

Singled Out



Consumer understanding — and misunderstanding —
of data broking, data privacy, and
what it means for them

Singled Out

CPRC

The Consumer Policy Research Centre (CPRC) is an independent, not-for-profit, consumer think-tank established in 2016.

CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates.

Statement of Recognition

CPRC and UNSW Sydney acknowledge the Traditional Custodians of the lands and waters throughout Australia. We pay our respect to elders, past and present, acknowledging their continuing relationship to land and the ongoing living cultures of First Nations peoples across Australia.

Acknowledgements

The authors thank Helen Lewis for design and editing assistance and Anna Johnston for feedback on the survey design. The authors are responsible for the views in this report, including any errors or omissions.

Published by Consumer Policy Research Centre and UNSW Sydney

cprc.org.au | unsw.edu.au

Kemp, K., Gupta, C., Campbell, M., Singled out – Consumer understanding — and misunderstanding — of data broking, data privacy, and what it means for them (February 2024)

Copyright 2024

Katharine Kemp, Chandni Gupta, Marianne Campbell.

Contents

Executive Summary	4
Key Findings	6
Data broking broken down for consumers	7
Background	8
Survey Methodology	11
Part 1: Survey Findings	12
Consumer recognition of data tracking descriptions	13
Consumer understanding of tracking and targeting capabilities	16
Consumer perceptions of control over personal information.....	19
Use of personal data by third parties.....	21
Consumer impact: lack of trust, frustration, anxiety and anger	23
Part 2: What do these terms mean and how can the data be used?	24
Personalised information	25
Pseudonomised information	26
Hashed email addresses	27
De-identified information	28
Anonymised information.....	32
Aggregated information	33
Audience data	34
Part 3: Conclusions	35
Consumer lens on data broking.....	36
Policy recommendations	37
Annexure 1: Examples of privacy terms of consumer-facing businesses	41
Annexure 2: Examples of privacy terms of data-broking services	43
Annexure 3: Data broking definitions	45
Endnotes	46

Executive Summary

Consumers' activities online and offline are being constantly tracked by a multitude of commercial organisations. This includes data about a consumer's activities and purchases on websites and apps, relationship status, children, financial circumstances, life events, health concerns, search history, and location data.

Organisations describe types of information collected in ways that are confusing and unfamiliar for consumers — such as 'pseudonymised', 'anonymised', 'hashed', 'audience data', and 'aggregated'. These descriptions do not have any definition in law nor any fixed meaning in practice. They also appear to suggest that the data in question is not related to the consumer as an individual and cannot be used to track, monitor, profile, single out, exclude, or influence the consumer when they certainly can.

It appears that much of this wording is designed to avoid consumers understanding or objecting to the collection and use of their personal information. This research confirms that consumers largely don't understand the convoluted terms used by industry to describe when they will collect data and track someone's activities.

Australians do not feel in control of their personal information. Only a third of consumers feel they have at least moderate control over whether businesses use their personal information to create a profile about them. More than 70% of consumers believe they have very little or no control over what personal information online businesses share with other businesses.

Most consumers feel it is unacceptable for businesses they are not directly in contact with to use data including their search history, location data, information about their device, device identifier, cookie data, or hashed email address. However, data brokers, data analysts and other 'data partners' not in direct contact with consumers commonly use such data.

Consumers feel a lack of trust, frustration, anxiety and/or anger about their inability to control how their information is collected and used.

Most consumers don't recognise important categories of personal information that are used to track them, single them out and influence what they see online. This undermines the argument that consumers are making informed choices about personal data uses based on privacy notices. These notices are notoriously difficult for consumers to understand and provide negligible choices.



Executive summary, continued

Most consumers appear to have no understanding of terms commonly used by industry in privacy notices including ‘pseudonymised information’ (81%), a ‘hashed email address’ (74%) or an ‘advertising ID’ (67%). These types of information are widely used to track and influence consumers, unbeknownst to them.

When consumers don’t recognise descriptions of personal information, they are also less likely to know whether that data could be used to single them out for tracking, influencing, profiling, discrimination, or exclusion. Most consumers either don’t know, or think it unlikely, that ‘pseudonymised information’ (70%), a ‘hashed email address’ (60%) or ‘advertising ID’ (50%) could be used to single them out from the crowd, when in fact they can.

The position is likely to be worse than these statistics suggest since some consumers are likely to have overestimated their knowledge and understanding of these terms.

While consumer education might seem an obvious solution to a lack of consumer understanding, education is not the answer in a digital economy that is swiftly evolving and continuing to place significant levels of cognitive load on consumers.

We need substantial amendments to the *Privacy Act 1988 (Cth)* (*Privacy Act*) to protect consumers, including an updated definition of ‘personal information’ which includes information that allows an individual to be singled out from the crowd, and a ‘fair and reasonable’ test for handling of personal information which cannot be circumvented by pointing to the fine print of privacy policies and spurious ‘consents’.

Key findings

Australians don't feel in control of their personal information — for good reason. Privacy policies use vague terms to describe how consumer data can be sold or used by others (like data brokers that share mass sets of data that can shape everything from which political ads someone will see on the internet to the price they may be offered for services). Those vague terms are also used inconsistently and in ways that seem designed to be hard to understand. This means it is far too difficult for consumers to understand who is sharing their personal data and what is being done with it.



Businesses use vague, confusing, and undefined terms in their privacy messaging that consumers can't understand.



Consumers don't understand key types of information companies — including data brokers — can use to track, profile, and monitor them.



Most consumers don't know the meaning of terms like:

Hashed email address	74%
Pseudonymised information	81%
Audience data	63%
Advertising ID	67%



Terms used in many privacy policies have no definition under Australian law and businesses use them inconsistently:

Anonymised information
Pseudonymised information
Hashed email
Aggregated data
Audience data



There is controversy over when information is personal vs de-identified.

Businesses try to argue information is de-identified so it's not covered by privacy law.



Consumers think it's unacceptable for businesses they have no direct relationship with to use their:

Email	74%
IP address	73%
Device information	68%
Search history	71%
Location data	68%



Most consumers feel they have little or no control over:

What personal information businesses collect about them from other businesses 72%

Businesses sharing their personal information with other businesses 71%

Data broking broken down for consumers

Data brokers are probably dealing in your personal information as you read this. This data broking involves one business supplying information about you to another business as part of a commercial swap, sale, match, or licence deal.

Your data can be used against you.

Businesses can use your data to make more profit at your expense, including by charging you a higher price; preventing you from seeing better offers; showing you ads related to a private medication, health condition or grief; reducing the priority you're given in customer service; or creating a profile (which you'll never see) to be provided to a prospective employer, insurer or landlord.

Where did they get your data?

There are two main types of data brokers that use personal data. **Third-party data brokers** are likely to be companies you've never heard of because you've never dealt with them. They got your data from other companies, including more companies you've never heard of. Some belong to multinational corporate groups that make tens of billions of dollars from their data businesses.

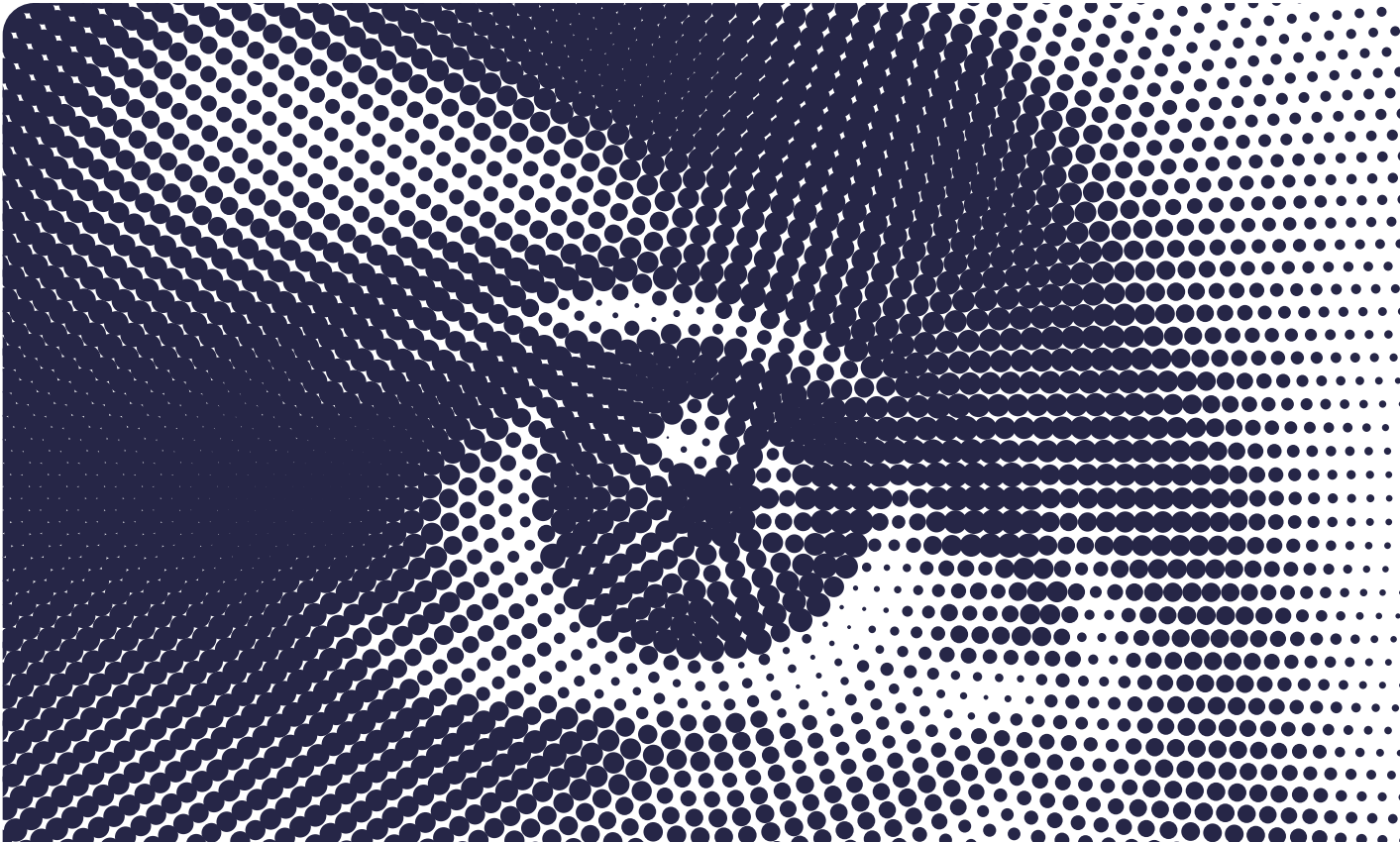
Second-party data brokers are more likely companies you recognise — for example, retailers, customer loyalty schemes, apps, or digital platforms. They got your data by collecting it from you or by monitoring your use of their store, website or app. You're unlikely to be aware of the full extent of the data they collected on you, which can also include data collected from other companies.

Examples of data broking services include:

- **'Data enrichment'** — the broker supplies further details about your age, income, marital status, family situation, and/or purchase intentions to a company that may have only had your email address;
- **'Identity resolution'** — the broker helps the company work out that you are the same person whether you logged in or not, whether you used your personal phone or your work laptop, and even if you use a different email or mobile number;
- **'Audience data'** — the broker allocates you to a group of people and claims that that group or 'audience' has certain things in common like income level, family situation, health situation, how often and how much they spend on various things.

'Data matching' vs 'We never sell your data'

Companies that say they never 'sell' your data often still supply your data to others as part of commercial deals even if there's not a payment of money. Data matching, for example, involves two or more companies taking the dossier of information they each have on you and combining it so they each walk away with a more detailed — and profitable — profile on you.



Background

Many businesses profit from harvesting and monetising consumers' personal information. The services sold by these businesses include online advertising and advertising technology, data 'enrichment', curation of 'audiences', and various other data supply and data broking services.

These organisations often seek to justify this use of personal information on the basis that privacy notices or disclosures have been made available to consumers, and individual consumers have supposedly given their 'consent' to these practices. Data brokers, for example, argue that they have 'consumer permissioned data' or 'user permissions' to collect consumers' personal information from various third parties and tracking technologies, and to disclose this personal information to other companies.

However, the mere fact that a privacy policy has been published on a website or linked to an app does not mean that the consumer has made an informed decision to allow their personal information to be disclosed to other retailers and/or data brokers for additional commercial purposes. The purported notices and consents are generally presented to consumers as take-it-or-leave-it terms where use of data for the purpose of providing the service is bundled with additional purposes in the fine print: if they use the service, the organisation considers they have consented to all purposes, no matter how vague or broad.



It is not surprising then that consumers often believe they have no real choices about whether and how their personal information will be used by organisations. For example, only 32% of Australian consumers surveyed by the Office of the Australian Information Commissioner (OAIC) feel in control of their personal information, while 50% of consumers feel they have no choice but to accept privacy terms imposed by organisations.¹ Research by the Consumer Policy Research Centre (CPRC) confirms similar sentiment, revealing that only 7% of Australians feel companies give them real choices to protect their privacy online.²

Further, consumers do not understand terminology used by organisations in many privacy notices when they attempt to make informed choices. One of the difficulties consumers face in understanding privacy terms is the wording organisations choose to describe the kind of data they collect, use, and disclose to others for their various commercial purposes. It appears that much of this wording is designed to avoid consumers understanding or objecting to the collection and use of their personal information.

Organisations describe types of information collected in ways that are confusing and unfamiliar for consumers — such as ‘pseudonymised’, ‘anonymised’, ‘hashed’, ‘audience data’, and ‘aggregated’. These descriptions do not have any definition in law nor any fixed meaning in practice.³ They also appear to suggest that the data in question is not related to the consumer as an individual and cannot be used to track, monitor, profile, single out, exclude, or influence the consumer.⁴

Aside from confusing and potentially misleading consumers, these descriptions are not in keeping with the distinctions which are important under privacy law. The law distinguishes between 'personal information' which is covered by the *Privacy Act* and information which is not 'personal information' that generally falls outside the *Privacy Act*.⁵ It is therefore, for the most part, entirely irrelevant that personal information is pseudonymised or hashed, for example. The organisations in question may still be dealing with personal information, which is subject to the Australian Privacy Principles (APPs) under the *Privacy Act*.

Part 1 of this report explains the findings of a survey conducted by CPRC regarding Australian consumers' perceived understanding of descriptions of information used in privacy notices, as well as their perceptions of the risk that each category of information could be used to single them out as an individual and/or influence what they see online.

Part 2 examines the meaning of these descriptions of information in practice and under the Australian law and the law of other major jurisdictions to demonstrate both the obstacles and challenges for consumers in understanding the meaning of privacy terms presented to them, and the problematic and inconsistent use of this language in Australian privacy notices.



“ I avoid many websites and social media companies because I don't like their information management, but it's practically impossible to be online and not have your information used. ”

Comment by CPRC survey participant

Survey methodology

The aim of this survey was to determine consumer perceptions of their understanding of, and risks associated with, different descriptions of information related to people which organisations collect, use, and disclose to others. Each of these terms are used in privacy notices displayed to Australian consumers by various retail companies.⁶ They are also used in privacy notices displayed by data brokers on their Australian websites.⁷

We asked consumers about their perceived knowledge and understanding of these types of information, rather than directly testing their knowledge of these terms. This is because it is not possible to test consumer knowledge of terms when many of these have no fixed meaning under the law or in practice: for example, ‘aggregated’, ‘anonymised’, ‘hashed email address’, ‘pseudonymised’, ‘audience data’ or ‘device ID’.⁸ Even a term such as ‘de-identified information’, which is defined under the *Privacy Act*, appears to be used inconsistently by organisations.⁹

As such, the statistics in this report are likely to underrepresent consumers’ lack of knowledge because our survey did not test consumers on their knowledge but asked for their opinion about whether they understood these terms. Some groups of consumers have likely overestimated their understanding of the terms.

The survey design was led by CPRC with expert advice and review from A/Prof Katharine Kemp of UNSW Sydney. For ease of reference, we refer to survey respondents as ‘consumers’. This survey was undertaken from 18 to 22 September 2023 with a nationally representative sample of n=1,000 consumers.



Part 1: Survey Findings

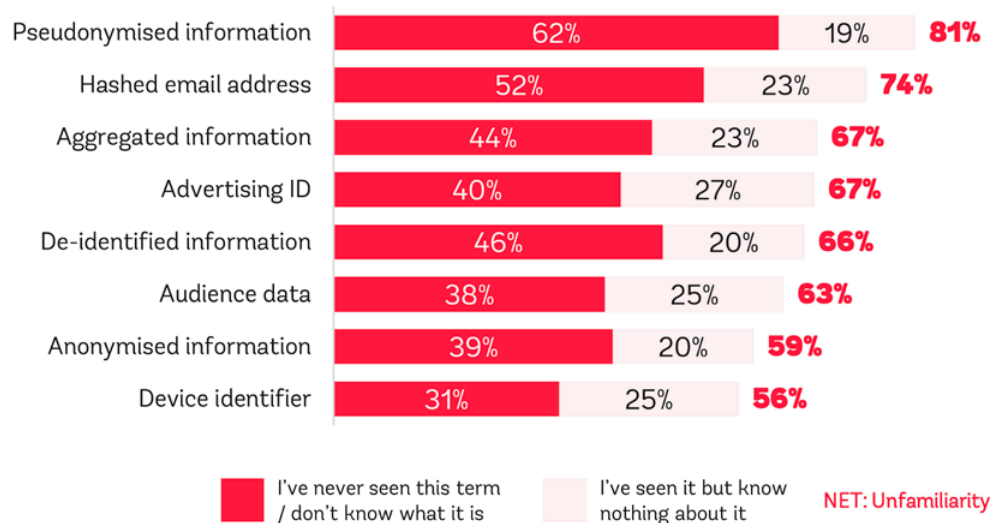




Consumer recognition of data tracking descriptions

Most consumers report that they have no knowledge of, or familiarity with, the terms ‘pseudonymised information’, ‘hashed email addresses’, ‘aggregated information’, ‘advertising ID’, and ‘de-identified information’. These terms are often used in the privacy terms of consumer-facing businesses when describing information that they collect from other businesses or provide to other businesses.

Terms with least familiarity

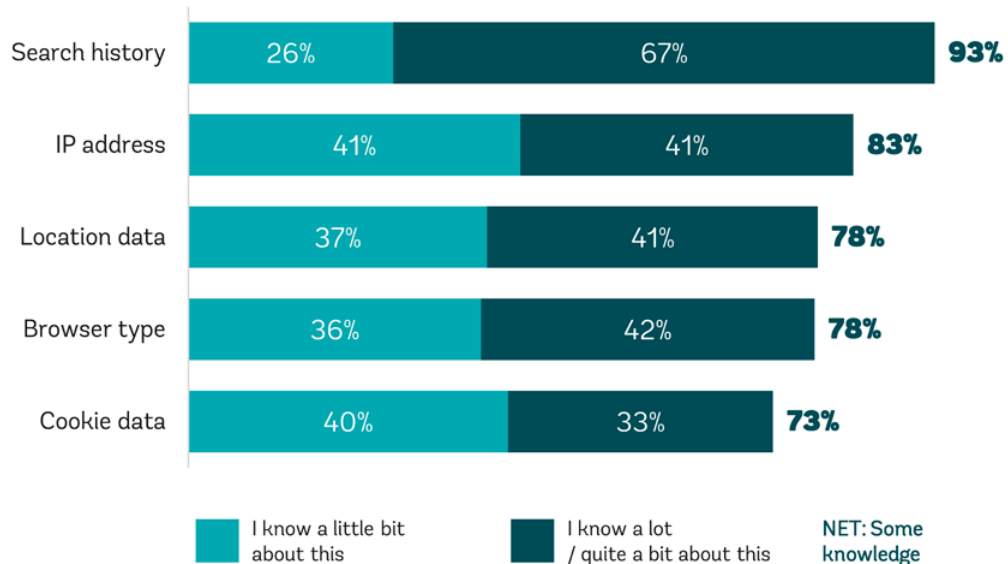


Q: Here is a list of terms that you may have seen, when using products and services, both online and offline. For each term below, how much knowledge do you have about what it is and what it means? Note: Chart shows types of information receiving 50% or more unfamiliarity / uncertainty.



In contrast, consumers are much more confident of their knowledge of the meaning of terms such as ‘search history’, ‘IP address’, ‘location data’, and ‘browser type’. This is in keeping with the intuition that these are likely to be terms that consumers have encountered in their own use of the internet and digital services.

Terms with most familiarity



Q: Here is a list of terms that you may have seen, when using products and services, both online and offline. For each term below, how much knowledge do you have about what it is and what it means? Note: Chart shows types of information receiving >50% at least some knowledge.



Women (17%) are half as likely as men (34%) to believe they have strong or sound knowledge of the meanings of privacy terms used in the survey. Men between 35 and 54 with heavy online activity tend to be most confident about their knowledge.

However, a recent OAIC survey indicated that, despite having greater confidence in their privacy knowledge than females, males had lower privacy knowledge when tested.¹⁰

“ I tried to adjust the [cookie] settings on a website that I visited. However, the process was so complicated and time consuming that I gave up. Yes, they allow a user to control what information they collect BUT it's not a user-friendly process that allows changes to be made quickly and simply. The information gathering continues unabated! ”

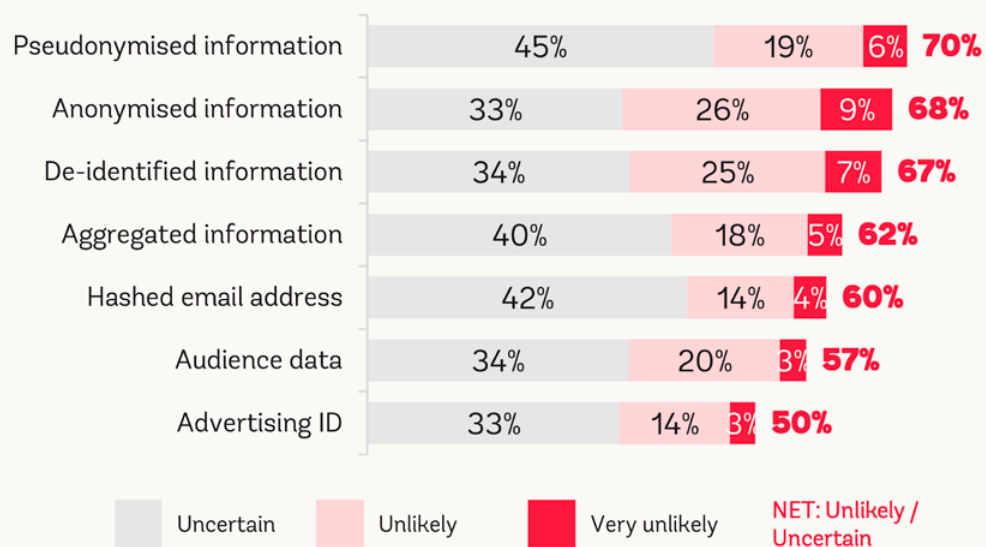
Comment by CPRC survey participant



Consumer understanding of tracking and targeting capabilities

Consumers' lack of knowledge about the meaning of certain terms appears to prevent them from understanding which types of information can be linked back to them or influence what they are shown online.

Uncertainty / perceived unlikelihood of items pinpointing them as an individual

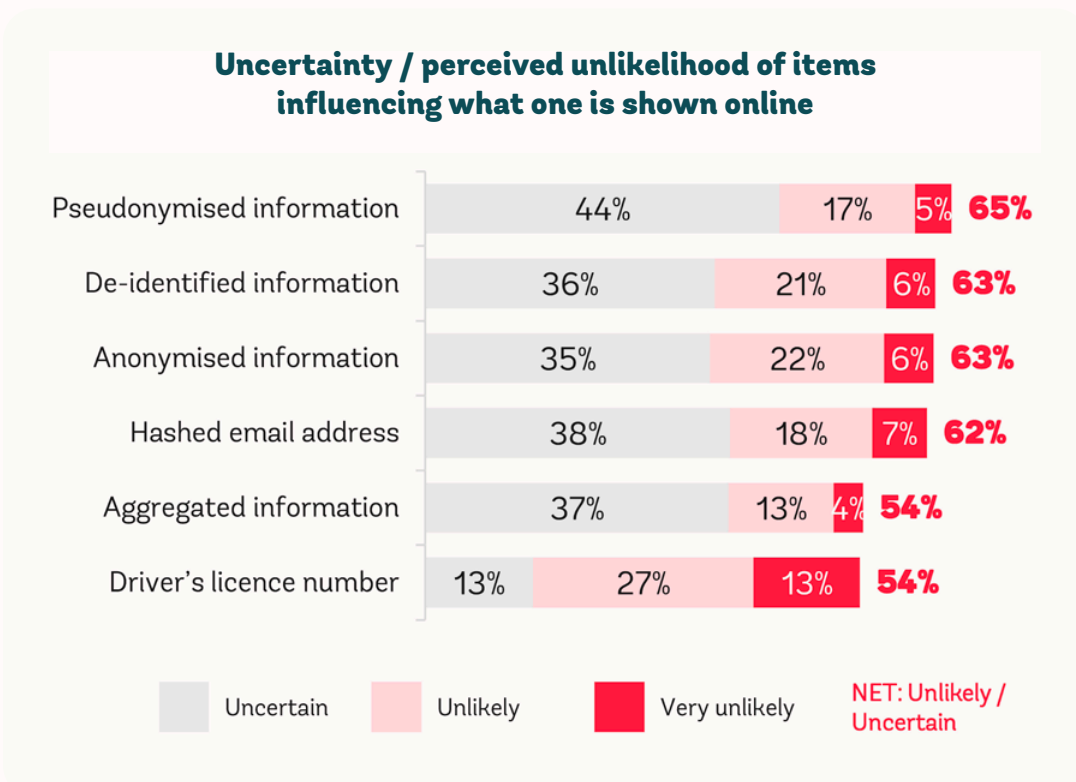


Q: In your opinion, what do you think is the likelihood that this type of information can be traced or linked back to you specifically, that is, used to single you out as an individual? Note: Chart shows types of information receiving 50% or more perceived unlikelihood/uncertainty.

The less familiar consumers are with a category of information, the less likely they are to think that type of information could be traced or linked back to them or used to *single them out* as an individual.


Age and gender also impact perceptions of risk. There is a skew towards females perceiving lower levels of risk that types of information can be used to single them out. Younger consumers believe it is less likely that even certain familiar categories of information — such as search history or browser type — could be linked to them as an individual.

Again, the less familiar consumers are with a category of information, the more uncertain they are about whether that information can be used to *influence* what they are shown online.



Q: In your opinion, what do you think is the likelihood that this type of information can be used to influence what you are shown online – e.g. in advertising? Note: Chart shows types of information receiving 50% or more perceived unlikelihood/uncertainty.

Pseudonymised information is regularly used to influence what consumers see online. However, 65% of consumers are either uncertain of this or believe it to be unlikely.



“ Clearly somehow my email is being shared around to wherever sends out these bogus emails with no content. ... I have no idea how to stop them or find out what causes them. ”

“ I used a website to see what third parties had shared and accessed my information. It was alarming but I don't know how to rectify this. ”

“ I did not sign up or anything but [the] company knows my location. ”

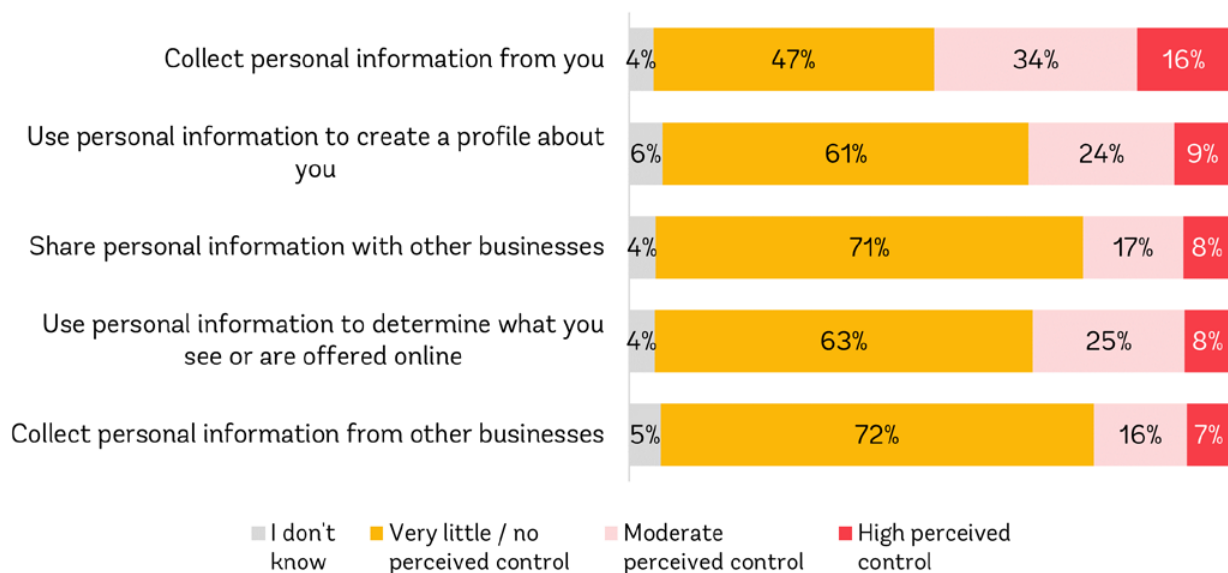
Comments by CPRC survey participants

Consumer perceptions of control over personal information

In general, consumers tend to perceive that they lack control over online businesses sharing their personal information with other businesses. Older consumers tend to be more sceptical of the control individuals have over what businesses can do with their personal data.


However, there appears to be a higher level of perceived control over what personal information businesses can collect from the individual themselves; one in two consumers believing they have at least moderate control over this.

Perceptions of control over what businesses do with personal information



Q: Overall, how much control do you feel that you have in relation to what personal information of yours that businesses online: Collect from you? Collect from other businesses? Share with other businesses? Use to create a profile about you? Use to determine what you see or are offered online?

Overall, 72% believe they have very little or no control over what information is collected from other businesses; 71% believe they have very little or no control over businesses sharing their personal information with other businesses.



“ I have a rare medical condition, I am a Medibank Private member, my medical data including name and email address was stolen and on the dark web and now in addition to battling illness, I am daily battling fake scam emails and texts. It feels very unfair. ”

“ I feel that this is taking away my choice. They are holding it over me — give us the info or we wouldn't let you use [our] stuff. It's very frustrating, especially when the info they are asking for is not necessary for what I want to do on that site. ”

Comments by CPRC survey participants

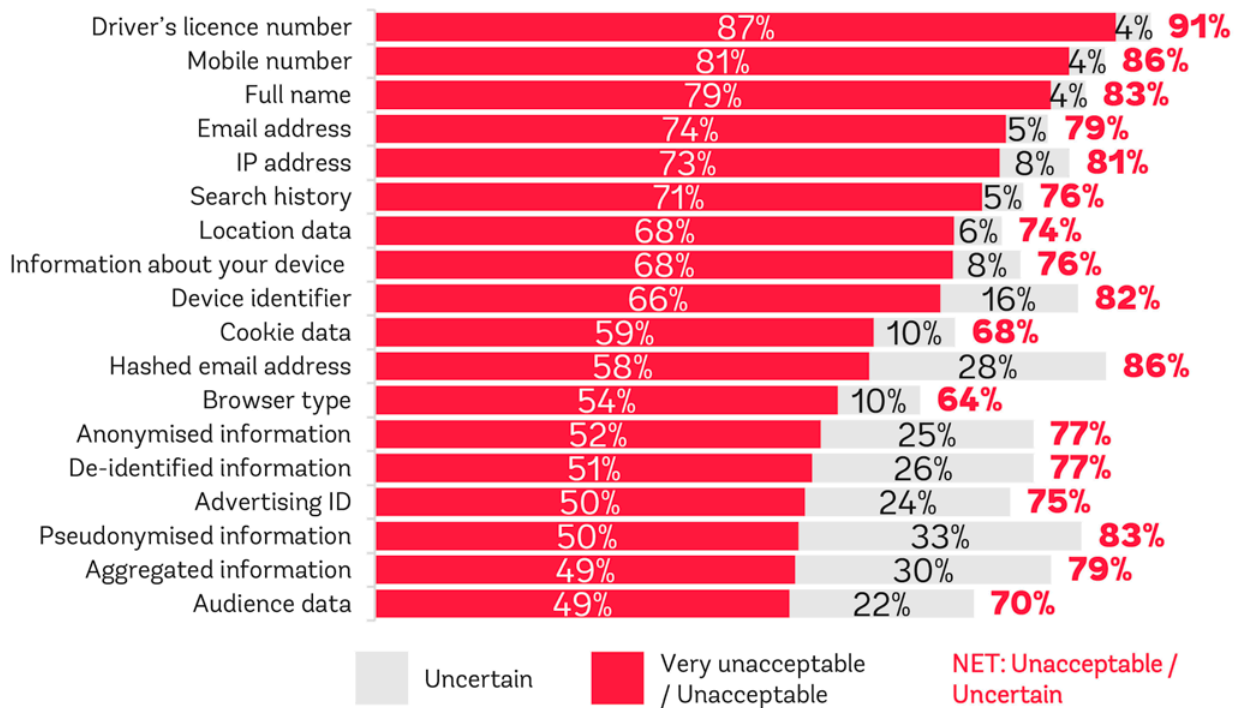


Use of personal data by third parties

Most consumers feel it is unacceptable for businesses they are not directly in contact with to use data including their search history, location data, information about their device, device identifier, cookie data, or hashed email address.

However, data brokers, data analysts and other 'data partners' not in direct contact with consumers commonly use such data.¹¹

Unacceptability / uncertainty of other businesses using personal information



Q: How do you feel about each piece of information below being used by businesses you're not directly in contact with (information can be used for activities such as marketing products to you, or creating a profile on you)?

This is consistent with earlier survey results regarding data practices that consumers regard as misuses of their personal information.¹²

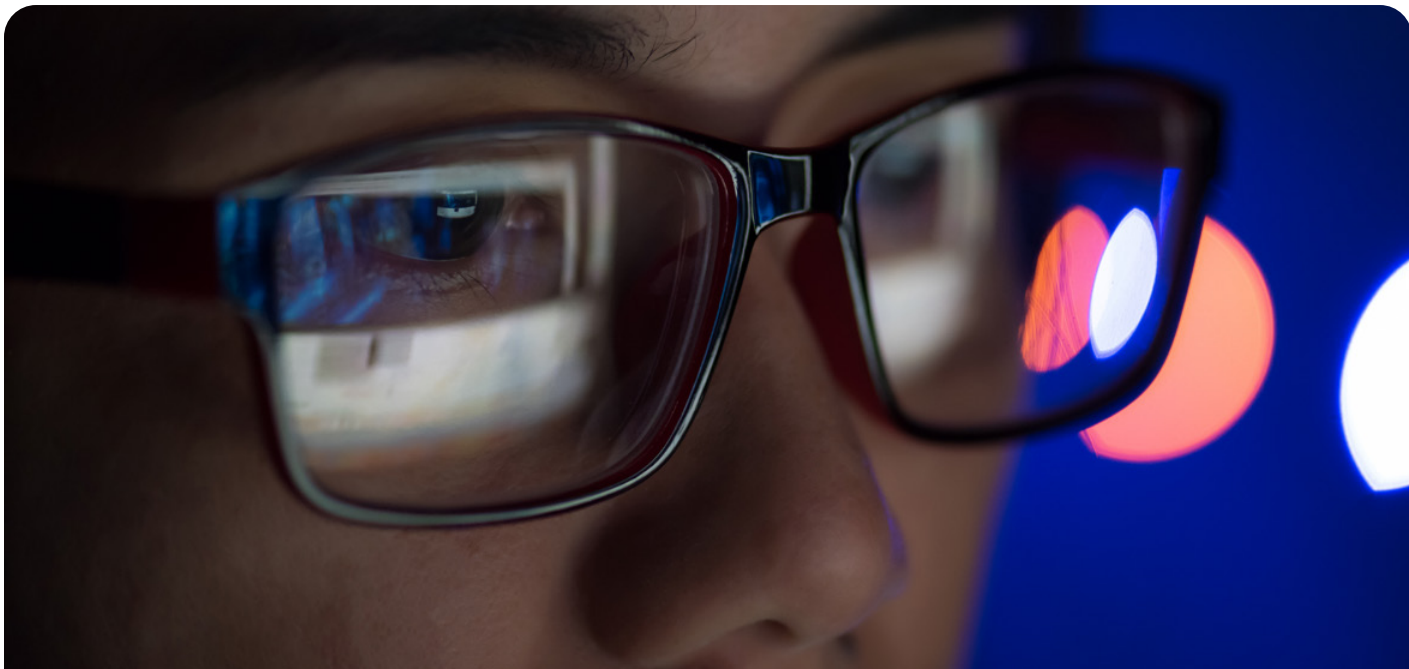


“

I think it's really scary that everything we do or see or talk about daily is always heard and reviewed for advertising purposes through our technological devices such as phones, tablets or laptops. It is a breach of personal privacy and I think it's unacceptable.

”

Comment by CPRC survey participant



Consumer impact: lack of trust, frustration, anxiety and anger

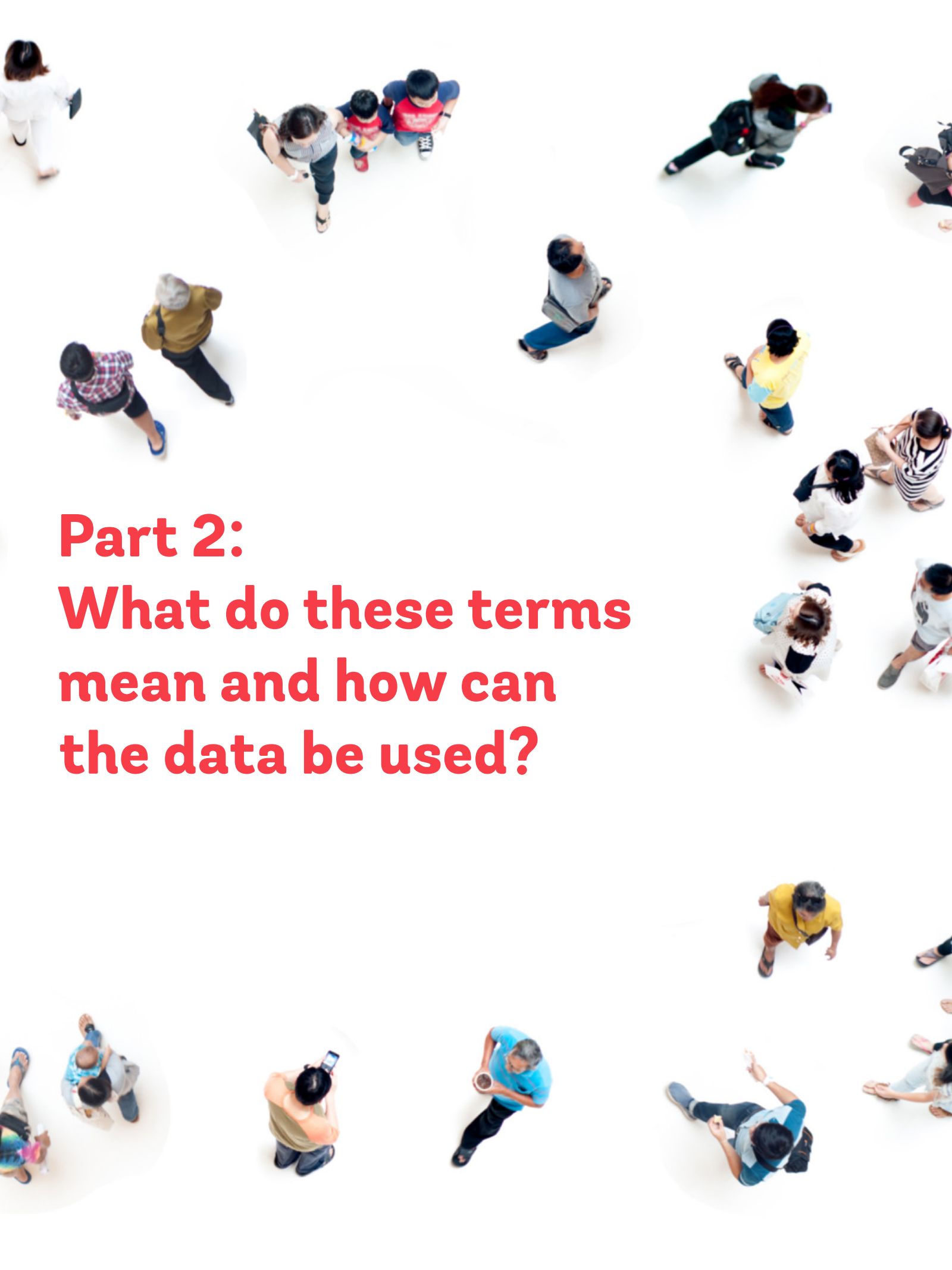
Consumers feel distrust, frustration, anxiety and/or anger about their inability to control how their information is collected and used. Survey respondents were asked an open-ended question about whether they wished to share any recent experiences online. Trends in responses to this question included comments about anger and frustration over thwarted efforts to protect privacy; anxiety about data security and impacts of data breaches; comments about 'scary' developments in data practices; and discomfort and concern about how advertising is targeted.

“ I no longer trust anyone and with no company taking responsibility for these hacks I believe that providing any personal information [online] is flawed, unsafe and should not be done. ”

“ I have had emails from sites that say they have information on me and they will upload it ...I ignore them and delete them ..but it makes me anxious. ”

Comments by CPRC survey participants

Aside from direct economic loss and increased exposure to risk, inappropriate data practices take their toll on consumers through ongoing negative feelings of distrust, anger, frustration, and anxiety.¹³ These feelings, in turn, can lead consumers to avoid beneficial products and services causing further detriment in the form of welfare losses to the individual, suppliers and society in general.¹⁴

An aerial, top-down view of a diverse group of people of various ages and ethnicities scattered across a plain white background. Some individuals are standing alone, while others are in small groups. The people are dressed in casual, everyday clothing. The overall scene suggests a public space or a gathering of people.

Part 2: What do these terms mean and how can the data be used?



In this section, we explain the use of various terms used to describe information collected about people. Because these terms must be understood in the context of the central concept of ‘personal information’ (the kind of information covered by the *Privacy Act*), we present them in an order that builds on the previous terms conceptually, rather than in alphabetical order.

Personal information

The *Privacy Act* imposes data handling obligations on organisations and government agencies under the Australian Privacy Principles (APPs). The obligations under the APPs only apply to ‘personal information’ and explain when and how the covered entities can collect, use, and disclose personal information, as well as what privacy policies and notices they must publish, how they must store and delete personal information, and requirements to permit individuals to access and correct their personal information.¹⁵

The *Privacy Act* defines the core concept of ‘personal information’ to include information or an opinion about an *identified individual*, but also information or an opinion about an individual who is *reasonably identifiable*.¹⁶ This means that a record can be covered even where it does not use the relevant individual’s name, date of birth, email address or mobile phone number, for example.

Pseudonymised information

There is no definition of ‘pseudonymised information’ under Australian law and its meaning therefore lacks certainty. The term is used in privacy notices directed at consumers and in the descriptions of some marketing and data services offered to businesses.¹⁷ In this context, it generally refers to information which has had traditional identifiers such as a name or email address or phone number removed and replaced by a unique number (or alphanumeric string).

This allows data in respect of one individual to be matched and combined between organisations — including data brokers — without the use of more traditional identifiers. This can, for example, allow each of these organisations to develop a more detailed profile on the individual by matching and combining the data they have all collected in relation to that individual. The use of the term in Australia does not indicate to what extent personal information related to the pseudonymised data is kept separate through technical and organisational measures, and therefore how easy it would be to link the individual to their profile.

The OAIC has not provided specific guidance about whether ‘pseudonymised information’ as such is ‘personal information’, but its guidance on when an individual is ‘reasonably identifiable’ from particular information is relevant on this question.¹⁸ According to the OAIC guidelines, the question whether an individual is ‘reasonably identifiable’ will depend on considerations that include “*other information either held by or available to the APP entity that holds the information*” and “*whether it is possible for the individual or entity that holds the information, using available resources (including other information available to that individual or entity)*”.¹⁹ By the OAIC’s reasoning, pseudonymised information can therefore be personal information where it is possible for the relevant organisation to use information and resources available to it to determine which individual the collected information is about.²⁰



The position is made clearer under the EU General Data Protection Regulation (GDPR) and the UK GDPR. According to Recital 26 of the GDPR:²¹

“[p]ersonal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered information on an identifiable natural person.”

Pseudonymised information is therefore personal data which falls within the scope of the GDPR.

According to the UK GDPR, 'pseudonymisation' is:²²

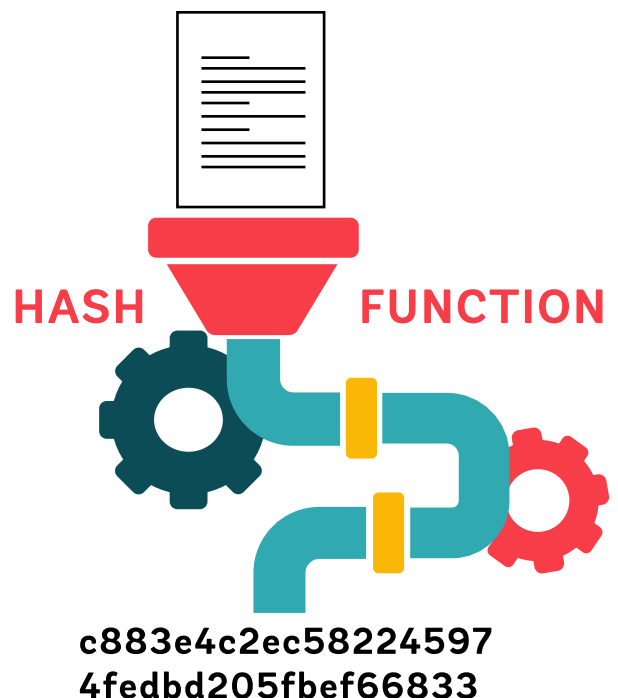
"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

The UK ICO acknowledges that pseudonymisation can be used as a security measure to reduce risks to data subjects (for example, where two groups of employees in an organisation need access to the same data about individuals but only one of those groups needs to know the identity of each individual to whom the data relates), but that it remains 'personal data' which is covered by the GDPR.²³

Hashed email addresses

'Hashed email addresses' (and hashed phone numbers) can be used as pseudonyms which may assist in linking various collections of information about an individual in the pseudonymisation processes above. Again, this is not a term defined under Australian law. 'Hashing' refers to the application of a particular hash function (or formula) to an email address which produces a string of numbers and letters that bears no resemblance to the email address. It is therefore impossible for a human to read a hashed email address and associate it with a particular individual without further information.

However, if two or more organisations arrange to apply the same hash function to email addresses which they each hold this will result in an identical string of numbers and letters for any email address they have in common. In this way, organisations often transfer information to each other in association with a given hashed email address (and without the use of any further name or email address) in the knowledge that all the information relates to the individual associated with the original email address. This is the basis of many 'data matching' arrangements which allow organisations to develop more detailed profiles on their customer with the addition of further personal information collected from third parties and/or to track a given customer across different websites and apps.²⁴



De-identified information

'De-identified' information is not personal information and therefore falls outside the scope of the *Privacy Act*. Organisations have an interest in arguing that information is de-identified, because the obligations imposed on organisations under the APPs do not generally apply in respect of de-identified information. However, references to 'de-identified' information in published privacy notices do not always indicate that the information cannot be linked back to the individual, both due to lack of understanding of the legal meaning of the term and the ongoing risk of re-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".²⁵ The OAIC states that de-identification is generally a two-stage process of removing personal information (such as name and date of birth) and removing information that may allow the individual to be identified (such as a rare characteristic or a rare combination of characteristics).²⁶

There appears to be a trend of data businesses making self-serving claims that certain information is 'de-identified' and therefore, expressly or impliedly, not covered by the *Privacy Act*. These claims of de-identification require scrutiny especially in cases where businesses are acquiring or matching extra information about an individual by agreeing with other businesses on a pseudonym for the individual and claiming that information exchanged under that pseudonym is not personal information even though it adds to their profiles on the individual. The same result is often achieved by an intermediary data broker providing a data matching service which relies on the allocation of a pseudonym or unique code to each individual.²⁷



Even de-identification as defined under the *Privacy Act* does not necessarily remove all risk that the individual will be re-identified. It may be possible, for example, that de-identified information will be linked to the relevant individual if it is matched with another dataset, especially with advances in machine learning. De-identification is not a permanent state; it can be undone.

The OAIC has recently recommended that the term 'de-identified' should be replaced with 'anonymised' in the *Privacy Act*, because it believes clarification is required to avoid confusion with technical definitions of 'de-identification' used by organisations, which impose lower

standards than the legal definition of the term in the *Privacy Act*.²⁸ It points out that the technical understanding of 'de-identification' may only require the application of some de-identification techniques (such as the removal of name and contact details) without ensuring that the information is no longer about a reasonably identifiable individual.²⁹

An individual might reasonably be identified by their other uncommon characteristics or combinations of characteristics. For example, an unnamed individual might be identified by their age range, region and birth date of their eldest child if they were unusually young or old when they became a biological mother; or by their location data at particular points of day mapped across a time period; or by the details of the last five transactions on their credit card.³⁰



De-identification claims: Quantium ‘does not operate as a data broker’

Quantium’s claims about its data business provide a highly concerning example of some organisations’ current interpretation of ‘de-identification’. Quantum is part of the Woolworths Group and conducts a data business which uses information about individuals, including information sourced from various consumer-facing organisations that are clients of Quantum.

Quantium is recognised as a supplier of data broking services by the ACCC in its DPSI Data Brokers Issues Paper, and nominated as a data broker in submissions to that inquiry.³¹ However, Quantum has claimed in its submission to the ACCC that it is not a data broker and that “it does not share or sell personal information or any other information on persons to third parties”.³² Further, Quantum’s Privacy Policy claims that its data business does not deal in personal information, as explained in the extracts in Table 1 below.

According to Quantum, it uses ‘de-identified’ information to provide its data services but it provides ‘insights’ and ‘modelled scores’ about individuals to its clients because Quantum **collects and combines data about each individual using a unique code for that individual ‘transactor’** instead of their name.³³ The clients receiving the further information from Quantum about each individual know the name and/or contact details of that person, but Quantum claims its collection, use and disclosure of the information is not covered by the *Privacy Act*.

In our view, such information should be regarded as ‘personal information’ under the *Privacy Act*. Quantum’s argument is almost certainly that the information is de-identified in its hands since Quantum itself is contractually prevented from learning the name or identifying details of the individual associated with the unique code.

However, Quantum is apparently making its profit by providing extra information about an individual knowing that its clients can identify, influence, and address that individual from the information provided, even if Quantum uses a code for that individual. If there is currently doubt that this is personal information in the hands of the data intermediary, urgent legislative clarification is required to avoid a mockery of the *Privacy Act*’s objectives.

Table 1: Quantum’s claims about ‘de-identified’ information in its data business

<p>Quantum Privacy Policy Extract³⁴</p>	<p>Significance</p>
<p>“The data we receive from our clients contains information about their transactions with their customers or suppliers.”</p>	<p>Quantum receives information from its business clients about transactions between the businesses and their customers.</p>
<p>“Our clients provide this data in de-identified form, after they remove the personal identifiers of any individual person, so that an individual person is not identified or reasonably identifiable by us.”</p>	<p>Quantum says it receives this data in “de-identified form” and implies that it does not regard this as “personal information” covered by the <i>Privacy Act</i>.</p>
<p>“In our core business data is generally provided to Quantum in de-identified form after personal identifiers of individuals have been removed by our clients but with code that enables a single unique de-identified transactor to be associated with the data sets made available to Quantum by different Quantum clients.”</p>	<p>However, Quantum indicates that the “de-identified” information about a given individual received from various Quantum clients will be linked using a unique code associated with that individual.</p>
<p>“This is done through a de-identified code linkage process.”</p>	<p>Various data received about an individual are linked via a unique code which is likely a hashed value from an email address or similar identifier. Various business clients will use the same code for that individual.</p>
<p>“Using this process Quantum may draw inferences about an unidentified individual’s behaviours, interests and preferences, and use these inferences to provide insights reports to our clients ...”</p>	<p>Quantum draws inferences about the individual’s behaviours, interests, and preferences, which it uses to provide further information about the individual to its clients.</p>
<p>“Where insights from Quantum’s data analytics services are provided to our clients at an individual level, these insights are provided as modelled scores that are applied to de-identified data sets.”</p>	<p>Quantum provides its clients with opinions about how an individual is likely to behave or attributes the individual is likely to have, based on all the information it has combined about that individual.</p>
<p>“The provision of any modelled scores to a client is subject to strict contractual provisions that require that the client use such modelled scores in compliance with all applicable privacy laws.”</p>	<p>Quantum implies that the information it provides to its clients about an individual is further personal information in the hands of the client, while claiming it is not personal information in Quantum’s hands.</p>



Anonymised information

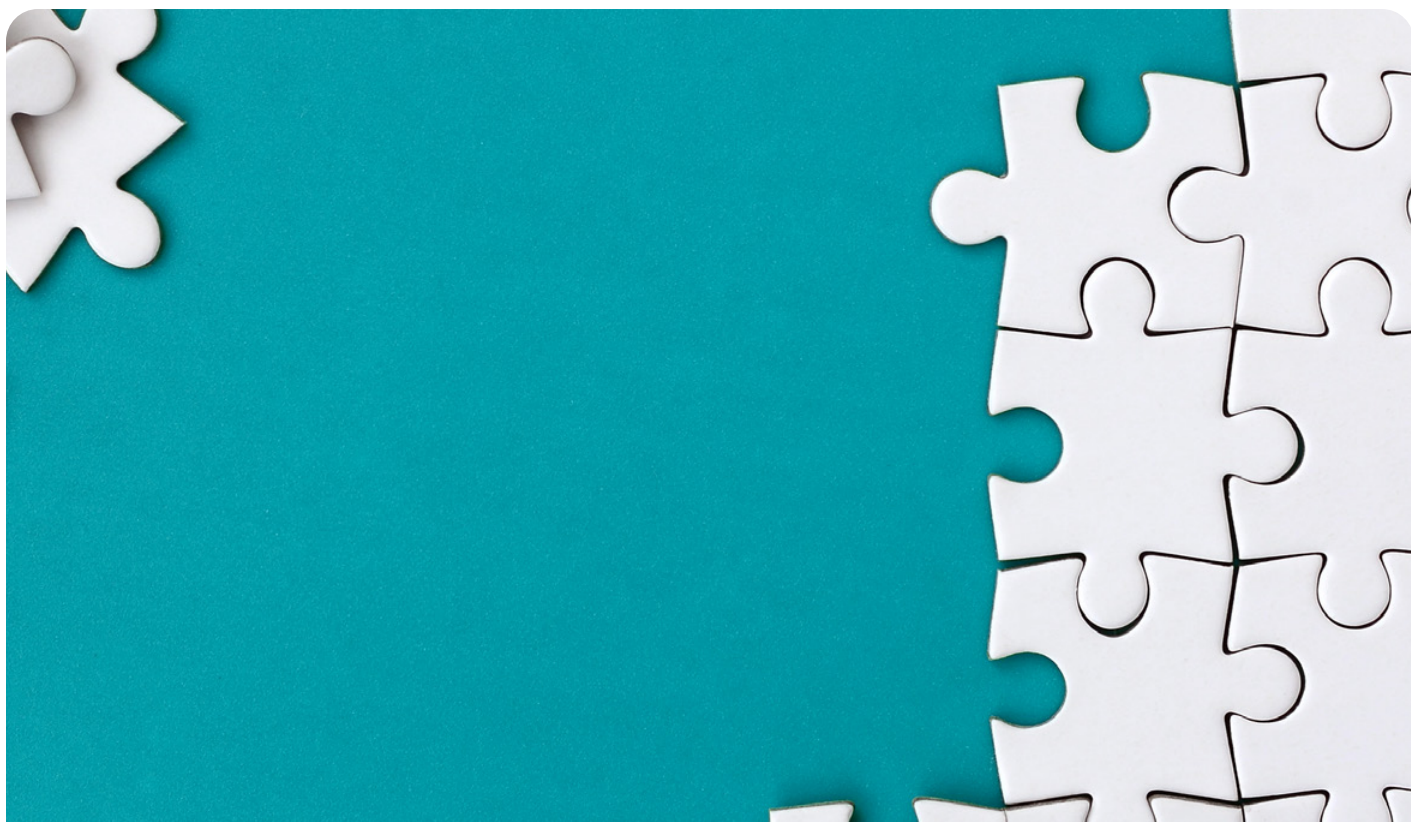
The term ‘anonymised information’ is not defined under Australian law and its meaning is therefore uncertain. In some cases, it seems organisations using this term only intend to indicate that the individual’s name and/or contact details have been removed from the record. This would fall far short of the meaning of this term under the laws of other countries where the term ‘anonymous information’ is used in preference to ‘de-identified information’.

According to the GDPR, the principles of data protection should “not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable”.³⁵

Similarly, the UK GDPR does not apply to information that has been ‘anonymised’. The UK ICO explains the difference between ‘anonymisation’ and ‘pseudonymisation’ and the potential confusion between the two:³⁶

“In order to be truly anonymised under the UK GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified. However, if you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised. This means that despite your attempt at anonymisation you will continue to be processing personal data.”

The OAIC has recently recommended that the *Privacy Act* should be amended to use the term ‘anonymised information’ — rather than ‘de-identified information’ — in part so that Australian law will be more closely aligned with international privacy regimes, promoting ‘clarity in legal standards’.³⁷

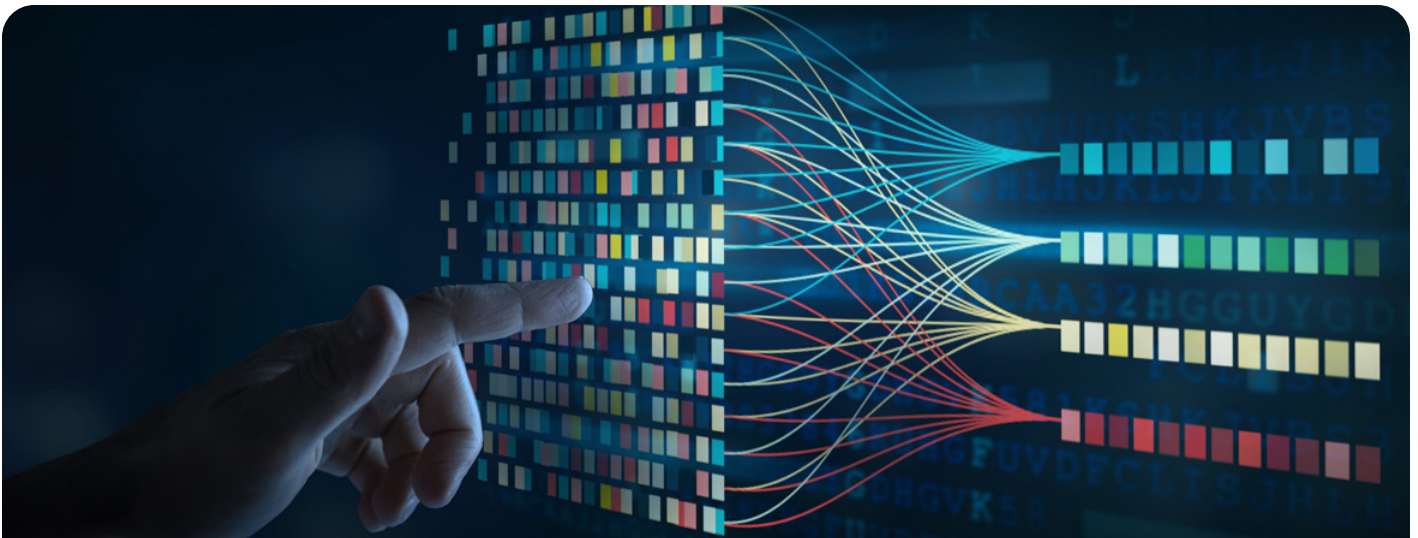


Aggregated information

‘Aggregated information’ or ‘aggregation’ is not defined under Australian law and the term has no fixed meaning. It generally indicates that certain information has been combined and is sometimes intended to indicate that the information is combined information about a group of individuals as a whole rather than containing ‘unit level’ information about any one individual. It is also sometimes used to refer to aggregation of data about a single reasonably identifiable individual, which is clearly personal information.

However, even where ‘aggregated information’ is intended to refer to information that is only about a group of individuals as a whole, that does not mean it cannot contain any personal information. This will depend on the circumstances, including the size of the group, the types of information included and the outputs of the aggregation. For instance, aggregated information that indicates that 100% of men over the age of 50 residing in a certain suburb have been divorced contains personal information about every man known to be over the age of 50 and residing in that suburb.

Aggregated information may also contain personal information if an organisation is able to use additional data and resources to extract personal information from it. To take a simplistic example, the aggregated information may indicate that for all the patients aged between 70 and 80 in a particular care facility, those with Parkinson’s disease also suffer from dementia. If an organisation has access to a list of patients receiving Parkinson’s medication at the facility and their dates of birth, the aggregated information combined with this list will also reveal personal information about the individual’s dementia diagnosis. The likelihood of revealing personal information through combining various aggregated datasets clearly increases enormously with progress in machine learning.³⁸



Audience data

The term ‘audience data’ has no fixed or legal definition. Companies providing marketing or data services often use the term to refer to information about the common attributes or inferred or predicted attributes of a group of individuals, such as gender, age, family situation, location, financial situation, fitness and/or health issues. The company providing the service determines how the group will be described and/or which of the attributes of the individuals will be used to allocate them to groups.

‘Audience data’ is sometimes sold to companies to add information to the profiles they have constructed on their customers. In other cases, companies advertise that they have detailed ‘audience data’ that allows other companies to address or direct advertisements or communications to selected ‘audiences’ with chosen attributes.

Companies using ‘audience data’ sometimes claim that they do not disclose personal information when they direct advertisements or communications on behalf of another organisation to a particular ‘audience’ because they do not provide that other organisation with identifying information of the individuals within that group, but act essentially as a conduit for communications to that group. However, the supply of that information will often determine what information, prices, terms and/or offers an individual in that group is shown or whether they are excluded from receiving certain information or offers. Further, the fact that an individual responds to an advertisement addressed to a particular ‘audience’ may indicate to that organisation that the individual possesses the attributes that ‘audience’ is said to possess.

As an aside, the euphemistic adoption of the word ‘audience’ in this context seems perverse.³⁹ Members of an audience — in the usual sense of the word — generally decide for themselves that they wish to view certain entertainment or receive certain information. In the case of ‘audience data’, the group of people is generally curated by a company of which the individual has no knowledge (let alone contact) without the individual’s awareness or consent for the benefit of that company and other organisations. Various entities then decide what the individual will be shown on the basis of those curations without the individual’s awareness or consent in that process.

Part 3: Conclusions





Confusion, obstruction, frustration – consumer lens on data broking

Consumers do not understand terms regularly used to describe information about them which is collected and shared by an ever-increasing number of organisations for their various commercial purposes. We also know that consumers' lack of knowledge prevents them from understanding that these types of information can be linked back to them or influence what they are shown online. However, consumers should not be expected to become experts in data terminology to confidently participate in the digital economy.

Using terminology which confuses or misleads consumers may aid organisations in avoiding privacy objections or dissatisfaction on the part of consumers. That is, if a consumer is unfamiliar with the term used and has no reasonable way of firmly understanding the meaning of it, the consumer is less likely to feel that the data described presents a risk to their privacy, and therefore less likely to object to the data practice they do not understand.

In addition to undermining consumers' autonomy and choices, the use of confusing terminology contributes to a consumer's lack of trust in organisations to use their personal information fairly. This negatively impacts the organisation's relationship

with its customers and potential customers and jeopardises the quality of information it can collect and use for legitimate purposes. Some consumers indicated that they have declined to use services due to privacy concerns, while others formed the view it was best to provide 'fake' data, such as incorrect names or dates of birth.

These confusing descriptions also undermine the usefulness of privacy notices in general and contribute to a kind of 'learned helplessness' in consumers' privacy decisions. That is, where consumers' experiences in attempting to read privacy notices constantly lead to confusion, obstruction and frustration, those consumers will come to believe that they are unlikely to understand such notices (or make any choice about the data practices). Even if consumers do attempt to make time to read the privacy notices, this can make them less likely to read privacy notices in general and more likely to give up on attempting to take action to protect their information.



Policy recommendations – the data shift Australians deserve

While consumer education might seem an obvious solution to a lack of consumer understanding, education is not the answer in a digital economy that is swiftly evolving and continuing to place significant levels of cognitive load on consumers.

Firstly, many of the terms used have no fixed meaning under the law or in practice and even consumers educated about how these terms are used cannot be certain about the meaning an organisation is giving to that term. Secondly, there are no restrictions on the terminology organisations can use to describe information and old terms may be tweaked and new terms added to the current lexicon, ad infinitum. Thirdly, almost all consumers lack the time and resources necessary to read and interpret the ballooning volume of privacy terms that apply to them and are not offered the choice to refuse tracking of their behaviour and use of their information for additional purposes.

Modernise what it means to be identifiable

The Federal Government must update the definitions of both ‘personal information’ and ‘de-identified information’ in the *Privacy Act* and recognise datapoints such as geo-tracking data within the definition of ‘sensitive data’. The *Privacy Act Review Final Report* proposes amendments to these definitions which will help strengthen protections for Australians that are finally closer to what consumers of other jurisdictions have taken for granted and benefited from for years. Vitally, these changes should include express recognition that information which singles out an individual from the crowd is personal information, even in the absence of a link to traditional identifiers.⁴⁰

Enforce the direct collection rule

While some aspects of the *Privacy Act* may be outdated, the law presently provides a valuable protection by requiring organisations to collect information from the individual themselves unless it is *unreasonable* or *impracticable* to do so. Impracticable means ‘practically impossible’. However, this law has not been enforced in the context of consumer tracking, profiling, and targeting, and no explanation has been provided for the absence of compliance or enforcement.⁴¹

Put the onus on businesses to keep data safe and use it fairly

The *Privacy Act* should be amended to impose an overarching requirement that entities’ dealings with personal information are ‘fair and reasonable’. Australia’s privacy law still relies on consumer notification and consent as the primary means of protecting consumers. Forcing consumers into a situation where they ‘decide once’ about whether to share their data but bear the consequences potentially for the remainder of their life is unfair. The Federal Government must make businesses accountable for the data they are collecting, sharing, and using and shift the onus that is currently placed on individual consumers.

Ensure data is dealt with in the interest of Australians

Once a 'fair and reasonable' requirement has been embedded in the *Privacy Act*, the Federal Government should consider future steps to further enhance the protections via a best-interests duty or a duty of care obligation for data. CPRC's consumer research confirms that Australians support their data being used with the best interests of the community in mind, with 83% agreeing that their personal information should not be collected or used in a way that harms them or others.⁴² Such an obligation, which is already in place across other jurisdictions, would help safeguard individuals who are unable to provide consent, foster a culture of data minimisation (i.e. businesses collecting what they need, not what they want) and address issues of low consumer trust and confidence in both government and industry.⁴³

Make unfair data practices illegal

While the implementation of *Privacy Act* reforms would enable several key protections for Australians when it comes to their data, another reform that can also help address issues raised through data broking practices is a prohibition on unfair business practices. In 2023, the Federal Government commenced consulting on proposals for how such a reform could be achieved in Australia — a law that has existed for decades in other jurisdictions such as Europe and the United States.⁴⁴

The Federal Government should implement the proposed option which includes an overarching prohibition supplemented by a blacklist of practices that are deemed unfair. The blacklist should specifically prohibit data practices that make unfair use of aggregated data about consumer behaviour and preferences such as their vulnerabilities for commercial purposes.⁴⁵ This has the potential to course-correct business models that:

- predicate on opaque business processes that undermine consumer autonomy
- thrive on profiting from exploiting consumer vulnerabilities, and
- fail to provide accessible and meaningful support to customers.⁴⁶

It can lead to businesses (including data brokers) considering data-based practices through a lens of fair outcomes for consumers, enabling regulators to hold businesses accountable when they fail to do so.

Enable strong, proactive enforcement more broadly

In reforming the *Privacy Act*, the Federal Government must ensure that the regulator is adequately resourced to monitor and enforce privacy breaches. It must be empowered to undertake proactive investigations before widespread harm has taken place.

Currently, regulators largely rely on reports from individuals, identifying harm after it takes place. This is not sustainable in a digital environment where harms are difficult for individual consumers to identify and often occur at a community or collective level. Instead, regulators need to proactively uncover harm that is currently obfuscated. Regulators should have the ability to push businesses to be radically more transparent about how they use consumer data.

One way to achieve this is to consider implementing reforms similar to either a product intervention power that currently exists for the Australian financial sector or the provision of interim and permanent bans under Australia's product safety framework.⁴⁷ Such reforms are designed to empower regulators and governments to address emerging issues and ascertain how consumers may be protected from foreseeable harms.

Many businesses continue to focus their efforts on finding new ways to track and profile the consumer — and seek extra information about the consumer from third parties — despite repeated evidence that consumers regard these data practices as misuses of their personal information. These practices are hidden behind confusing and sometimes misleading privacy messaging.

Consumers are understandably frustrated, anxious, and angry about the unfair and untrustworthy ways organisations presently make use of their personal information. Urgent law reform is needed to ensure that consumers can participate in the digital economy with full confidence that the law requires dealings with their personal information — including data that singles them out from the crowd — to be fair and trustworthy and that the law will be enforced.

Annexure 1:

Examples of privacy terms of consumer-facing businesses

Amazon Australia:

“Some third-parties may provide us **pseudonymized information** about you (such as demographic information or sites where you have been shown ads) from offline and online sources that we may use to provide you more relevant and useful advertising.”⁴⁸

[It is not clear why Amazon uses the word “pseudonymized” when the data it collects from third parties appears to be personal information. Consumers are liable to be confused about the significance of the word “pseudonymized”.]

Aramex Australia:

“In addition, we use data from Google’s interest-based advertising or third party **audience data** (such as age, gender and interests) with Google Analytics to help us understand how user activity varies based on these factors.”⁴⁹

Binge:

“We, or our service providers, may use your information to:

...

personalise the marketing of our Services to you on third party sites, applications or social media services, where **we may match an anonymised common account identifier (such as a hashed email address)** with third party sources to send you personalised communications (or to exclude you from receiving a particular communication) on the third party site, application or social media service;...”⁵⁰

[This term leaves open the possibility that the individual is “reasonably identifiable” from the information which is shared with other organisations.]

Domain Group:

“You may use our website without providing any personal information. In this case, we will collect metadata that results from your usage of our website including browser type and version, operating system and interface, website from which you are visiting us (referrer URL), webpage(s) you are visiting on our website, date and time of accessing our website and internet protocol (IP) address. We use this data to improve the quality and services of our website and services by **analysing the usage behaviour of our users in anonymised form** ...”⁵¹

Meta:

“In some cases information is de-identified, aggregated or anonymised by third parties so that it no longer **identifies** individuals before it’s made available to us. We use this information as described below **without trying to re-identify** individuals.”⁵²

[It appears that Meta is not ruling out the possibility that an individual is “reasonably identifiable” from the data in question or Meta’s use of the data may re-identify individuals “without trying”, despite labelling it “de-identified, aggregated or anonymised” and thereby creating the impression that it is not personal information.]

News Corp Australia:

“We may also remove certain information or alter the information we collect about you so you can no longer be identified from that information. We do this so that we can use it or disclose it to third parties for other purposes.”⁵³

[News Corp does not actually claim that this information is “de-identified” or not “personal information” or that the individual is not “reasonably identifiable” from the information. Is it still personal information, but News Corp intends to disclose it to third parties for other purposes in any case?]

Sixt.com.au:

“Our collaboration with advertising partners is based on retargeting technologies. These enable us to better customise our offers according to your interests, and to win back your custom for our products and offers. We pursue this goal using a cookie-based analysis of previous visit patterns that involves creating pseudonymised user profiles.”

... “In order to design and optimise this website accordingly, anonymised usage data is collected and stored in aggregated form and usage profiles are created from this data using pseudonyms.”⁵⁴

[It is not clear why Sixt would need to use pseudonyms if the data used is anonymised and aggregated. Pseudonymisation would only be required if the underlying data was still personal information.]

Annexure 2: Examples of privacy terms of data broking services

Equifax Australia Privacy Policy:

“For third party online behavioural advertising, we may disclose any data about your activities which is not personal information and does not allow you to be reasonably identifiable to a third party — for example, **data associated with a cookie, pixel tag, mobile advertising ID or other tracking code** — and permit them to use this data for the purpose of associating that tracking code with your use of our websites, and of third party websites where we or our advertising partners have an arrangement in place to serve ads to you on those third party websites.

We may also collect and use, and permit third parties to collect and use, data from third parties **about your online or offline activities, as linked by that third party to that tracking code**, to facilitate display of advertisements, goods, services, recommendations or content to you that are selected using inferences as to your preferences or interests. ...”

“We may also use and disclose **de-identified, aggregated account information** collected through MOGOplus and Tenant Affordability Check for analytical and research purposes. No personal details, like name and address, will be used.⁵⁵

Illion Risk & Marketing Solutions Privacy Policy:

“We also use **aggregated, de-identified information** (this information is not Personal Information as it does not identify any individual/s) for research, analysis and product development. This non-personal information may be incorporated into products and services provided to our customers for their business use.”⁵⁶

LiveRamp Services Privacy Policy:

“Such client sends us a file of their customer data, which we then create a client-specific **pseudonymized LiveRamp proprietary identifiers** (“RampID”) using our algorithm. We then delete all **directly identifiable personal information** received from the clients/partners, unless we are instructed. We exchange this RampID data list (the audience) with our Distribution Partners, who then facilitate the sending or display of the client’s advertisements to those consumers. The recognition process is used to assist our clients with online targeted advertising and measurement of advertising effectiveness. ...”

“We may also collect, use, and share statistical information that is not particular to you or any other individual, but rather represents a category or group with the same or similar interests or characteristics (which we call ‘Aggregated Data’) and that could be derived from your personal information and may be used for any purpose. **You should be aware that Aggregated Data is not considered personal information under law**, as it does not directly or even indirectly reveal your identity. However, if we combine or connect Aggregated Data with your personal information so that it can then directly or indirectly identify you, we

treat the combined data as personal information and only use it in accordance with this Website and Marketing Privacy Policy and relevant laws.”⁵⁷

Oracle Australia Advertising Privacy Policy:

“Personal information that is collected **online** and that may **indirectly** identify you may include, for example:

- unique IDs such as your mobile **device identifier**, or a cookie ID on your browser;
- a connected device identifier such as an ID from a smart or connected television or streaming device (US only);
- ...
- **obfuscated personal information such as hashed email addresses** (direct identifiers are removed);
- ...
- behavioral data of the internet connected computer or device you use when interacting with websites, applications, or other connected devices, such as advertisements clicked or viewed, websites and content areas, date and time of these activities, or the web search used to locate and navigate to a website.”⁵⁸

Quantium Privacy Policy:

“In our core business data is generally provided to Quantium in **de-identified form after personal identifiers of individuals have been removed by our clients but with code that enables a single unique de-identified transactor to be associated with the data sets** made available to Quantium by different Quantium clients. This is done through a de-identified code linkage process. Using this process Quantium may draw inferences about an unidentified individual’s behaviours, interests and preferences, and use these inferences to provide insights reports to our clients which they may use to improve the customer experience that they offer.”⁵⁹

Annexure 3: Data broking definitions

Second-party data broking entails the commercial supply of information relating to an individual where the supplying entity / obtained the information through its own direct relationship with an individual customer (known as 'first party data' for the collecting entity) and supplies it to another entity (known as 'second party data' for the acquiring entity). The broker might originally collect the data directly from the individual themselves, but also by monitoring the individual's behaviour in ways that are not clear to the individual.

Third-party data broking entails the commercial supply of information relating to an individual where the supplying entity obtained the information from various other entities, sources, and/or tracking technologies rather than through its own direct relationship with the individual (making this 'third party data' for the acquiring entity).

Both these kinds of services involve the supply to other entities of information that can be linked to an individual, including inferences, profiles, probabilistic scores or ratings, predictions, and/or allocation to particular 'audiences' or groups of individuals considered to share certain attributes and/or behaviours. These services range from the sale of whole datasets of personal information through to data licences, 'data matching', 'data enrichment', curation of 'audiences', and 'identity resolution'.

Endnotes

1. Office of the Australian Information Commissioner ('OAIC'), Australian Community Attitudes to Privacy Survey (Report, 2023) https://www.oaic.gov.au/_data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf
2. Consumer Policy Research Centre ('CPRC'), Not a Fair Trade – Consumer views on how businesses use their data, (Report, 2023) <https://cprc.org.au/not-a-fair-trade>.
3. As explained in Part 2 below.
4. See Part 1 below.
5. See Privacy Act 1988 (Cth) ('Privacy Act'), ss 6(1), 13(1).
6. See Annexure 1 below.
7. See Annexure 2 below.
8. See Part 2 below.
9. See Part 2 below ("De-identified information").
10. OAIC, Australian Community Attitudes to Privacy Survey (Report, 2023) https://www.oaic.gov.au/_data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf pp 18-21.
11. See Annexures 1 and 2 below.
12. Australian Competition & Consumer Commission (ACCC), Digital Platforms Inquiry: Final Report (Report, 2019) <https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report> pp 389-390.
13. See Katharine Kemp and Melissa Camp, 'Pecuniary Penalties under the Privacy Act: Damage and Deterrence' in Deniz Kayis et al (eds), *The Law of Civil Penalties* (Federation Press, 2023).
14. Ibid.
15. Privacy Act, Sched 1 (Australian Privacy Principles).
16. Privacy Act, s 6(1) ('personal information').
17. See, eg, Annexure 1 below.
18. OAIC, Australian Privacy Principles Guidelines (December 2022) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#de-identification> para B.94.
19. Ibid.
20. This is also consistent with the OAIC's findings as to when an individual will be 'reasonably identifiable' in Commissioner initiated investigation into Clearview AI, Inc. [2021] AICmr 54 (14 October 2021) and Commissioner initiated investigation into 7-Eleven Stores Pty Ltd [2021] AICmr 50 (29 September 2021)
21. General Data Protection Regulation, Recital 26 <https://gdpr-info.eu/recitals/no-26/>
22. Regulation (EU) 2016/679 of the European Parliament (United Kingdom General Data Protection Regulation) ('UK GDPR') <https://www.legislation.gov.uk/eur/2016/679/contents> Art 4(5).
23. Information Commissioner's Office ('ICO'), United Kingdom, What is Personal Data? (Webpage, undated) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/#pd4> accessed 30 January 2024.
24. See, eg, 'Google Ads Help: About the customer matching process' (Webpage, undated) <https://support.google.com/google-ads/answer/7474263?hl=en-AU> accessed 30 January 2024.
25. Privacy Act, s 6(1) ('de-identified information').
26. OAIC, Australian Privacy Principles Guidelines (December 2022) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#de-identification> para B.63.
27. See, eg, Table 1 below.
28. OAIC, Privacy Act Review Issues Paper: Submission by the Office of the Australian Information Commissioner (Submission, 11 December 2020) <https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-2-definition-of-personal-information#de-identified-anonymised-and-pseudonymised-information> para 2.31-2.40.
29. Ibid.
30. See Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague, Health Data in an Open World: A Report on Re-identifying patients in the MBS / PBS Dataset and Implications for Future Releases of Australian Government Data (University of Melbourne, 18 December 2017).
31. See, eg, Equifax, Digital Platform Services Inquiry: Consultation (Submission to the ACCC DPSI March 2024 Interim Report, 7 August 2023); ACCC, Digital Platform Services Inquiry: March 2024 Report on Data Brokers: Issues Paper, (Issues Paper, 10 July 2023) p.7 <https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202024%20report%20-%20Issues%20paper.pdf>
32. Quantum, The Quantum Group (Quantum) submission to the Digital Platform Services Inquiry – March 2024 Issues Paper on Data Brokers (Submission, 21 August 2023) <https://www.accc.gov.au/system/files/Quantium.pdf> accessed 30 January 2024.
33. Quantum, Privacy Policy: The Quantum Group (July 2021) para 4.2 <https://quantium.com/privacy-policy-27-july-2021-web-version-2/> accessed 30 January 2024.
34. Quantum, Privacy Policy: The Quantum Group (July 2021) para 4.1-4.2 <https://quantium.com/privacy-policy-27-july-2021-web-version-2/> accessed 30 January 2024.
35. General Data Protection Regulation, Recital 26 <https://gdpr-info.eu/recitals/no-26/>

36. Information Commissioner's Office ('ICO'), United Kingdom, What is Personal Data? (Webpage, undated) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/#pd4> accessed 30 January 2024.
37. OAIC, Privacy Act Review Issues Paper: Submission by the Office of the Australian Information Commissioner (Submission, 11 December 2020) <https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-2-definition-of-personal-information#de-identified-anonymised-and-pseudonymised-information> para 2.35.
38. See, eg, Kai Packhauser et al, 'Deep Learning-Based Patient Re-identification is Able to Exploit the Biometric Nature of Medical Chest X-ray Data' (2022) 12 Scientific Reports <https://doi.org/10.1038/s41598-022-19045-3>; Elad Jacobson et al, 'De-identification is Insufficient to Protect Student Privacy, or – What Can a Field Trip Reveal?' (2021) 8 Journal of Learning Analytics 83.
39. See Katharine Kemp and Graham Greenleaf, Ignoring Privacy Practices Would Distort Data Broker Issues: Submission on Digital Platform Services Inquiry March 2024 Report on Data Brokers Issues Paper (Submission, 8 August 2023) p. 4.
40. Anna Johnston, 'Individuation: Re-imagining Data Privacy Laws to Protect Against Digital Harms' (Brussels Privacy Hub, Working Paper Vol 6 No 24, July 2020).
41. See Katharine Kemp, 'Australia's Forgotten Privacy Principle: Why Common "Enrichment" of Customer Data for Profiling and Targeting is Unlawful' (20 September 2022) <https://ssrn.com/abstract=4224653>
42. CPRC, Not a Fair Trade – Consumer views on how businesses use their data, (Report, 2023), <https://cprc.org.au/not-a-fair-trade>.
43. CPRC, In Whose Interest – Why businesses need to keep consumers safe and treat their data with care, (Report, 2023) <https://cprc.org.au/in-whose-interest>.
44. The Treasury, Unfair trading practices – Consultation Regulation Impact Statement, (CRIS, 2023), <https://treasury.gov.au/consultation/c2023-430458>.
45. CPRC et.al., Make unfair illegal – Submission from consumer advocates on Treasury's CRIS – Protecting consumers from unfair trade practices, (Submission, 2023) <https://cprc.org.au/submission/make-unfair-illegal>.
46. CPRC, Unfair Trading Practices in Digital Markets: Evidence and Regulatory Gaps, (Report, 2021).
47. CPRC, In Whose Interest – Why businesses need to keep consumers safe and treat their data with care, (Report, 2023) <https://cprc.org.au/in-whose-interest>.
48. Amazon Australia, 'Interest-Based Ads Notice' <https://www.amazon.com/gp/help/customer/display.html> accessed 30 January 2024.
49. Aramex Australia, 'Privacy Policy' <https://www.aramex.com.au/terms-and-conditions/privacy-policy/> accessed 30 January 2024.
50. Binge, 'Privacy Policy' <https://help.binge.com.au/s/privacy-policy> accessed 30 January 2024.
51. Domain, 'Privacy Policy' <https://www.domain.com.au/group/privacy-policy/> accessed 30 January 2024.
52. Meta, 'Privacy Policy: How Meta Collects and Uses User Data' <https://www.facebook.com/privacy/policy/> accessed 30 January 2024.
53. News Corp Australia, 'Privacy Policy' <https://preferences.news.com.au/privacy> accessed 30 January 2024.
54. Sixt, 'Privacy Policy' <https://www.sixt.com.au/privacy/#/> accessed 30 January 2024.
55. Equifax Australia, 'Privacy Policy (Australia)' <https://www.equifax.com.au/privacy> accessed 30 January 2024.
56. illion, 'Risk & Marketing Solutions Privacy Policy' <https://www.illion.com.au/privacy-policy-risk-marketing-solutions/> accessed 30 January 2024.
57. LiveRamp, 'LiveRamp Services Privacy Policy' <https://liveramp.com.au/privacy/service-privacy-policy/#personalinfo> accessed 30 January 2024.
58. Oracle Australia, 'Oracle Advertising Privacy Policy' <https://www.oracle.com/legal/privacy/advertising-privacy-policy.html> accessed 14 November 2023.
59. Quantum, Privacy Policy: The Quantum Group (July 2021) para 4.2 <https://quantum.com/privacy-policy-27-july-2021-web-version-2/> accessed 30 January 2024.