 2018, p 5. The researchers note some users may not realise how public their Amazon profiles are or the amount of information Amazon reveals.

In 2014, following a freedom of information request, the New York City Taxi and Limousine Commission (TLC) released data on the locations, times, fares and tips paid for over 173 million taxi trips taken in the city in 2013.[682] TLC had sought to anonymise this data by replacing every taxi and driver combination with a unique hashed code, but a computer scientist was able to reverse this in under 2 hours with the help of other publicly available information.[683] In addition, a blogger was able to combine this data with other public information to map specific trips made by actors Bradley Cooper and Jessica Alba, and infer the names and home addresses of frequent visitors to a well-known strip club.[684]

The ACCC understands that some data firms include a prohibition on the re-identification of data as part of the standard terms and conditions governing the supply of their data products and services to business customers. While we note the existence of such measures, the UK Information Commissioner's Office has observed that in practice, once data is out of the hands of one party, generally that party has little or no way to guarantee that the data will remain subject to appropriate protection and controls.[685]

5.2.2. Identification and targeting of vulnerable consumers

As discussed in chapter 3, many data firms supply customer segments for use in targeted advertising. These segments can provide a means for advertisers to reach relevant audiences in an efficient way. However, the ACCC notes there is a risk that certain consumer segments could be used to target vulnerable groups in potentially harmful ways, including through the delivery of certain content, such as scam messages.

Box 5.6 provides examples of consumer segments identifying groups of consumers that, depending on the context, could be considered vulnerable groups capable of being targeted in potentially inappropriate or harmful ways.

These examples are intended to illustrate the types of consumer segments available and are not intended to signal particular concern on the part of the ACCC about the conduct of Microsoft. Microsoft has previously made public statements that the Xandr dataset was inadvertently published on its website, and that it was outdated and has since been removed. Microsoft also notes that Xandr's data privacy policies are regularly evaluated to ensure compliance with applicable data protection laws.[686]

682 A Hern, New York taxi details can be extracted from anonymised data, researchers say, *The Guardian,* 28 June 2014, accessed 15 March 2024.

683 A Hern, New York taxi details can be extracted from anonymised data, researchers say, *The Guardian,* 28 June 2014, accessed 15 March 2024. Other publicly available information the computer scientist used included the possible formats of driver licence and taxi numbers, totalling around 24 million possible combinations that his computer un-hashed within minutes. He also ran a 'quick Google search' and found TLC resources mapping driver licences and taxi numbers to driver names.

684 A Tockar, Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset, 15 September 2014, accessed 15 March 2024.

685 UK ICO, Update report into ad tech and real time bidding, 20 June 2019, pp 20–21.

686 A Bogle, 'Heavy TAB gamblers' among groups targeted by online advertising database, *The Guardian Australia*, 15 August 2023, accessed 15 March 2024.

Box 5.6 Examples of consumer segments capable of identifying vulnerable consumer groups

In August 2023, a dataset containing 650,000 Australian and international customer segments was discovered on the website of Microsoft's advertising technology platform Xandr.[687]

Reset.Tech Australia analysed this dataset, and its submission to this Report highlights a number of what it considers to be 'especially concerning themes' within the dataset. These include lists of consumers who Reset.Tech Australia considers may be experiencing vulnerabilities capable of being exploited, such as:

- children, teenage girls and teenage boys
- indigenous Australians
- religious minorities
- unemployed people
- elderly people living alone
- people experiencing financial difficulties and distress
- people deemed 'financially unsavvy'
- new migrants
- people using browsers in other languages
- people with low education
- people experiencing pain or who have visited certain medical facilities.[688]

The ACCC notes Microsoft's explanation that this dataset is no longer being used. The ACCC also considers it important to illustrate, as per the Xandr dataset, the types of consumer segments that may be used by data firms.

We note that while customer segments made available by other data firms may use slightly different language to describe their segments to those illustrated above, we have observed other customer segments could potentially be used to reach a similar audience. For example, segments identifying groups as 'culturally diverse' could be used in a similar way to Xandr's 'new migrants' and 'people using browsers in other languages' segments to identify and target consumers who may have lower English skills.

Gambling segments

Reset.Tech Australia's analysis of the Xandr dataset also identified a number of customer segments capable of targeting advertising to consumers for gambling products and services. For example, its submission identifies more than 40 Australian customer segments relating to frequent gamblers, including:

- 'Casino frequenters'
- 'People who have gambled in the last 7 days'
- 'People who have gambled in the last 4 weeks'

687 A Bogle, 'Heavy TAB gamblers' among groups targeted by online advertising database, *The Guardian Australia*, 15 August 2023, accessed 15 March 2024.
688 Reset.Tech Australia, Submission to the Report, 28 September 2023, p 5.

- 'People who have gambled in the last 3 months'[689]

Such customer segments capable of facilitating targeted advertising for gambling products and services to certain individuals and groups of consumers may be especially problematic. Research highlights that frequent gamblers are at an increased risk of being harmed by gambling ads,[690] while the use of consumer data to facilitate targeted advertising may amplify online gambling harms.[691]

The ACCC notes that the use of customer segments for the purpose of targeting adverting of gambling products may be phased out if proposed a ban on gambling advertisements in Australia is introduced. A June 2023 report by the House of Representatives Standing Committee on Social Policy and Legal Affairs recommended that 'a phased, comprehensive ban on all gambling advertising on all media – broadcast and online, that leaves no room for circumvention, is needed.'[692]

In addition to the use of particular consumer segments for the purpose of online targeted advertising, there are other ways in which data products and services could be used by individuals or businesses to identify and target vulnerable consumers. For example, it was recently reported that data from Valuation NSW had been sold to third parties who reportedly matched it to court lists for people involved in divorce, repossession or family law proceedings. These matched lists were then used to target emotionally or financially distressed individuals to sell their homes for below-market prices.[693]

Collection, sharing and use of children's data by data firms

The ACCC remains concerned that excessive tracking, collection and use of data can lead to increased risks for vulnerable consumers and children who may be more easily identified and targeted.[694] The government's response to the Privacy Act Review Report acknowledges that children increasingly rely on online platforms, social media, mobile applications and other internet-connected devices in their everyday lives.[695]

While these services provide many benefits to children and young people, there is concern that children are increasingly being 'datafied', with thousands of data points being collected about them, including information about their activities, location, gender, interests, hobbies, moods, mental health and relationship status.[696] While this practice is not unique to children, there are concerns that this information can be used to build profiles on children and to identify moments when they are particularly vulnerable in order to more effectively target and engage them. Some stakeholders to the Privacy Act Review raised concerns that this information could be used to engage in harmful forms of targeted advertising to children,

689 Reset.Tech Australia, Australians for sale: targeted advertising, data brokering and consumer manipulation, December 2023, p 14.
690 A Bogle, 'Heavy TAB gamblers' among groups targeted by online advertising database, *The Guardian Australia,* 15 August 2023, accessed 15 March 2024.
691 OAIC, House of Representatives Standing Committee on Social Policy and Legal Affairs – Inquiry into online gambling and its impacts on those experiencing gambling harm: Submission by the Office of the Australian Information Commissioner, 24 February 2023, p 1.
692 Parliament of Australia, You win some, you lose more: online gambling and its impacts on those experiencing gambling harm, June 2023, p iv.
693 E Linder, Property data allowing distressed owners to be targeted, *The Canberra Times*, 27 October 2023, accessed 15 March 2024. See also ACCC, Dominique Grubisa and DG Institute in court for alleged misleading representations, 16 December 2022, accessed 15 March 2024: In December 2022, the ACCC commenced proceedings against Master Wealth Control Limited (trading as DG Institute) for allegedly making false or misleading representations about its Real Estate Rescue program and Master Wealth Control program, in breach of the Australian Consumer Law. The ACCC action does not cover the use or misuse of data itself; rather, it is focused on alleged misrepresentations relating to the strategy taught in the program.
694 ACCC, Digital Platform Services Inquiry – Interim Report No. 5 – Regulatory Reform, 11 November 2022, p 65.
695 Attorney-General's Department, Government response to the Privacy Act Review Report, 28 September 2023, p 13.
696 Attorney-General's Department, Government response to the Privacy Act Review Report, 28 September 2023, p 13.

including marketing that can promote unhealthy or harmful products, or produce psychological or mental health changes such as negative body image.[697]

The ACCC understands that some data firms currently have mechanisms in place to prevent the use of data from consumers known to be under 18 years old in their products and services. However, these preventative measures are only useful where the age of a person can be verified. The collection, sharing and use by and between data firms of personal information or other information about persons aged under 18, may sometimes occur due to an individual having provided a fake date of birth at the time their information was collected.[698] Many stakeholders have previously raised concerns that introducing age verification technology to address this practice may negatively impact users' privacy.[699]

The ACCC considers that as new technologies emerge, including those involving the use of artificial intelligence, future age verification measures may negate the need for users to disclose or provide additional personal information to a business directly in order to verify their age. For example, it is possible that identification verification services, such as those offered by firms accredited under the Trusted Digital Identity Framework (and later the proposed Digital ID Bill), could be used for this purpose. As discussed in chapter 3, the accreditation framework ensures all identity providers meet strict rules and standards for usability, access, privacy protection, security, risk management and fraud control.

Box 5.7 Measures proposed to protect children's data

Privacy Act Review Proposal 20.7 – Prohibition on the trading of personal information about children

To address some of the concerns raised regarding the collection and use of children's data, in its response to the Privacy Act Review Report, the government agreed in-principle to prohibit the trading of personal information about children[700] and targeted advertising to children.[701] To support these additional protections, and to provide further guidance on how entities are expected to meet new requirements, the government has agreed to develop a Children's Online Privacy code to provide additional protections for children.[702]

5.2.3. Potential for discrimination and exclusion

In the original Digital Platforms Inquiry, the ACCC found that increased data collection enables more detailed targeting of individual consumers. This increases the likelihood and magnitude of consumer harm resulting from risks associated with discriminatory or exclusionary targeting. The Digital Platforms Inquiry noted that these risks are exacerbated

697 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 146.
698 This was also discussed in the ACCC's Social Media Report, where the ACCC acknowledged that the majority of instances where underage people are exposed to advertising of age-restricted products on social media platforms likely occurs as a result of circumvention of the platforms' age verification processes. ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, p 154.
699 ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, p 154.
700 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 13 (see proposal 20.7); Australian Government, Government Response – Privacy Act Review Report, 28 September 2023, p 13.
701 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 12 (see proposal 20.6); Australian Government, Government Response – Privacy Act Review Report, 28 September 2023, p 13. The proposal to prohibit targeted advertising to children includes an exception for targeting that is in the best interests of the child.
702 Attorney-General's Department, Privacy Act Review Report, 16 February 2023, p 10 (see proposal 16.5); Australian Government, Government Response – Privacy Act Review Report, 28 September 2023, p 13.

by the opacity of information provided to consumers about how their data is, or may be, used and who it may be shared with.[703]

Some stakeholders raised concerns that data firms and their customers could use consumer data to discriminate in how they offer products or services to consumers.[704] Reset.Tech Australia notes the prices a consumer is offered for products and services online may be calibrated by reference to various known or inferred demographic and behavioural factors about them. This can create an information asymmetry between the seller and consumer, which Reset.Tech Australia considers can unfairly prejudice the consumer.[705]

5.2.4. Reliance on incorrect or incomplete data

The Australian Communications Consumer Action Network notes that data obtained from a third party is not always complete or accurate, and entities that rely on this data may make incorrect decisions based on flawed data.[706] Equifax submits that an obligation of the data brokerage process is to enrich, cleanse and analyse consumer profiles before licensing or selling them to third parties. It acknowledges, however, that consumer harms may arise when individual profiles are inaccurate or incomplete, leading to inaccurate profiling, or consumers being excluded from product or service offerings.[707]

Equifax points to an effective corrections and complaints process as necessary to ensure the data that a business obtains, holds and uses is up to date.[708] However, as discussed at section 5.1.4, many consumers may be unaware that third parties collect and use their data in the first place, limiting their ability to access and correct any errors in the data held on them.

5.2.5. Use of consumer data to facilitate scams and fraud

The ACCC notes the risk that some data products and services may be misused by bad actors to facilitate scams or fraud. While data products and services do not themselves necessarily create new categories of scams or fraud, their use may exacerbate existing risks if they are used to identify individuals or groups of consumers who may be more vulnerable to scams or fraud activity. Access to additional information on an individual can also increase a scammer's ability to impersonate that individual or impersonate an entity that the individual deals with, to further a scam.

The ACCC is not suggesting that data firms make data available to scammers for this purpose. Rather, we note that this information may be obtained by scammers as a result of a data breach or other data security incident, or as a result of data being sold or acquired without sufficient due diligence. Data security and data breaches are discussed further at section 5.2.7.

In 2023, the US Consumer Financial Protection Bureau highlighted the risks of data brokers' products being used to facilitate scams, harassment and fraud.[709] Box 5.8 provides an example of this from the US. In Australia, there appear to be few or no vetting mechanisms on the purchase of large amounts of potentially vulnerable consumer data. This presents a

703 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 447.
704 CHOICE, Submission to the Report, 28 September 2023, p 5; ACCAN, Submission to the Report, 28 September 2023, p 4; CPRC, Submission to the Report, 28 September 2023, p 4.
705 Reset.Tech Australia, Submission to the Report, 28 September 2023, p 6.
706 ACCAN, Submission to the Report, 28 September 2023, p 3.
707 Equifax, Submission to the Report, 28 September 2023, p 21.
708 Equifax, Submission to the Report, 28 September 2023, p 21.
709 CFPB, Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices, 15 August 2023, accessed 15 March 2024; CPRC, Submission to the Report, 28 September 2023, p 5.

potential avenue for scammers' misuse of data sold by data firms. Several submissions also raise concerns that data products and services can facilitate, or contribute to risks of, scams and fraud activity in Australia.[710]

Box 5.8 Use of data broker products to facilitate fraud against the elderly

In January 2021, data broker Epsilon entered into a US$150 million settlement with the US Department of Justice after it was found to have facilitated fraud schemes targeting elderly consumers by selling modelled lists of American consumers whom it had identified as likely to be susceptible to such schemes.[711]

The lists were sold to clients whom Epsilon staff knew had been arrested, charged, and in some cases, convicted of offences relating to false and misleading conduct. These business customers used the lists to engage in mass-mailing fraud schemes that sent false sweepstakes and astrology solicitations to consumers, promising them non-existent cash prizes or individualised psychic services in exchange for a fee.[712]

The ACCC notes that while Epsilon also has a presence in Australia, we are not suggesting it has engaged in similar conduct here.

Existing measures to protect against scams, fraud and data misuse

As discussed in chapter 3, the ACCC acknowledges that some data firms also provide data verification and fraud detection services. These are useful tools to assist in the detection of scam and fraud activity by confirming the authenticity or reliability of information provided, and to assess and mitigate the risk of fraud occurring. This includes the ability to use data to identify potential scam activity in real time.[713]

The ACCC understands that many data firms have in place various controls to protect consumer data against improper access and use by their employees, as well as from improper use by business customers. We also understand many data firms include terms and conditions in their standard supply agreements governing the use of their data products and services by business customers, including prohibitions on re-identifying or modifying the data provided.

5.2.6. Misuse of location data

As noted in the original Digital Platforms Inquiry, the increase in personal mobile devices such as smartphones and the improvement in location-tracking technology has led to an increase in the amount of location data collected and used.[714] Location data can be collected or inferred from a wide variety of sources, including GPS, IP addresses and

710 See, for example, CHOICE, Submission to the Report, 28 September 2023, p 5. Some submissions noted that data breaches can increase consumers' susceptibility to scams – see OAIC, Submission to the Report, 28 September 2023, p 4 and ACCAN, Submission to the Report, 28 September 2023, p 3.

711 United States Department of Justice, Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes, 27 January 2021, accessed 15 March 2024.

712 United States Department of Justice, Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes, 27 January 2021, accessed 15 March 2024.

713 For example, in October 2023 it was reported that the Commonwealth Bank had switched on its 'scam indicator', developed in partnership with Quantium Telstra, a joint venture between Telstra and Quantium. This followed a successful pilot program which used algorithms to spot potential scam phone calls in real-time by matching two sets of data to identify when a customer was simultaneously on the phone and attempting to transfer funds, suggesting they may be in the process of being scammed. K Weber, CBA and Telstra 'scam indicator' feature officially switched on, 30 October 2023, accessed 15 March 2024.

714 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 385.

information from Wi-Fi access points, mobile towers and Bluetooth-enabled devices.[715] As discussed in chapter 3, location data is an input into a number of data products and services supplied in Australia.

Box 5.9 below provides an example of the alleged misuse of location data by a US data broker to build comprehensive consumer profiles, including using data based on sensitive locations consumers may have visited. In this particular example, the issue is not that this location data was collected and used, but that this allegedly occurred without consumer consent. This example illustrates the ways in which data firms may use location data as an input to their data products and services, including to create consumer segments for the purpose of targeted advertising.

As discussed in section 5.1.3, consumers may often consent to the collection and use of their data without being fully aware this practice is occurring. The ACCC has observed that location data on Australians may be similarly collected and used for a variety of purposes,[716] including for targeted advertising.[717]

Box 5.9 Case study – US FTC complaint against data broker Kochava's collection and use of consumer location data

As discussed in chapter 1, in June 2023 the US Fair Trade Commission (FTC) re-filed its complaint against data broker Kochava, alleging that Kochava had collected and used precise geolocation data without consent. The FTC alleges Kochava secretly collects and sells its 'Kochava Collective' data, which includes precise geolocation data, comprehensive profiles of individual consumers, consumers' mobile app use details and Kochava's 'audience segments'.[718]

The FTC alleges Kochava can connect consumers' mobile advertising IDs (MAIDs) with their precise geolocation data as well as names, email addresses, phone numbers, email addresses and other identifying information.[719] This combined data can reveal precise and sensitive information about a person, such as visits to hospitals, reproductive health clinics, places of religious worship, homeless and domestic violence shelters and addiction recovery facilities. In addition to targeted advertising, the FTC's case alleges that in making this information available for sale, Kochava is 'enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence'.[720]

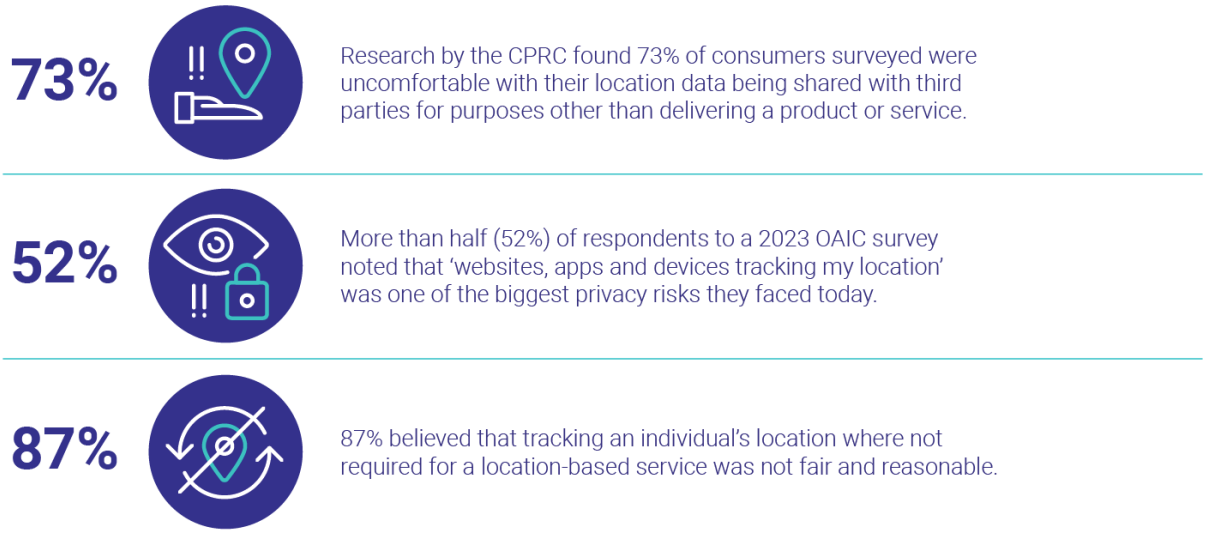
The FTC notes Kochava acquires data in two ways – through the use of Kochava-supplied software development kits (SDK) installed in over 10,000 mobile apps globally, as well as directly from other data brokers. The FTC alleges Kochava's SDKs collect data and provide it back to Kochava without the consumer being told, or consenting to their data being collected.[721]

715 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 385.
716 For example, in response to a case brought by the ACCC, in April 2021 the Federal Court found that Google LLC and Google Australia Pty Ltd misled consumers about personal location data collected through Android mobile devices between January 2017 and December 2018. Google was found to have not disclosed that consumers' location data may be used by Google for a number of purposes, unrelated to the consumer's use of Google services. ACCC, Google misled consumers about the collection and use of location data, 16 April 2021, accessed 15 March 2024.
717 For example, Google's Privacy Policy includes detail on how Google uses location information, including 'to show you more relevant ads.' Google, Privacy & Terms, accessed 15 March 2024.
718 FTC, FTC v Kochava, Inc, updated 5 February 2024, accessed 15 March 2024.
719 FTC, Amended Complaint for permanent injunction and other relief: Case No. 2:22-cv-00377-BLW, 5 June 2023, accessed 15 March 2024, p 16.
720 A Toomey McKenna, Data brokers know everything about you – what FTC case against ad tech giant Kochava reveals, *The Conversation*, 13 January 2024, accessed 15 March 2024.
721 FTC, FTC v Kochava, Inc, updated 6 November 2023, accessed 15 March 2024.

While the ACCC has found evidence to suggest Kochava provides some services to the Australian market,[722] we are not alleging it has similarly engaged in the collection of geolocation data without consent in Australia, as alleged by the FTC in the US. However, given the FTC's complaint alleges Kochava's SDKs were installed in over 10,000 apps globally, it is likely some of these apps have been accessed by Australian consumers.

Some stakeholders have raised concerns regarding the use of consumers' location data.[723] Figure 5.4 below sets out consumer views from recent surveys conducted by OAIC and the CPRC relating to the sharing of location data.

Figure 5.4: Consumer concerns regarding the collection and use of their location data[724]



Box 5.10 below identifies proposals from the Privacy Act Review Report that may have future bearing on the way in which data firms collect and use location data.

722 For example, Kochava's website notes McDonalds Australia enlisted the help of Kochava to assess the impact of a customised campaign strategy in the MyMacca's app. The strategy refers to a multi-media campaign Spotify ran for McDonalds, using targeted audience segments based on custom behavioural analysis. Kochava analysed the campaign impressions data and activity data from the MyMacca's app. See Kochava, Learn how Kochava assessed the incremental lift impact of Spotify's multi-media campaign for McDonald's MyMacca's Rewards app (post), LinkedIn, accessed 15 March 2024.

723 CHOICE, Submission to the Report, 28 September 2023, p 5; Salinger Privacy, Submission to the Report, 28 September 2023, p 7. Also, in the US, some examples have arisen of consumer harm from the use of location data. See NBC News, Priest outed via Grindr app highlights rampant data tracking, 23 July 2021, accessed 15 March 2024; J Cox, Data broker is selling location data of people who visited abortion clinics, VICE, 4 May 2022, accessed 15 March 2024.

724 CPRC, 2020 Data and Technology Consumer Survey, 7 December 2020, accessed 15 March 2024; OAIC, Australian Community Attitudes to Privacy Survey, August 2023, pp 23, 52.

Box 5.10 Measures proposed to address the collection and use of location data

Privacy Act Review Proposal 4.10 – Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent

The ACCC has previously recommended the definition of personal information under the Privacy Act be amended to clarify that it captures technical data such as IP addresses, device identifiers and location data.[725] In its response to the Privacy Act Review, the government agreed in-principle that collection, use, disclosure and storage of precise geolocation tracking data is a practice which should require consent, and said it will consider further whether this should be included as a new sub-category of sensitive information.[726]

Privacy Act Review proposal 4.1 – Change the word 'about' to 'relates to' in the definition of personal information

The ACCC notes the government agreed in-principle to change the word 'about' in the definition of personal information to 'relates to' to clarify that personal information is an expansive concept that includes technical and inferred information (such as IP addresses and device identifiers). This in-principle agreement extends to the inclusion of a non-exhaustive list of information that may be considered personal information under the Privacy Act, including the proposed inclusion of an identification number, online identifier or pseudonym.[727] Proposal 4.1, including its potential implications beyond location data, is discussed further in chapter 1.

The ACCC notes the above future changes to the Privacy Act may impact the current business practices of some data firms, resulting in increased alignment with consumer expectations as to how their location data may be collected and used.

5.2.7. Data security and data breaches

As discussed in chapters 2 and 3, businesses which supply data products and services typically collect large volumes of data on consumers. The Australian Communications Consumer Action Network submits that the scale of this collection creates a significant risk of security breaches.[728] Similarly, the CPRC submits that the risks of identity theft and fraud may be exacerbated in the case of data brokers or other businesses who retain large amounts of sensitive personal information.[729] An individual's risk of having their data compromised increases as it is shared with and stored by additional firms.

As highlighted by recent high-profile data breaches experienced by Medibank and Optus, the incidence of data breaches is a prevalent issue that can lead to consumer detriment. A study by US academics Cheong, Wang and Sokol examined 470 firms and found that 10% had experienced at least one instance of 'customer privacy information leakage' between 2016 and 2021.[730] In Australia, the OAIC was notified of 890 data breaches under the Notifiable Data Breaches scheme in the 2023 calendar year.[731] There was a 19% increase in the

725 ACCC, Digital Platforms Inquiry – Final Report, 26 July 2019, p 34 (see Recommendation 16(a)).
726 Australian Government, Government Response – Privacy Act Review Report, 28 September 2023, p 6.
727 Australian Government, Government Response – Privacy Act Review Report, 28 September 2023, p 5.
728 ACCAN, Submission to the Report, 28 September 2023, p 3. See also J Sherman, Data brokers and data breaches, 27 September 2022, accessed 15 March 2024.
729 CPRC, Submission to the Report, 28 September 2023, p 5.
730 A Cheong, T Wang and D Sokol, Submission to the Report, 28 September 2023, pp 4, 18–20.
731 OAIC, Notifiable data breaches report July to December 2023, 22 February 2024, p 7.

number of notifications for the July-December 2023 period compared to January–June 2023.[732]

In the July-December 2023 period, contact and identity information were the most common kinds of personal information involved in data breaches (88%). This includes information such as an individual's name, home address, phone number and email address. Identity information, comprising information to confirm an individual's identity such as date of birth, passport details and other government identifiers, was exposed in 63% of breaches for the period.[733]

According to a 2023 OAIC survey, 3 in 4 Australians who had been involved in a data breach said they experienced some form of harm as a result.[734] The types of harm consumers may experience include financial harm, emotional distress or humiliation, harassment, and a loss of trust in businesses seeking to collect their data in future.[735] They may also face higher risks of being targeted by scams, fraud and identity theft[736] and damage to reputation and relationships.[737] There can also be significant time and money costs to consumers who are required to update and replace identification documents following a data breach.[738]

Data breaches may also exacerbate some of the other issues identified in this chapter. For example, a data breach could result in the loss of de-identified data rather than personal information. While these types of data breaches may not be notifiable under the Privacy Act, we note the release of this data may still result in consumer harm. This is because, once released, data that has been de-identified in one context may be capable of being re-identified when combined with other data sources.[739] This risk of data re-identification is discussed in more detail in section 5.2.1.

Furthermore, consumers may simply be unaware that they have been affected by a data breach. As identified in section 5.1.3, consumers may be unaware of which data firms their data has been shared with and what data may be held. In such circumstances, a consumer will generally lack the ability to limit or rectify the harm they suffer if that business experiences a data breach.[740] This is echoed in a recent report on notifiable data breaches by the OAIC, which highlights the risk of outsourcing personal information handling to third parties.[741] The ACCC considers that in many cases, affected individuals may have been unaware that these third parties held their data (that is, if they had not been notified as a result of the notifiable data breach contact requirements).

732 OAIC, Notifiable data breaches report July to December 2023, 22 February 2024, p 3.
733 OAIC, Notifiable data breaches report July to December 2023, 22 February 2024, p 12.
734 OAIC, Australian Community Attitudes to Privacy Survey, August 2023, p 54.
735 CHOICE, Submission to the Report, 28 September 2023, pp 5–6; OAIC, Submission to the Report, 28 September 2023, p 4.
736 OAIC, Submission to the Report, 28 September 2023, p 4.
737 OAIC, Submission to the Report, 28 September 2023, p 4.
738 For example, following the 2022 Optus data breach, many consumers were required to replace their driver's licence, passport and Medicare card. While Optus would bear the costs of replacing passports and driver's licences, affected consumers were often required to attend a state government service centre in-person to request a new driver's licence. There were reports of consumers having to travel significant distances to attend a centre in person, where they were faced with lengthy queues. J Lim, Optus data leak victims face long queues to change drivers licence numbers at Service SA locations, *ABC News*, 28 September 2022, accessed 15 March 2024.
739 OAIC, Submission to the Report, 28 September 2023, p 4.
740 CPRC, Submission to the Report, 28 September 2023, p 9; UNSW Allens Hub (K Kemp and G Greenleaf), Submission to the Report, 28 September 2023, pp 7-8.
741 OAIC, Data breach report highlights supply chain risks, 22 February 2024, accessed 15 March 2024.

6. Market dynamics

Key observations

- The ACCC is concerned about potential practices that seek to restrict data access between data firms, and that may have the effect of foreclosing rivals in downstream markets.
- There is competitive tension between data firms and digital platforms that provide products or services related to online advertising.
- There are tensions between promoting competition in data markets (such as through facilitating data sharing) and promoting improved privacy outcomes for consumers.
- Data firms specialise in servicing different business functions or industry sectors, based on their access to data and knowledge.
- Data firms may compete with one another through non-price factors, including product differentiation, privacy and data security, and quality and scope of data and analysis.
- Many business customers of data firms examined in this report rely on more than one data firm, either combining similar products or relying on specialised knowledge of multiple data firms in different industries or business functions.
- Several large merger and acquisition activities involving data firms have focussed on obtaining access to data and analytical tools.

This chapter explores, in broad terms, the market dynamics between data firms which provide products and services to Australian businesses. It sets out the ACCC's observations of these market dynamics, based primarily on the 9 sample firms considered in this Report.

- **Section 6.1** examines the ways in which data firms specialise by focussing their products or services towards industry sectors or by fulfilling the requirements of a business function.
- **Section 6.2** examines the ways in which data firms compete to provide products, focussing on product specialisation, privacy and data security practices, and quality and scope of data and analysis.
- **Section 6.3** examines the approach that some business customers take in engaging multiple data firms to meet their data analytics needs (referred to as a 'multi-firm approach').
- **Section 6.4** examines trends in merger and acquisition activity involving data firms.
- **Section 6.5** examines a potential competition concern relating to vertical foreclosure in downstream markets because of restricted access to data.
- **Section 6.6** examines the ways digital platforms compete with data firms when providing products or services oriented towards online advertising.
- **Section 6.7** examines the potential alignment, or tension, between competition policy and privacy regulation objectives in relation to data firms.

As the ACCC has only identified a *potential* competition concern between data firms, this chapter does not seek to specifically define any market(s) in which data firms operate, nor to arrive at a conclusion about the market power of any individual firm(s).

6.1. Data firm specialisation

6.1.1. Industry sector or business function specialisation

The data products and services that data firms offer to business customers are marketed towards:

- meeting broad demands of an **industry sector** (and as such, data firms may offer products and services to meet multiple business functions within that sector), or
- meeting the demands of **business functions** (or specific tasks) of various business customers operating in a variety of industry sectors.

For further discussion of the industry sectors that data firms and their customers operate in, see section 4.3. See figure 4.2 in section 4.1 for information on which sample firms operate in which industry sectors.

Industry sector specialisation

Data firms may expand from an initial specialised product or service to a product range that fulfils a variety of functions common to an industry sector. For example, CoreLogic's initial product offering was an automated valuation model (AVM) for property.[742] Over time, CoreLogic expanded its product offering, including through acquisition. In 2011, CoreLogic acquired RP Data, which offers tools to real estate professionals for comparative analysis of property values.[743] More recently, CoreLogic's product offering has further expanded to a range of property-focussed data analytics products, including lead generation products for real estate agents and property-related risk management tools.[744]

Business function specialisation

Data firms may also expand from providing one business function to adjacent functions that are relevant to a range of industries. For example, Nielsen has a history of providing products and services related to market research.[745] It now offers products and services for a range of online advertising functions, such as audience measurement products aimed at improving advertising campaign effectiveness.[746] Nielsen's products and services can be used by business customers in a wide range of industry sectors.

742 TA, First American Core Logic, accessed 15 March 2024.
743 AAP, RP Data makes a stellar debut, *Sydney Morning Herald*, 16 December 2006, accessed 15 March 2024.
744 CoreLogic, Unlock market insights to power your business, accessed 15 March 2024.
745 Nielsen, Celebrating 95 Years of Innovation, accessed 15 March 2024.
746 Nielsen, Solutions: Media Planning, accessed 15 March 2024.

6.1.2. The role of historical expertise and first-party proprietary data

The role of historical expertise in obtaining datasets

When a data firm expands its products or services within its historical industry sector or type of business function, it can rely on its own historical datasets or information it obtains from its business customers. Data firms employ these historical datasets to produce and market a variety of new products or services. For example, PropTrack advertises property data 'covering a 45-year period… including current and historical property listings, historical sale and rental transactions data.'[747]

Access to industry- or business function-specific data can also be achieved through mergers and acquisitions. For further discussion of merger and acquisition activity involving data firms, see section 6.4.

First-party proprietary data

Some data firms invest in accessing **first-party proprietary data**, that:

- is sourced from a business or entity with a direct connection to consumers (who are usually the subjects of the dataset)
- is sourced on commercial terms
- provides enhanced or specialised insights
- is not otherwise available from other data suppliers.

[747] PropTrack, Submission to the Report, 28 September 2023, p 3.

Box 6.1 First-party proprietary data

'First-party proprietary data' combines the concepts of first-party data (being data sourced from an entity with a direct connection to consumers), and proprietary data (data generated by a firm such as a business and made available on commercial terms). Some characteristics of first-party data and proprietary data are listed below. These characteristics have been considered by some users and regulators of data to be particularly relevant to product development or business utility.

First-party data means here:	Proprietary data means here:[748]
Data sourced from a business or entity which collects that data directly from the source or subject of the data, e.g. a business and their customer transactions, or a real estate agency and property data.[749]	Data that is not available from other suppliers and is not easily replicated by another company.[750]
	Data that may have restricted rights of ownership.[751]

The ACCC understands that several data firms access and use first-party proprietary datasets in developing their products or services. These include:

- **Equifax**, which has cited News Corp Australia and REA Group as sources of proprietary data.[752]
- **NielsenIQ**, which receives data from data agents appointed by major retailers,[753] and also recruits panels for marketing analysis.[754]
- **PropTrack**, which has access to property listing data from its websites realestate.com.au and flatmates.com.au, for use in ancillary analytics products.[755]
- **Quantium**, which has a retail product, Q.Checkout, that provides insights (such as customer loyalty, customer segments and category performance) 'derived from 10 million customers from Australia's largest retailer'.[756]

Data firms may use first-party proprietary data to complement or enhance the insights derived from their existing pool of data. This data can be used to generate or enhance knowledge of consumers, businesses, or groups at a granular level.[757] Data firms are therefore likely to improve the quality of their products or services provided to business customers by getting information on consumers from first-party proprietary datasets.[758]

748 Sources of data more broadly for business customers of data firms are also discussed at section 2.4.
749 A Barker, Consumer Data and Competition: a new balancing act for online markets? *OECD Going Digital Project*, 18 December 2020, p 7. Once purchased by the data firm, the data will be considered second-party data. Second-party data is defined in the Glossary of this Report.
750 T Davenport and T Redman, Your Organisation Needs a Proprietary Data Strategy, *Harvard Business Review*, 4 May 2020, accessed 15 March 2024.
751 US Geological Survey, Proprietary and Sensitive Data, accessed 15 March 2024.
752 Equifax, Submission to the Report, 28 September 2023, p 4.
753 The ACCC acknowledges that NielsenIQ and Nielsen [Pty Ltd] are separate entities.
754 NielsenIQ, Submission to the Report, 28 September 2023, p 8.
755 PropTrack, Submission to the Report, 28 September 2023, p 1.
756 Quantium, Q.Checkout, accessed 15 March 2024.
757 J Krämer, D Schnurr and S Micova, The Role of Data for Digital Markets Contestability: Case Studies and Data Access Remedies, September 2020, Centre on Regulation in Europe, pp 57–58, 65, 133.
758 A Cheong, T Wang and D Sokol, Submission to the Report, 28 September 2023, p 8.

Data firms can also access a large amount of first-party proprietary data to improve the accuracy of their algorithms and provide better analytical results to business customers. An example of this is PropTrack's AVM. It has access to proprietary sources, including the customer-facing property listing portal realestate.com.au operated by PropTrack's parent company, REA Group Limited.[759] Access to first-party proprietary data allows PropTrack to refine and update its algorithm over time and provide more accurate property valuations to its customers.[760]

6.1.3. Data exchange and acquisition

Whilst data firms may invest heavily in access to first-party proprietary data, the ACCC also understands that data firms buy and sell datasets from one another on a non-exclusive basis.

As previously discussed in section 4.3.7, many of the 9 sample firms purchase data products or services from one another, which reflects broader industry trends relating to the exchange and acquisition of data between data firms. ACCC analysis also indicates that data firms are involved in the exchange and acquisition of aggregated data, data of shared customers, and data processing and analysis tools.[761]

Non-exclusive exchange or acquisition of data may increase competition:

- between data firms. Where products or services of data firms benefit from more common or exchanged datasets, these products or services may compete more vigorously with one another
- downstream, between the business customers of those products or services. Where data firms have exchanged datasets and developed products or services that compete more vigorously with one another, business customers may have greater choice between products or services relevant to their industry sector or business function.

The ACCC also notes a trend of data being bought and/or sold between data firms, where those firms specialise in *different* business functions or industry sectors.[762] Data exchange and acquisition can help a data firm obtain a specific dataset that, in turn, supports its specialisation in certain industry sectors or business functions.

However, data firms specialising in more similar industry sectors or business functions may be less inclined to exchange their datasets with other data firms, particularly if data can become a unique strategic resource or a source of potential competitive advantage.[763] Of particular interest is first-party data (discussed above at 6.1.2), which is considered by some industries to be more valuable than second- or third-party data in driving competitive advantage through data.[764] Equifax and Experian submit that data firms do compete for access to specific sources of data, with factors such as quality, breadth, volume and exclusivity of access as reasons for competition in accessing datasets.[765] Quality and scale of data as non-price competition factors are discussed in more detail in section 6.2.3.

759 PropTrack, Submission to the Report, 28 September 2023, p 1.
760 Proptrack, Automated Valuation Models (AVMs), accessed 15 March 2024.
761 Information provided to the ACCC.
762 Information provided to the ACCC.
763 A Cheong, T Wang and D Sokol, Submission to the Report, 28 September 2023, pp 4–5, 9, 15.
764 Winterberry Group, White Paper: Data as Competitive Advantage, October 2015, accessed 15 March 2024, p 5.
765 Equifax, Submission to the Report, 28 September 2023, p 5; Experian, Submission to the Report, 28 September 2023, p 6.

6.2. How data firms compete to provide products or services

Data firms compete to provide their products or services through the following non-price dimensions:

- product differentiation
- privacy and data security (discussed in section 6.7)
- quality and scale of data.

The ACCC also considered price competition of products and services provided by the sample data firms. The ACCC analysed the pricing strategies used by the 9 sample data firms, which appears throughout section 4.4.1, and notes that:

- the 9 sample firms employed different approaches to pricing their products and services. This is due, in part, to the breadth of products and services offered by data firms, and the breadth of industry or business-function specialisation that data firms engage in
- the ACCC's analysis does not factor in the broader market participants (beyond the 9 sample firms) that could be relevant to an analysis of the pricing of data products and services.

Equifax and Experian submit that data firms compete on price and/or pricing structures.[766] However, most submissions from data firms did not name price as a key competitive or differentiating factor.

6.2.1. Product differentiation

Section 6.1 considered how data firms specialise in supplying products specific to different industries and business functions. As such, the products available from the sample data firms can differ extensively, which suggests not all data firms compete against each other.

Data firms may seek to differentiate themselves by providing particular data analytics expertise or providing the infrastructure for a business customer to conduct its own data analytics. Analytics services are particularly useful to data-intensive business functions such as demand and supply analysis, business intelligence and market research.[767] Database Consultants Australia submits that while big data analytics have become important tools for Australian businesses, small and medium-sized Australian businesses are 'rarely able to accrue the skilled data workers and necessary resources to operate "big data" analyses'.[768] The ACCC notes commentary referring to data analytics as the best way 'to turn data into a source of competitive advantage'.[769]

Data firms may also seek to differentiate by offering specific features that are derived from data analytics. For example, CoreLogic and PropTrack both provide AVMs using historical property data that is enhanced with artificial intelligence (AI) analytics. PropTrack's advertising suggests that its model is unique due to 'image scoring', which is the automated analysis of property images to measure individual properties' aesthetic appeal, renovation

766 Equifax, Submission to the Report, 28 September 2023, p 5; Experian, Submission to the Report, 28 September 2023, p 6.
767 Database Consultants Australia, Submission to the Report, 28 September 2023, p 3.
768 Database Consultants Australia, Submission to the Report, 28 September 2023, p 6.
769 V Desai, T Fountaine and K Rowshankish, A Better Way to Put your data to Work, *Harvard Business Review*, July-August 2022, accessed 15 March 2024.

status and features.[770] CoreLogic does not publicly advertise image scoring as a feature of its AVM.[771]

6.2.2. Privacy and data security

Privacy

Some data firms market privacy as a differentiating factor in their promotional materials, or as a way to minimise risk when using data products or services.[772] NielsenIQ submits that consumer privacy is connected to competition and product differentiation, stating that consumer privacy protection is a key asset it in its ability to effectively compete.[773]

Firms can undertake a variety of steps to enhance the privacy practices associated with their products or services, such as:

- limiting the capacity for data to be shared outside of the infrastructure of a data product or service. For example, LiveRamp seeks to differentiate itself in its product offering by marketing its audience segmentation product as 'privacy-conscious'.[774] LiveRamp also advertises that its data clean room service is 'privacy-enhancing,' because it enables targeted advertising without sharing the original data directly with the advertiser.[775]
- limiting the use of data for purposes that it was not collected for.[776] This particularly applies where consumers have not consented to any additional use cases for their personal information. PropTrack submits that an internal understanding of the restrictions on data is important to 'protect our reputation as a trusted guardian of the information we receive'.[777]
- limiting the collection and use of third-party data obtained through tracking tools. As discussed in chapter 1, the ACCC notes access to data through third-party cookies or from IP targeting is becoming more limited, in part because of initiatives from digital platforms such as Apple and Google.[778]

Business customers are increasingly mindful of broader concerns that their end customers may have around the potential data collection processes in a data product or service. For example, 10 Viacom CBS (now Paramount ANZ) notes that a factor for partnering with LiveRamp on its data strategy is that the brands LiveRamp engages with in online advertising are conscious of respecting consumer privacy.[779] The link between privacy and competition is discussed in section 6.7. As also considered in section 6.7, competition on its own may not always result in better consumer outcomes regarding privacy.

770 PropTrack, Demystifying the AVM, accessed 15 March 2024, p 7.
771 CoreLogic, Automated Valuation Model (AVM): Reliable residential property valuations in real time, accessed 15 March 2024.
772 LiveRamp, Enable growth while minimising risk, accessed 15 March 2024.
773 NielsenIQ, Submission to the Report, 28 September 2023, p 5.
774 LiveRamp, Data Collaboration, accessed 15 March 2024.
775 See box 3.2 for further discussion on data clean rooms, and box 3.1 for discussion of data management platforms. See also M Noonan, To Deliver Better Customer Experiences, Put Privacy-Enhancing Technologies to Work, *AdWeek*, accessed 15 March 2024; L Rapp, How LiveRamp Operationalizes Data Privacy by Design, *LiveRamp*, 20 April 2020, accessed 15 March 2024.
776 Equifax, Submission to the Report, 28 September 2023, p 8.
777 PropTrack, Submission to the Report, 28 September 2023, p 8.
778 LiveRamp, Submission to the Report, 28 September 2023, p 2.
779 Paramount, 10 ViacomCBS and LiveRamp Partner to Announce Australian-First Broadcast Data Collaboration for Advertisers, accessed 15 March 2024.

Data security

The ACCC understands that some data firms may invest more heavily than others in data security or may build data security features into their standard offering to establish a reputation of privacy and security for the business customer. These features might include: information security (i.e. ISO/IEC) certification; cryptography; data loss prevention policies; data retention and sanitation;[780] encryption; security practices for access controls; and movement to cloud storage and away from physical storage.[781] The ACCC received submissions from several sample firms indicating that data security was a differentiating factor in product or service sales.[782]

Equifax submits that both privacy and security are 'must-have' features for business customers and of relevance when deciding between data products and services.[783] It notes that potential business customers consider both the data firm's security practices, and the potential impact of new data on the security of existing data.[784] Quantium also submits that its business depends on demonstrably reliable security and data privacy standards.[785] LiveRamp submits that it has invested in its reputation as a trusted vendor in the data ecosystem 'by working to establish best-in-class compliance practices that go beyond legal and regulatory guidelines'.[786]

6.2.3. Quality and scale of data

Data firms may also compete on the quality and scale of their data, which may enable them to provide more accurate data-driven insights or tools.

Quality of data was raised as a distinguishing feature in submissions the ACCC received from multiple data firms in response to the Issues Paper. Equifax and Experian both submit that the quality of data is a factor for business customers of data firms (including Equifax and Experian themselves) in deciding between firms.[787] NielsenIQ also submits that data quality is a factor in business customer decision-making.[788] The ACCC has also observed marketing materials for some data firms, such as their websites, which promote the source or volume of data available as an indication of the quality of firms' products and services.[789]

The number of data points used in the data product or service is often also marketed by data firms as improving the accuracy of data products, much like data quality. In its submission, Experian notes a key area of competition, in addition to quality, is the 'volume and breadth of information'.[790] PropTrack says that its business model is 'based on [its] ability to organise and analyse large volumes of property data and make it available to customers'.[791] NielsenIQ submits that 'comprehensive data from data agents' is an essential input for market participants.[792]

---

780 PropTrack, Submission to the Report, 28 September 2023, p 8.
781 Equifax Submission to the Report, 28 September 2023, p 22–23.
782 Equifax, Submission to the Report, 28 September 2023, pp 5–6; Quantium, Submission to the Report, 28 September 2023, p 1.
783 Equifax, Submission to the Report, 28 September 2023, p 6.
784 Equifax, Submission to the Report, 28 September 2023, pp 6–7.
785 Quantium, Submission to the Report, 28 September 2023, p 1.
786 LiveRamp, Submission to the Report, 28 September 2023, p 3.
787 Equifax, Submission to the Report, 28 September 2023, pp 7–8; Experian, Submission to the Report, 28 September 2023, p 6.
788 NielsenIQ, Submission to the Report, 28 September 2023, p 6.
789 CoreLogic, AVMs: Updated to Stay in Tune with Volatile Markets, 15 March 2023, accessed 15 March 2024; Quantium, Q.Checkout, accessed 15 March 2024; Equifax, Data-driven marketing: smarter marketing with better market knowledge, accessed 15 March 2024.
790 Experian, Submission to the Report, 28 September 2023, p 6.
791 PropTrack, Submission to the Report, 28 September 2023, p 1.
792 NielsenIQ, Submission to the Report, 28 September 2023, p 5.

6.3. The multi-firm approach by business customers

Some business customers use multiple data firms to serve their data analytics needs. This includes using multiple data firms for similar products and services to improve accuracy, and using different data firms to serve different business needs or functions. In other words, these business customers may adopt **a multi-firm approach** to meeting their data analytics needs.

The ACCC's approach to discussing the multi-firm approach is based on an analysis of the top 20 customers of the 9 sample firms.[793] The ACCC notes therefore, that this analysis only provides a snapshot, not the full picture, of how Australian businesses use data firms.

6.3.1. Combining similar products and services

Business customers may use several similar data products and services to achieve greater accuracy and reduce risk in one specific business function. More accuracy can be a result of having a greater breadth of relevant data points, corroborating data points from different sources, and/or running multiple models developed by different data firms. For example, a bank may purchase multiple property valuation products, and use them all to conduct valuations on the same property. This aims to improve the accuracy of a valuation, which has direct implications on the risk profile of the bank's activities.

The fact that some business customers use multiple data products and services and cross-reference the corresponding outputs suggests some substitutability between these products and services, particularly when they relate to a specific business function. Conversely, a business customer that does not find it efficient to use similar products from multiple firms may rely only on a single data firm's product or service.

6.3.2. Facilitating business functions

The ACCC has also observed several business customers that use a range of data products or services, each sourced from a different specialised data firm. This presents a different type of multi-firm approach.

A business customer may rely on multiple data products and services for its various needs. Here, the use of multiple data products and services by the same business customer is not an indication of substitutability of products, as they all serve different functions. For example, for the purposes of a mortgage application, a bank may acquire the data products and services of:

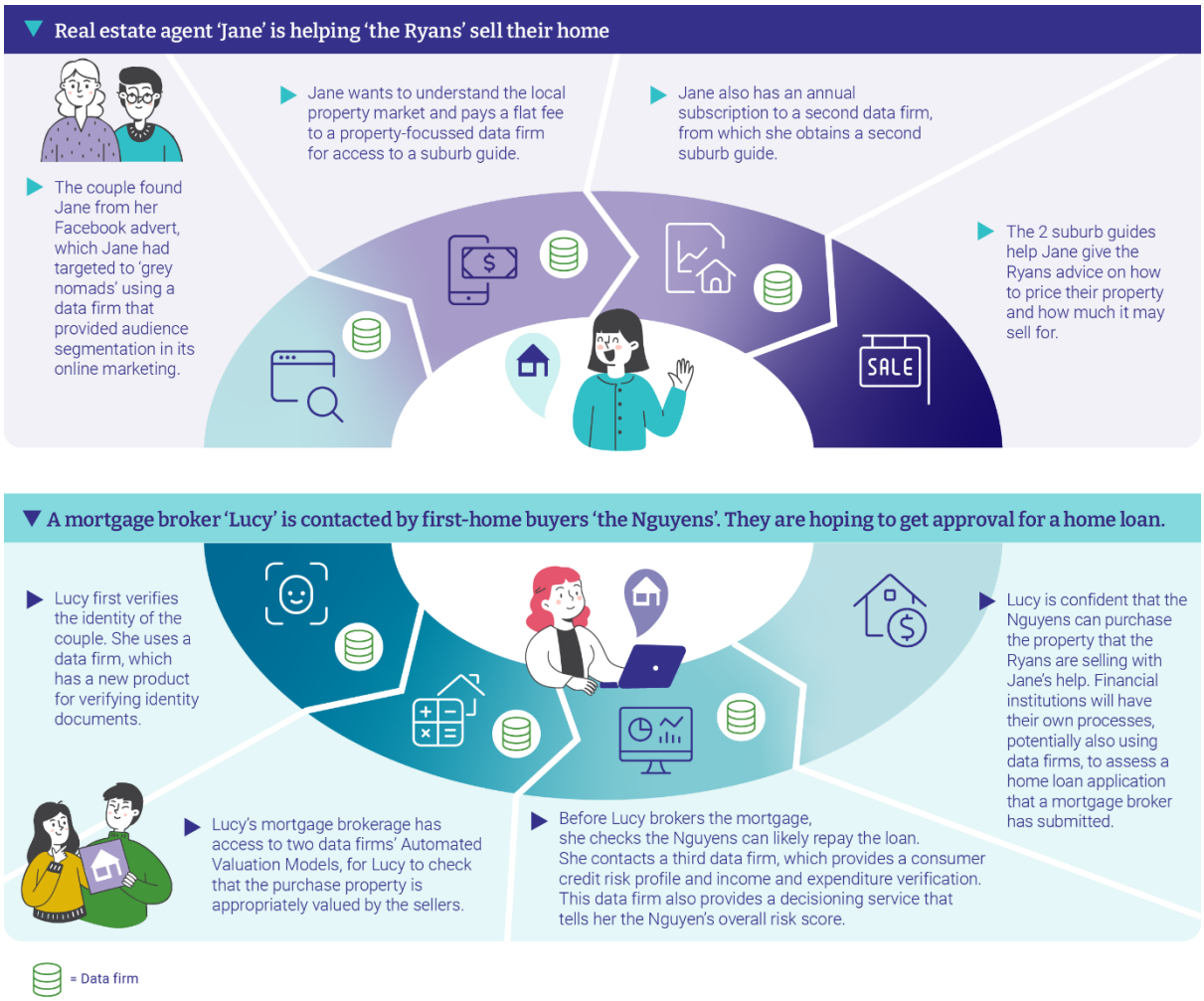
- an online advertising tool, to promote a mortgage product to prospective applicants
- an AVM product, to provide property valuations on residential properties that are the subject of mortgage applications
- an income verification service, to help verify the suitability of applicants for a mortgage product.

Figure 6.1 below demonstrates how some business customers may adopt multi-firm approaches. These approaches show how business customers may use different data firms to meet a range of business functions. These data firms' products and services may help a

[793] Information provided to the ACCC.

business customer work more efficiently, or with less risk. The illustration shows how a business customer may combine similar products or use a wide range of different products.

Figure 6.1: Examples of how data products and services may be used in the sale of a home



In marketing, business customers may use multiple data firms to improve audience access and engagement. A media company might use one data firm to match subscribers to an IP address or advertising ID. The media company – or a second data firm operating on its behalf – could then use this dataset to create audience segments to target advertising to the right customer groups. The same media company might then use a third data firm to analyse the impact of that advertising campaign on sales.[794]

The ACCC is aware that the multi-firm approach may give rise to interoperability issues, particularly when:

- a business customer seeks to use multiple products or services from different data firms in one business process, or
- a business customer seeks to transfer data (i.e. switch) from a product or service of one data firm to another data firm.

[794] See, for example, R Shields, Amid a dearth of ad tech M&A, LiveRamp fielded inbound inquiries over a potential sale, *Digiday*, 5 June 2023, accessed 15 March 2024 ('What all these companies are looking for is to offer the ID, the clean room, and then do testing and measurement, that's the utopia if you will. But in practicality, that's not necessarily how advertisers and publishers want to work…They want to sometimes use agnostic third-party measurement or their own proprietary clean room tech, and then use one of the IDs and keep that pricing compressed.').

In either scenario, a business customer may choose to develop or invest in its back-end infrastructure to facilitate interoperability between the products or services of different data firms. In circumstances where it is particularly difficult to achieve interoperability, a business customer may be less inclined to proceed with the multi-firm approach (including retaining existing data products or services from one data firm).[795]

6.4. Mergers and acquisitions

6.4.1. Acquisitions made by data firms

There is a long-term trend internationally of data firms acquiring firms with access to either datasets or data analytics capabilities. These acquisitions allow data firms to expand and enhance their data products and services. Big data companies have historically been very active in acquisition. The OECD reported that in the first half of 2013 alone (in the US), big data companies raised almost US$1.25 billion to fund a total of 127 deals.[796] Further, data analytics and cognitive analytics[797] have been identified as some of the most popular digital assets to target in mergers and acquisitions.[798]

The ACCC has observed these trends in the Australian context. Data firms operating in Australia have conducted acquisitions to increase their market share, analytical capabilities, and/or access to datasets. In addition, overseas data firms have acquired Australian data firms to enter or expand their product offerings in Australia. Larger data firms tend to acquire smaller ones offering products servicing the same industries. Among the 9 sample firms, the ACCC is aware of the following acquisitions relating to datasets and/or data analytics capabilities:

- **Equifax:** The Australian division of Equifax was rebranded from Veda Group, which the US-based Equifax acquired in February 2016.[799] Veda had itself conducted several acquisitions of note, including of the National Tenancy Database in 2007.[800] In 2021, Equifax acquired CreditWorks Australia, which provides commercial credit and risk management technology.[801] These acquisitions allowed Equifax to expand its data insights on consumers and businesses.[802]
- **Experian**: Experian acquired Pacific Micromarketing in 2013 for its customer database analysis, which included its 'household classification system' Mosaic.[803] In 2019 Experian acquired Australian fintech Look Who's Charging (LWC), whose platform provides instant clarification of the merchant behind bank transactions. Experian noted that the acquisition would allow it to 'combine Experian's global open data solutions with [LWC's] advanced enrichment capabilities...' and 'create a market leading open data platform'.[804]

795 S Gulati-Gilbert and R Seamans, Data portability and interoperability: A primer on two policy tools for regulation of digitized industries, *The Brookings Institution*, 9 May 2023, accessed 15 March 2024; M Stoltz, Interoperability as a Remedy in Antitrust cases, *Competition Policy International,* 17 November 2022, accessed 15 March 2024.
796 OECD, Data Driven Innovation: Big Data for Growth and Well-Being, 6 October 2015, p 23.
797 'Cognitive Analytics brings together a number of intelligent technologies, including semantics, artificial intelligence algorithms, deep learning and machine learning.' See Ulster University, Harnessing the Power of Cognitive Analytics, accessed 15 March 2024.
798 Freshfields, The World of Digital M&A, November 2018, accessed 15 March 2024, p 23.
799 Equifax, Veda rebrands to become Equifax in Australia and New Zealand, 13 March 2017, accessed 15 March 2024.
800 National Tenancy Database, About Us, accessed 15 March 2024.
801 Equifax, Equifax acquires CreditWorks helping SMEs manage risk, 1 March 2021, accessed 15 March 2024.
802 Equifax, 2Q23 Earnings Call, 20 July 2023, p 70.
803 Business Information Industry Association, Experian Acquires Melbourne-based Pacific Micromarketing, 22 January 2013, accessed 15 March 2024.
804 Experian, Experian A/NZ acquires Australian fintech Look Who's Charging to bolster open data offering, 21 August 2019, accessed 15 March 2024.

- **illion**: In 2018, illion acquired Australian fintech firm Proviso, which provides bank statement retrieval, analysis and categorisation.[805]
- **CoreLogic**: CoreLogic's initial product offering included an AVM for property valuations.[806] CoreLogic has since expanded into other property-related services, including lead generation (identifying and matching purchasers to property listings using data analytics). It has achieved this through purchasing adjacent Australian companies in the industry, like proptech firm AiRE, which developed RiTA, a digital assistant for real estate agents (purchased in 2021).[807] CoreLogic also expanded its lead generation offerings through its 2022 acquisition of Plezzel, an online property enquiry automation platform.[808]

The ACCC observes that the sample firms' acquisitions listed above are primarily acquisitions of data analytics capabilities. The acquisition of data analytics capabilities may enhance a data firm's ability to extract valuable information from existing datasets.[809] For example, when purchasing AiRE, Corelogic commented on the role of the acquisition in commercialising its business customers' existing data: 'Agents will appreciate the intrinsic value of their CRM data but may have struggled to fully commercialise and maximise its full potential'.[810] Both Experian and illion's abovementioned recent acquisitions of Australian fintech firms offer capability to synthesise and categorise transaction data for commercial benefit.

6.4.2. Acquisitions of data firms by non-data firms

The ACCC notes that, in some cases, data firms have been acquired by other companies that may collect first party data or use data products and services. This includes:

- **PropTrack and REA Group**: REA purchased PropTrack (formerly Hometrack) in 2018. This was followed by several further acquisitions, such as fintech and advertising company CampaignAgent in July 2023[811] and the purchase of a 34% interest in mortgage application software Simpology.[812]
- **Quantium and Woolworths:** Quantium was awarded the tender for Woolworths' data agency and scan services in 2018.[813] Woolworths then purchased a controlling stake in Quantium in April 2021.[814] It announced a new business unit within Woolworths called Q-Retail to advance Woolworths' analytical capabilities. It now has a joint venture with Woolworths called 'wiq' to advance and commercialise Woolworths' retail analytics capability.[815]

---

805 Start Up Daily, Data and analytics firm Illion acquires Adelaide fintech startup Proviso, 19 January 2018, accessed 15 March 2024.
806 TA, First American Core Logic, accessed 15 March 2024.
807 Elite Agent, RiTA by AiRE wins industry innovation award second year running, 26 October 2021, accessed 15 March 2024.
808 Plezzel, Plezzel signs acquisition agreement with CoreLogic, 14 December 2022, accessed 15 March 2024; Onthehouse.com.au, CoreLogic signs deal to acquire digital real estate marketing firm Plezzel, 14 December 2022, accessed 15 March 2024.
809 'It may be not so much the exclusive quality of the newly acquired data that is of concern, but the acquirer's ability to combine it with its existing datasets (that is, expanding its store of Big Data) and mine it to extract valuable information', OECD, Theories of Harm for Digital Mergers, 2023, p 22.
810 CoreLogic, CoreLogic deepens investment in real estate solutions with acquisition of prop-tech firm AiRE, 7 March 2022, accessed 15 March 2024.
811 M Martin, REA Group's Australian revenue drops 1% in FY3, *Broker News* 12 August 2023, accessed 15 March 2024; ListCorp, REA Group Investor and Analyst Presentation FY23, 11 August 2023, accessed 15 March 2024.
812 M Bleby, REA to offer exclusive home loan rates, quick applications, *Australian Financial Review,* 15 June 2021, accessed 15 March 2024.
813 S Mitchell, Woolworths hands data sharing contracts to Quantium, Nielsen, *Australian Financial Review,* 4 October 2018, accessed 15 March 2024.
814 R Crozier, Woolworths to take control of Quantium for $223 million, *IT News*, 20 April 2021, accessed 15 March 2024.
815 R Crozier, Woolworths and Quantium are now calling their combined entity 'wiq', *IT News*, 15 July 2022, accessed 15 March 2024.

Following acquisition, the parent company may benefit from data-driven insights provided by the acquired data firm, which may allow it to compete more effectively in its main business(es). This transaction rationale was highlighted by the parent companies of both sample firms listed above, PropTrack and Quantium. A spokesperson for REA Group noted, in relation to the purchase of PropTrack, that data was a 'huge competitive advantage for REA Group'.[816] When speaking to the purchase of its controlling stake in Quantium, Woolworths CEO Brad Banducci noted that Quantium's analytics capability would 'unlock value across our entire retail ecosystem'.[817]

The ACCC has observed that data firms that are vertically integrated with a firm that is a source of data may have greater access to that data, compared to other data firms that are not vertically integrated. As such, data firms may be able to leverage the direct relationships held by the (vertically integrated) parent company with customers to access high-quality data. The Consumer Policy Research Centre (CPRC) noted that Woolworths outsources data analysis and data agency roles to Quantium.[818] Therefore, vertical mergers may provide a competitive advantage for the acquired data firm.

6.5. Potential competition issue – vertical foreclosure

The ACCC is concerned generally about input foreclosure. Input foreclosure is where a vertical agreement causes a supplier to limit access to a relevant input to one downstream buyer, at the expense of that buyer's competitors.[819] Specifically, the ACCC considers there may be incentives for data firms to restrict access to unique datasets from other data firms providing similar products or services.

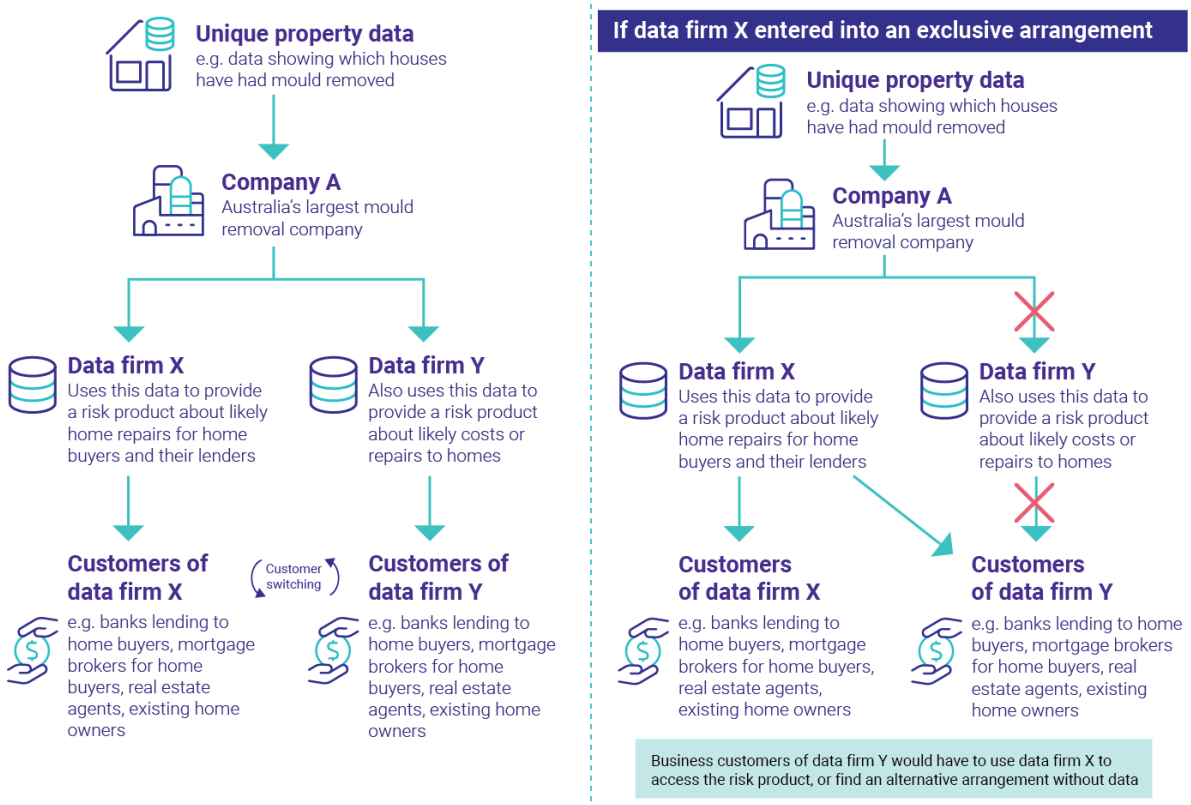
As discussed in sections 6.1.2 and 6.1.3, data may become a source of competitive advantage, particularly where data firms operate in more concentrated product or service segments. Restricting access to data may limit the accuracy of competing products or services (particularly if a product or service relies on continuous access to datasets) or limit the capacity of another data firm to develop a similar service. This behaviour may, over time, have the practical effect of foreclosing rivals in the relevant market(s). Restrictions on access to data may occur in several ways, discussed below.

6.5.1. Exclusivity arrangements

Input foreclosure could occur through the use of exclusivity arrangements to prohibit data suppliers from providing a dataset to a competitor, as described in figure 6.2. This could include a data firm seeking to be the 'sole supplier' of a first-party proprietary dataset.

816 K Weber, REA Group poaches PEXA data chief for PropTrack business, *IT News,* 5 March 2021, accessed 15 March 2024.
817 S Mitchell, Woolworths doubles down on data, takes control of Quantium, *Australian Financial Review*, 20 April 2021, accessed 15 March 2024.
818 CPRC, A Day in the Life of Data, 29 May 2019, p 10.
819 A Athayde, Input Foreclosure as Theory of Harm in in Vertical and Conglomerable Mergers, 11 September 2023.

Figure 6.2: Hypothetical example of exclusivity arrangements and data access

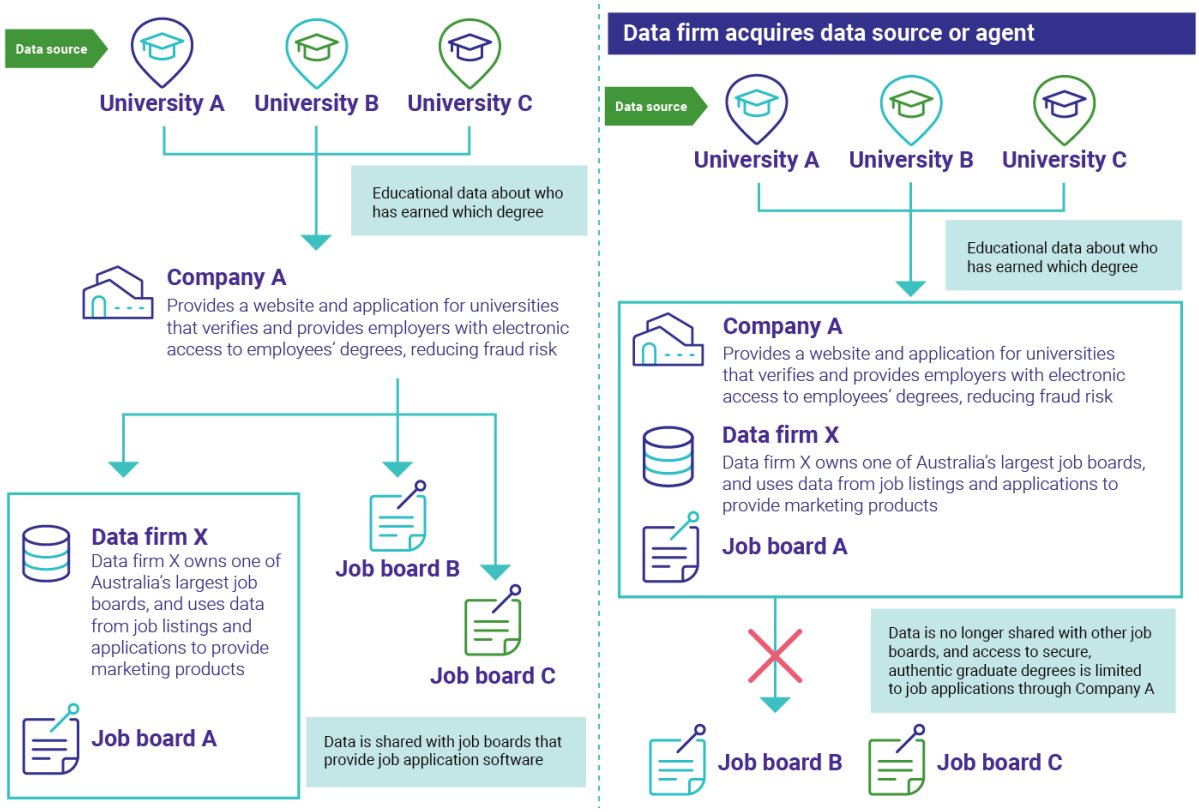


6.5.2. Acquisitions and joint ventures

Input foreclosure could also occur through the acquisition of, or a joint venture between, firms that have access to first-party proprietary data.[820] A hypothetical example of how acquisition could impact access to data and lead to input foreclosure can be found below at figure 6.3.

[820] The ACCC is currently conducting an informal merger review in relation to the potential acquisition of Dynamic Methods by REA Group. In the Statement of Issues published on 15 February 2024, the ACCC listed 'data-related foreclosure risks and entrenchment in the supply of digital real estate advertising' as an issue that may raise concern. ACCC, Statement of Issues: Realestate.com.au – proposed acquisition of Dynamic Methods, 15 February 2024, p 9.

Figure 6.3: Hypothetical example of acquisition and data access



6.6. Digital platform service providers and competition in online advertising

The ACCC notes that both data firms and digital platforms, such as Amazon, Google and Meta, provide audience segmentation products and services that support online advertising.

As the ACCC has previously discussed, digital platform service providers have access to large datasets on consumers.[821] Free TV Australia, IAB Australia and the Law Council of Australia note that data firms' services can have pro-competitive effects, such as helping smaller businesses advertise more efficiently online.[822] They submit that these data firms compete against large digital platforms (or other businesses with market power and access to significant first-party datasets).[823]

Amongst other services that support online advertising, Amazon, Google and Meta offer audience segmentation tools:

- Amazon provides audience segmentation tools for use in search and display advertising. As with both Google and Meta, Amazon's audience segmentation tools are built using first-party data accessed on Amazon-owned websites (such as Amazon Marketplace) and apps (such as Kindle) and can reflect a user's behavioural and lifestyle preferences.[824]

821 ACCC, Digital Advertising Services Inquiry Final Report, 28 September 2021, p 6; ACCC, Digital Platform Services Inquiry – Interim Report No. 6 – Social media services, 28 April 2023, p 118.
822 Free TV Australia, Submission to the Report, 28 September 2023, p 2; IAB Australia, Submission to the Report, 28 September 2023, p 6; Law Council of Australia, Submission to the Report, 28 September 2023, p 5.
823 Free TV Australia, Submission to the Report, 28 September 2023, p 2; IAB Australia, Submission to the Report, 28 September 2023, p 6; Law Council of Australia, Submission to the Report, 28 September 2023, p 5.
824 Amplio Digital, What is the Amazon Demand Side Platform?, July 2019, accessed 15 March 2024.

- Google provides audience segmentation tools using both its own first-party data, and the first-party data of the advertiser. An advertiser can make a custom segment and target consumers from its selected segment(s) within Google's online advertising platform. Google's segmentation is based on user activity in the Google ecosystem, and segments can reflect the user's interests, demographics, or recent purchases.[825]
- Meta also provides audience segmentation tools to advertisers. Meta allows advertisers on its platforms to select audiences for their campaigns based on age, gender, language, location, interests, or behaviours.[826] Given that some audience segments are based on behaviour such as users' engagement with advertisements or pages or device usage, Meta uses its existing first-party data to provide these audience segmentation services.[827]

However, there are differences between the audience segmentation tools provided by digital platforms and data firms. For digital platforms, their audience segmentation services and the first-party data that fuels them are components of their own advertising services, and therefore remain within their own ecosystems. On the other hand, data firms are more likely to provide audience segmentation tools that are platform-agnostic, allowing business customers to use audience segmentation to target consumers across a range of online services.

Large digital platforms potentially have relatively low barriers to entry with respect to platform-agnostic audience segmentation services, considering their scale and scope advantages in respect of the first-party data they already hold on consumers. However, they may have limited incentive to leverage this position into developing products or services that are platform-agnostic and that do not need advertisers to be a customer of their broader advertising ecosystems.

Research by EU regulators suggests that digital platforms are only willing to share some data with downstream business customers. While downstream business customers of e-commerce digital platforms can access data on their customers' interactions with their products, platforms are reticent to share broader market analytics data.[828]

Digital platforms may also limit the granularity of data available to downstream business customers.[829] While digital platforms argue this is intended to protect consumer data and reduce the prevalence of direct marketing to consumers (including by business customers), downstream business customers argue that the data is used by digital platforms to gain an unfair advantage in downstream markets where they are competitors.[830]

825 Google Ads, About Audience Segments, accessed 15 March 2024.
826 Meta, About Reaching New Audiences, accessed 15 March 2024.
827 Meta, About Detailed Targeting, accessed 15 March 2024.
828 V Gineikytė, E Barcevičius and G Cibaitė, Business User and Third-Party Access to Data, European Commission, 27 July 2020, accessed 15 March 2024, p 23.
829 V Gineikytė, E Barcevičius and G Cibaitė, Business User and Third-Party Access to Data, European Commission, 27 July 2020, accessed 15 March 2024, p 5.
830 V Gineikytė, E Barcevičius and G Cibaitė, Business User and Third-Party Access to Data, European Commission, 27 July 2020, accessed 15 March 2024, p 5.

6.7. Privacy and competition

6.7.1. Potential limitations to privacy and data security as non-price competitive factors

The concept of privacy and data security as non-price competitive factors is still an emerging topic in competition policy.[831]

The ACCC has recognised that a lack of competition can potentially reduce a firm's incentive to build strong privacy protections.[832] Similarly, overseas competition agencies have recognised privacy as an element of product or service quality that may be impacted by competition.[833] Where an erosion of data privacy occurs (either through increasing data collection or decreasing security), it may be framed as a reduction in quality (a non-price factor of competition).[834]

Box 6.2 Privacy as a non-price competition factor in overseas jurisdictions

- **Europe:** The European Commission has recognised data privacy as a parameter of non-price competition in specific industries.[835] In its decision regarding the *Facebook/WhatsApp* merger, the European Commission noted that firms can compete on privacy in communication services markets.[836] The European Commission similarly identified in its *Microsoft/LinkedIn* merger decision that firms can compete on privacy in social media markets.[837]
- **United States:** The United States Department of Justice's (DOJ) current case against Google, alleging that it has monopolised digital advertising products, has also raised allegations of degraded privacy standards for consumers. The DOJ has alleged that Google's market dominance in search has harmed consumers 'by reducing the quality of search (including on dimensions such as privacy, data protection, and the use of consumer data)'.[838]

Digital platforms are also increasingly claiming to offer higher privacy standards for consumers. Apple describes the various measures it implements across its products to limit data collection and implement data protection technologies as integral to its business model.[839]

831 E Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy, Temple University Legal Studies Research Paper No. 2021-40, 6 July 2021. See also section 2.4.2 of this Report for a discussion of the tension between competition and privacy.
832 G Cass-Gottlieb, Regulatory intersections between competition, consumer and privacy laws, *Asia Pacific Privacy Authorities 60th Forum,* 30 November 2023, accessed 15 March 2024.
833 E Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy, Temple University Legal Studies Research Paper No. 2021-40, 6 July 2021, pp 63–64.
834 S Esayas, Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers, 16 August 2018, pp 4–5.
835 S Esayas, Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers, 16 August 2018.
836 European Commission, Case No COMP/M.7217 – Facebook/Whatsapp, 3 October 2014, pp 15, 19.
837 European Commission, Press Release – Mergers: Commission approves acquisition of LinkedIn by Microsoft, 6 December 2016.
838 United States Department of Justice, Justice Department Sues Monopolist Google for Violating Antitrust Laws, last updated 21 October 2020, accessed 15 March 2024.
839 Apple, Submission to the Report, 28 September 2023, p 1.

The ACCC acknowledges views among competition policy experts about the limitations of privacy as a non-price competition factor, notably that:

- consumers may not be sufficiently informed to make decisions based on the level of privacy offered
- implementation of a firm's privacy policy may not be readily verified
- there may be limited or no effective punishment when a firm does not follow its privacy policy.[840]

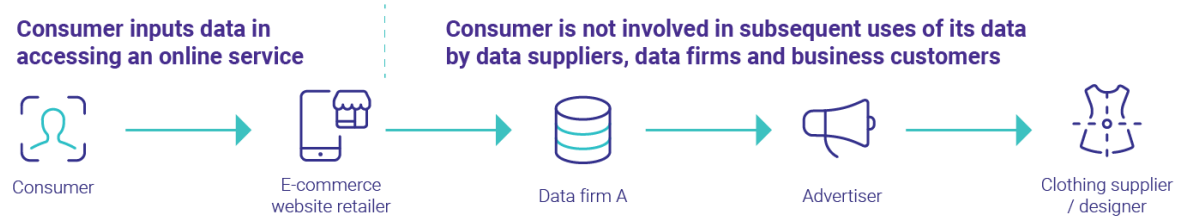
An additional complexity arises when undertaking an assessment of privacy or data security as an aspect of non-price competition – the fact that many data products or services are not 'consumer-facing'. As discussed in section 5.1, consumers are often unaware of the data collection practices of data firms in the first instance. Consumers also do not play an active role in the transactions between data firms and business customers.

In addition, there are multiple firms involved in the data supply chain, including:

- business customers seeking data-driven analysis
- data firms acting as data sources
- data firms processing and analysing individual datasets.

As such, many decisions in respect of privacy and data security standards are being implicitly made on a consumer's behalf and could involve any of the firms in the data supply chain.

Figure 6.4: Consumer involvement in the data supply chain



Various data firms made submissions outlining the link between implementing enhanced privacy or data protection practices and increased commercial success for relevant data products or services.[841] As mentioned in section 6.2, some business customers consider enhanced data security settings as a competitive factor, particularly in protecting their reputation by way of avoiding data breaches. While this could imply some consensus among business customers relating to the safeguarding of personal information, not all business customers may have this incentive front of mind.

6.7.2. Benefits of greater coordination between competition and privacy outcomes

As discussed in the original Digital Platforms Inquiry, there can be coherence between competition and privacy.[842] There are circumstances in which data firms are incentivised

840 J Tomas Llanos, A close look on privacy protection as a non-price parameter of competition, *European Competition Journal*, Volume 15, Issue 2-3, 16 July 2019.
841 Quantium, Submission to the Report, 28 September 2023, p 5; PropTrack, Submission to the Report, 28 September 2023, p 8; NielsenIQ, Submission to the Report, 28 September 2023, p 5.
842 ACCC, Digital Platforms Inquiry Final Report, 26 July 2019, p 5.

both to promote greater competition between firms and to implement enhanced privacy settings. In the context of data firms, this is evidenced by:

- the increasing role that privacy and data security can play as a standalone aspect of non-price competition between data firms[843] (as well as an aspect of the reputation of data firms)
- the adoption of data security features that seek to mitigate the extent to which data is shared outside a data product or service.

6.7.3. Tensions between competition policy and privacy regulation

There are, however, circumstances where the incentives for promoting greater competition between data firms and the implementation of enhanced privacy settings might not align. There can be a tension between protecting consumers' interests relating to (and control over) the collection, use and disclosure of their personal information, and enabling data firms to have greater access to the necessary data inputs to supply products and services to their business customers.

As discussed at section 6.5, the ACCC considers there may be potential competition concerns where first-party proprietary data is essential to providing a competing service and subject to a potentially anticompetitive exclusivity arrangement. A potential remedy to address such concerns and promote greater competition between firms might be to grant competitors access to relevant datasets on fair, reasonable and non-discriminatory (FRAND) or similar terms.[844] Other potential remedies may relate to the promotion of open-access data schemes or statutory data-sharing schemes, as discussed in section 2.4.

However, a competition remedy designed to increase the buying and selling of data between firms – and potentially the exchange of personal information on consumers – may also be at odds with promoting data privacy and security. As discussed in chapter 5, consumers have indicated a level of discomfort with having their personal information used and exchanged in ways they are not fully informed about or consent to.

The submission to this Report from academics Ariel Cheong, Tawei Wang and D. Daniel Sokol observed a potential positive correlation between market concentration and data security standards for data firms based in the United States, noting that:

- there is less sharing of consumer data between business customers and data firms in more concentrated markets
- correspondingly, these markets are associated with a decreased risk of data privacy breaches.[845]

However, the ACCC notes that the analysis of the interplay between market concentration and privacy settings in data-driven markets is nascent, and largely remains theoretical.[846] For example, there are contrasting views that the incentives of data firms to increase profits could 'provide the power to cause a decline in quality – including privacy quality.'[847]

---

843 See the discussion above at section 6.2.2.

844 M Botta, The principle of FRAND in B2B data sharing: Lessons from licensing of standard essential patents and competition law remedies, *Concurrences Review,* September 2023.

845 A Cheong, T Wang and D Sokol, Submission to the Report, 28 September 2023, p 1.

846 E Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy, Temple University Legal Studies Research Paper No. 2021-40, 6 July 2021, p 99.

847 E Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy, Temple University Legal Studies Research Paper No. 2021-40, 6 July 2021, p 100.

Commentary also reflects that in some jurisdictions, such as the European Union, the cost of compliance with data protection regulation may contribute to increased market concentration, particularly when smaller competitors with fewer resources must also comply.[848] The European Commission noted that in spite of the challenges faced by small and medium-sized enterprises in meeting privacy compliance standards, enforcement of these standards should be consistent across all markets, given that the 'risk of privacy harm to consumers does not necessarily correlate with firm size'.[849]

6.7.4. Inter-agency cooperation on competition and privacy issues

The ACCC acknowledges that an effective approach to addressing the nexus between competition policy and privacy regulation requires collaboration and coordination from relevant regulatory agencies.

In March 2022, the Australian Communications and Media Authority (ACMA), the ACCC, the Office of the Australian Information Commissioner (OAIC), and the eSafety Commissioner (eSafety) formalised existing collaborative arrangements to form the Digital Platform Regulators Forum (DP-REG).[850] While all 4 regulators already worked closely together, DP-REG facilitates greater engagement between them. The forum promotes sharing information about, and collaborating on, cross-cutting issues, including how competition, consumer protection, privacy, online safety and data issues intersect. This includes frequent formal and informal consultation on existing projects, as well as collaboration on research, capacity building and shared engagement with stakeholders in relation to issues of common concern.[851]

The ACCC would also welcome further research by other stakeholders, including academics and consumer advocacy groups, into the interrelation between competition policy and privacy regulation in data markets.

848 E Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy, Temple University Legal Studies Research Paper No. 2021-40, 6 July 2021, pp 100–101.
849 E Douglas, Digital Crossroads: The Intersection of Competition Law and Data Privacy, Temple University Legal Studies Research Paper No. 2021-40, 6 July 2021, pp 101–102.
850 Digital Platform Regulators Forum, DP-REG infographic, 20 November 2023, accessed 15 March 2024.
851 ACCC Chair Gina Cass-Gottlieb, Regulatory intersections between competition, consumer and privacy laws, *Asia Pacific Privacy Authorities 60th Forum,* 30 November 2023; Digital Platform Regulators Forum, DP-REG joint submission to Department of Industry, Science and Resources' AI discussion paper, 26 July 2023, accessed 15 March 2024.