Consumer Policy Research Centre

# Submission by the Consumer Policy Research Centre to the Australian Government - Review into Open Banking - Final Report

**Submission attachment to remain in confidence until 14th May 2018**

23rd March 2018

By email: data@teasury.gov.au

Dear Secretariat,

Consultation Paper: Review into Open Banking—Final Report

The Consumer Policy Research Centre (CPRC) would like to thank you for the opportunity to comment on the final report on Review into Open Banking. CPRC recognises the significance of consumer data sharing for driving innovation and competition. It is without question that effective regulation and data security is essential to establishing consumer trust and participation in Open Banking, in particular through more accurate and simple comparisons of products and services. Equally important is consumer's trust in companies and the system, and real informed consent for Open Banking to work effectively.

As the first major step in Australia towards a system to enable the transfer of consumer data, ensuring that adequate protections are in place now will assist in building consumer and community trust. Without consumer trust, this may jeopardise the many future benefits to flow from the growing field of 'big data' and associated digital advancements.

While the Open Banking consultation process itself has not had scope to more deeply explore emerging issues for consumers from data amalgamation, consumer profiling and the growing international evidence of the risks of discrimination, CPRC requests that the Australian Government, ACCC and OAIC establish a process to explore policy analysis and consultation on these issues. The issues of data amalgamation and the sale of consumer data is relatively new phenomenon crossing the portfolios and disciplines. 'Big data' as it relates to consumer markets, has the potential to significantly transform the consumer experience in both positive and negative ways. Increasing information asymmetry between suppliers and consumers, along with highly developed 'screening' practices to determine eligibility or price discrimination practices have significant implications. As mentioned above, the clear benefits to flow from consumer data need to be balanced with such emerging risks if the community is to derive maximum benefits from reform and innovation.

Consumer Policy Research Centre

In relation to the Review into Open Banking consultation, CPRC would like to further comment on:

- Genuine consumer consent and control
- Data asymmetry—consumer trust and choice
- Consumer protections against unfair use of data
- Consistent approach across sectors

The report highlights some important recommendations that we would like committed to by the Government in the final decision. However, some further considerations are still required which are highlighted in the discussion below.

## Genuine consumer consent and control

### Consumer data and well-functioning markets

The Review rightly highlighted that customers will only use Open Banking if they understand and trust it.

The UK Competition & Markets Authority[1] highlights that in order for consumers and businesses to benefit from consumer data, consumers must be able to trust businesses so that they would continue to provide data. They argue that consumer data can be used to support well-functioning markets if:

> *1) consumers know when and how their data is being collected and used, and have some control on whether and how they participate.*
>
> *2) businesses are using the data to compete on issues that matter to the consumer.*
>
> *3) the use of consumer data benefits both consumers and businesses.*
>
> *4) rights to privacy is protected through the regulation of data collection and use.*
>
> *5) there are effective ways to fairly manage non-compliance with regulation.*

### Lack of genuine consent and control by Australian consumers

CPRC conducted a recent research study surveying 1004 Australians—the results from this study is yet to be released. We kindly ask that that the results used to support this submission remain in confidence until 14th May 2018. The results show that 33% of Australians admit to not reading a Privacy Policy or Terms and Conditions when signing up for a product or service in

[1] Competition & Markets Authority (CMA). (2015). The commercial use of consumer data: Report on the CMA's call for information. Competition & Markets Authority, London, United Kingdom. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

the past 12 months, more than that found in the study conducted by OAIC which reported 12% of Australians never read the Privacy Policy before providing their personal information[2]. Of 67% who read these documents, two-thirds (67%) indicated that they still signed up for one or more products *even though they did not feel comfortable* with the policies.

When asked why they still accepted the Privacy Policies or Terms and Conditions, the most common reason was that it was the only way to access the product or service (73%). This suggests that consumers are lacking sufficient control over the type of data being collected and used, and how they participate. They feel they have no choice but to accept the terms of service or are otherwise denied access to products or services.

**Improving conditions for consent for better consumer protection and control**

Our research also suggests that the current process for obtaining consent through Privacy Policies and/or Terms and Conditions is flawed, because various permissions are bundled in the policy documents and therefore consumers cannot opt out of types of data collection or uses they are uncomfortable with. Nearly all of those surveyed (95%) said they wanted companies to give them options to opt out of certain types of information they can collect, use and/or share. Forty-four percent of consumers feel that it is not enough for companies just to notify them about how they collect, use and share data in the Privacy Policies or Terms and Conditions. Majority of Australians (73%) expect that the Government should mandate companies to provide consumers options to opt out. Surprisingly 19% of Australians wrongly believed that if a company has a privacy policy, it meant they will not share information with other websites or companies, and 22% did not know enough to answer this question. Additional efforts in educating consumers about privacy policies and consumer rights is needed.

Whilst 88% of consumers were aware that companies exchange information about them with third parties for purposes other than delivering the product or service, more detailed discussion in our focus group suggested that consumers are concerned because they do not know where their data goes and how it is used. It is evident that the ability to track and know what their data is being used for is important to consumers.

Australia should adopt the European Union's General Data Protection Regulation standard for consent. Article 7 GDRP[3] outlines conditions for consent:

1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*
2. *If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible*

---

[2] Office of the Australian Information Commissioner (OAIC). (2017). Australian Community Attitudes to Privacy Survey 2017. Office of the Australian Information Commissioner, Sydney, Australia. Retrieved from https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017.

[3] General Data Protection Regulation. Article 5 GDPR Conditions for consent. Available at https://gdpr-info.eu/art-7-gdpr/.

*form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

In other words, consent must be explicit, specific to purpose, unbundled, easy to understand, can be withdrawn, freely given, and not conditional if the data is not necessary for the provision of the service. Common practices such as pre-ticked consent boxes should not be allowed. Companies should not be allowed to unfairly deny customers access to products or services if consumers refuse to provide their data, particularly if the data is not essential to the provision of the products. The ACCC should work with OAIC to set the rules on how companies provide information and obtain consent based on these conditions. The ACCC and OAIC should consult with experts (e.g. legal experts, data ethicists and consumer groups) and test consumer comprehension to check the effectiveness of the consent process. This should be a pre-condition to reform.

'Recommendation 4.2- modifications to privacy protections', 'Recommendation 4.5- customer control', 'Recommendation 5.6- persistent notification' and 'Recommendation 5.11-transparency' should be adopted at the very least as a minimum level of consumer protection. Furthermore, CPRC supports the suggestion that control and consent in the Privacy Act extend to include small businesses as liable data holders so that consumers are better protected.

**Response to key recommendations**

- CPRC recommends that Consumer Data Right and Open Banking should adopt the European Union's General Data Protection Regulation standard for consent (GDPR Article 7). The ACCC and OAIC should consult with experts and test consumer comprehension to check the effectiveness of the consent process. This should be a pre-condition to reform.

- CPRC supports **'Recommendation 4.2- modifications to privacy protections', 'Recommendation 4.5- customer control', 'Recommendation 5.6- persistent notification'** and **'Recommendation 5.11-transparency'** at the very least as a minimum level of consumer protection.

- CPRC supports the Government extending the Privacy Act to include small businesses as liable data holders.

- Whilst CPRC agrees with **'Recommendation 4.6 - single screen notification'**, it is critically important to test consumer comprehension from the introduction of this notification to ensure that they are providing genuine consent to what and how their data is collected and used. CPRC is also wary of broad legal statements of consent that may be unclear and could hide possible uses of data that could be detrimental to the consumer. Statements should be specific, meaningful and in Easy English. There should also be a means for further explanation if required by the customer. Furthermore, the required information for disclosure on single screen should have consideration of the materiality of harm to the consumer. Having consideration for materiality of harm may include prioritising the requirement of the disclosure of information based on potential harm or disadvantage that may be experienced by the consumer (such as consent to access by a third party to data over long periods of time, access to multiple parties or on-selling).

- CPRC supports **'Recommendation 6.4 - consumer education programme'**. We urge the Government to consult with organisations that work with vulnerable consumer groups to ensure that the information provided is appropriate for people who may have low literacy, for example Culturally and Linguistically Diverse (CALD) communities and Aboriginal and Torres Strait Islanders. Similarly, consideration should be given for consumers with limited digital literacy or access, as the majority of reforms will deliver benefits to those who are digitally enabled. Community organisations should also be engaged early during the design and implementation stage of this programme. This will help to ensure greater informed consumer participation.

## Data asymmetry—consumer trust and choice

### Consumer access to 'value-added data' in Open Banking

As highlighted in the Review report, the key principle of Open Banking is to improve competition as well as to reduce data asymmetry, to enable consumers to make better decisions that suit their circumstances. Value-added data is defined in the report as 'data that has been created by the data holder through the application of insight, analysis or transformation of a customer's transaction data to enhance its usability and value.' Recommendation 3.3 suggests that value-added customer data should not be included in Open Banking. The reason presented was that the value of this data has largely been generated by the actions of the data holder, and that they risk breaching intellectual property rights if this information is shared. However, this restricts the benefits to flow onto consumers by maintaining data asymmetry.

CPRC believes further consideration of what is considered 'value-added data' needs to be undertaken. For example, if a company has acquired additional data about that consumer from other organisations – is this also considered value-added data? Consumers should presumably have a right to the information and data that a company holds that may influence the products or services that they are offered, or as the case may be excluded from. The very wide practice of

data sharing is currently occurring across multiple platforms, sectors and this is not always transparent to customers as to which companies hold what data relating to their preferences, payment profile, interests or behaviour.

Simply giving customers access to their personal and transaction data through Open Banking is alone, not adequate to reduce data asymmetry. Depending on how it is defined, value-added customer data can give companies more information than the consumer to influence consumer outcomes because it can determine if customers are targeted or excluded from offers for products or services, impacting consumer choice. Withholding this information from consumers for their own use effectively means that data asymmetry will continue to exist. Consumers similarly have no way of knowing or rectifying this data upon which decisions have been made about who they might be. CPRC's quantitative research suggest that 92% of Australians want companies to be open about how they use data to assess their eligibility. A customer-focussed approach would be to give consumers the right to know how companies have classified them in order to adjust their own behaviour for better outcomes or challenge incorrect classifications, ultimately having more control about the options available to them and level the playing field. However, consumers should not be obliged by competitors to transfer this information. Confidentiality rules should also apply to these data which are considered 'non-personal' under the Privacy Act. Transparency on how companies use the data to make decisions about the customers can facilitate trust, and make the market more fair and equitable.

Furthermore, without improving informed and unbundled consent among consumers more generally, significant data asymmetry would still exist because companies are often able to transfer, collect and combine data about their customers from third parties or customer's social media without the direction or knowledge of the consumer, as these permissions are bundled in their Privacy Policies or Terms and Conditions[4]. Our qualitative research shows that customers find it reasonable to directly provide some level of information to companies with their expressed and informed consent for products such as loans or insurance, however they do not agree with companies collecting information about them from third parties without their knowledge. Our quantitative research has shown that 87% of Australians find it unacceptable for companies to collect data about them *without their knowledge* to assess their eligibility or exclude them from a loan or insurance. Current practices that do this can negatively impact the trust and relationship the companies have with their customers.

**Inclusion of 'aggregated data' in Open Banking**

The Review report also recommends against including aggregated data in the scope of Open Banking. CPRC suggests further consideration of 'Recommendation 3.5- aggregated data' because providing *averaged de-identified* data would be useful for competitors to gather information without having to generate this by collecting detailed identifiable information from individual consumers. The current proposed model of Open Banking suggests that competitors must rely on individual consumers to provide detailed and identifiable information in order to compete and innovate. If aggregated data was provided, it is possible that companies may only feel the need to request individual level data where the individual would like tailored services.

---

[4] Kemp, K. Big Data, Financial Inclusion and Privacy for the Poor. (Accessed 16th March 2018). Available at https://www.dvara.com/blog/2017/08/22/big-data-financial-inclusion-and-privacy-for-the-poor/

However, aggregate data does not come without risks. For example, recent de-identified location data from Strava recently revealed sensitive information about U.S. military bases and could be used to re-identify individuals[5]. If aggregate data was to be made available, there should be a formalised process where the Data Standards Body or other suitable body are able to review possible negative implications of the data for consumers and manage the release of aggregated data based on proposed uses.

CPRC supports 'Recommendation 3.11-no charge for customer data transfers'. Any charge for customer data transfer can pose as a barrier for Open Banking participation.

**Response to key recommendations**

- CPRC recommends that greater consideration on **'Recommendation 3.3.-value-added data'.** Consumers should have the right to know how companies have classified them in order to either adjust their own behaviour for better outcomes or challenge incorrect classifications, ultimately having more control about the options available to them and level the playing field. Withholding this information effectively means that data asymmetry will continue to exist and grow, with the benefits flowing disproportionally to providers. However, CPRC acknowledges the value generated by companies through the development of insights and analysis from consumer data, thus we recommend that consumers should not be obliged by competitors to transfer this information. Confidentiality rules should also apply to these data which are considered 'non-personal' under the Privacy Act.

- CPRC suggests further consideration on **'Recommendation 3.5- aggregated data'** because providing *averaged de-identified* data would be useful for competitors to gather information without having to generate this by collecting more sensitive detailed identifiable information from individual consumers. However, if aggregate data was to be made available, there should be a formalised process where the Data Standards Body or other suitable body are able to review and manage the release of aggregated data based on proposed uses. There have been multiple examples of where assumed ***de-identified*** data has been able to be ***re-identified.*** Ensuring regulators have adequate discovery powers and technical knowledge to assess this will be crucial.

- CPRC supports **'Recommendation 3.11-no charge for customer data transfers'.** Any charge for customer data transfer can pose as a barrier for Open Banking participation.

[5] Bogle, A. Strava has published details about secret military bases, and an Australian was the first to know. Updated 20th Jan 2018 (Accessed 16th March 2018). Available at http://www.abc.net.au/news/science/2018-01-29/strava-heat-map-shows-military-bases-and-supply-routes/9369490

Consumer Policy Research Centre

## Consumer protections against unfair use of data

The Consumer Data Right regulatory model needs to provide consumers with adequate protections against irresponsible management and unfair use of their data.

Whilst the review suggested that accreditation based on 'use cases' may limit future innovation (under Recommendation 2.7- Accreditation section). CPRC recommends that 'use cases' for accreditation should be reviewed at a high level to ensure they meet ethical principles. This will help to ensure that data holders and data recipients are accountable to protect consumers from harm. Setting accreditation requirements based on data ethics will facilitate consumer trust otherwise consumers may quickly retract the use of the data if they felt their data was being misused. CPRC's quantitative research indicated that 82% of Australians find it unacceptable for companies to collect information about their payment behaviour to assess their eligibility or exclude them from essential products and services such as electricity, gas or telecommunications. Sixty-seven percent of Australians indicated that Government should develop protections to ensure consumers are not unfairly excluded from essential products or services based on their data and/or profile.

'Recommendation 2.10 customer complaints and remedies' is an important recommendation to adopt to provide consumers a means for redress. However, this alone is inadequate in protecting consumers because it is a reactive approach and relies on the consumer to have transparent knowledge of the issue (which can be unobtainable if hidden in algorithms), sufficient resources, literacy skills and power to effectively seek redress. This further supports the need to include a preventative approach to include rules outlining conditions for obtaining consent and accredit companies based on uses that align with ethical principles to minimise harm. Algorithm assessments as a component of accreditation should be considered to ensure that companies do not breach anti-discrimination, consumer protection, competition, and privacy laws. These laws can only be effective if there are means to check compliance and address problems. Companies should be accountable for the algorithms they implement that would unfairly exclude consumers or unfairly limit consumer choices. This should apply to both data holders and data recipients under Open Banking and the broader Consumer Data Right. Legal experts, data ethicists and consumer groups should be involved in consultations for developing rules on consent conditions and principles of ethical uses to protect consumers from unfair uses of data.

**Protecting vulnerable and disadvantaged consumers**

CPRC recommends further consideration of the impacts of Open Banking on vulnerable and disadvantaged consumers including:

- *Women experiencing domestic violence*- 'Recommendation 4.7-joint accounts' requires authorization of data transfer and notification of data requests by each joint account holder. Whilst this would enable greater transparency for the account holders, alternative approaches or exemptions should be considered for women experiencing domestic violence as this could pose a risk to their safety. Government should consult with key experts in the field of domestic violence to develop guidelines for best practice approaches.

- *Consumers without online banking accounts*- CPRC supports 'Recommendation 5.9- access without online banking' to ensure that those who do not use online banking are not excluded from the benefits of Open Banking, as they still contribute to data through their banking activities. However, those who are unable to access online banking may also face other barriers such as low literacy, digital literacy and financial literacy (e.g. the elderly and CALD communities). Consumer representatives supporting these groups should be involved in the consultations for reviewing rules around consent conditions and accreditation criteria to ensure that these consumers are not exploited.
- *Minors under 18 years of age*- Do those under 18 have full control of their data or will they require parental authorisation? There should be additional considerations on consent for this group. We can look to GDPR Article 8 for some guidance[6].

**Response to key recommendations**

- As a minimum for accreditation, CPRC recommends that 'use cases' for accreditation should be reviewed at a high level to ensure that companies meet ethical principles. Legal experts, data ethicists and consumer groups should be consulted on the development of the principles of ethical uses of data to protect consumers from unfair uses of data.

- CPRC recommends further consideration of the impacts of Open Banking on vulnerable and disadvantaged consumers including women experiencing domestic violence, minors under 18 years of age, consumers who do not use online banking (e.g. those with low digital literacy such as the elderly and CALD communities), to ensure they are adequately protected from data misuse and exploitation.

## Interoperability and consistent approach across sectors

CPRC commends the report for considering interoperability to other sectors. We support Treasury in leading this process to ensure consistency across sectors, as flagged, energy and telecommunications sectors are likely to be the next iteration that the Consumer Data Right will apply.

Issues currently most pertinent in the energy sector is the ability (or lack thereof) of consumers to adequately compare energy plans and switch providers. Data portability to enable more accurate comparison and facilitate switching is essential to improve consumer outcomes. Key data to enable a consumer to compare products and services in the energy sector includes: current retail tariff information, consumption data and National Metering Identifier (NMI). Together, these three pieces of data enable comparison of current plan with potential plan.

---

[6]General Data Protection Regulation. Conditions applicable to child's consent in relation to information society services. Available at https://gdpr-info.eu/art-8-gdpr/

Consumer Policy Research Centre

CPRC strongly supports a consistent approach to the establishment of a Consumer Data Right across the three sectors, with the full consultation and consideration of data standards, adequate protections and consent requirements. At the very least, existing consultations processes in the Australian and Victorian Government in relation to energy data hubs should not result in the locking in of a technology or platform solution ahead of adequate consultation by Treasury and the ACCC on the rules and appropriate data standards on the Consumer Data Right.

CPRC supports 'Recommendation 2.5- The standards' to include transfer standards (for uniform transfer mechanisms), data standards (for integrity, accuracy and consistency), and security standards (for cyber protection). Given that different sectors such as energy and telecommunications may have different needs and challenges for transferring their datasets, it would be worth expanding working groups to include representatives from these sectors when developing the standards to ensure interoperability.

Lastly, CPRC has embarked on an extensive research program in relation to consumer data in 2018. This includes: undertaking market research; funding a $100,000 interdisciplinary research grant exploring the impact of data amalgamation, consumer profiling and the associated benefits and risks; and a forthcoming report reviewing international research and reforms in relation to big data and the impact on consumer markets. We would welcome discussions with policymakers and regulators as the Consumer Data Reforms evolve throughout the coming year.

If you have any queries about this submission, please don't hesitate to contact Phuong Nguyen on 03 9639 7600 or phuong.nguyen@cprc.org.au.

Yours sincerely,

Lauren Solomon

Chief Executive Officer

**Consumer Policy Research Centre**

## About Consumer Policy Research Centre

CPRC is Australia's first consumer-focussed policy think tank, established by the Victorian Government in December 2016. Our vision is to deliver a fair outcome for all consumers. We believe that consumer confidence when engaging with businesses and markets is central to the long-term sustainability of those markets. We work with business, the community sector and policy markets to develop, translate and promote evidence-based research to inform practice and policy changes.

Roy Morgan Research

# Consumer Knowledge and Understanding of Consent to Data Collection, Usage and Sharing Research 2018

March 10, 2018

*- Prepared for -*

**Consumer Policy Research Centre**
Level 14, 10-16 Queen Street
Melbourne, 3000

*- Prepared by -*

**Roy Morgan Research**
386, Flinders Lane
Melbourne, 3000

*Discover your edge*

## Contents

# 1. INTRODUCTION

## 1.1 Research Background

The Consumer Policy Research Centre (CPRC) is a not-for-profit, independent research centre focusing on areas of consumer policy in increasing transparency around consumer outcomes and experiences, and supporting improvements in market practices. Overall, their focus is on improving information and education in consumer decision making. The role of the Consumer Policy Research Centre (CPRC) is to:

- identify and monitor pertinent consumer issues;
- research key consumer protection issues and outcomes;
- translate research into policy and practice for the public benefit; and
- collaborate with others to amplify all of their work.

In February and March 2018, the Consumer Policy Research Centre (CPRC) commissioned Roy Morgan Research to conduct research to measure consumer knowledge and gain an understanding of consent to data collection, usage and sharing

The initial research design involved a combination of qualitative and quantitative techniques, beginning with two focus groups conducted to briefly understand consumer knowledge and consent for data collection, use and sharing. The purpose of the focus groups was to provide a brief understanding of the specific topic and help design the questionnaire for the online survey. The second phase of the research involved an online survey of 1000 Australians consumers aged 18 or over, undertaken to further understand consumer knowledge and consent for data collection, use and sharing.

This report covers findings from the quantitative phase of the research.

# 2. RESEARCH OBJECTIVES

The objectives of the online study were to determine the extent to which Australians:

- read and accept Terms and Conditions and Privacy Policy documents;
- understand data collection, use and storage processes;
- accept processes around using data for marketing and personalized processes; and
- believe Government should play a role in protecting their data.

# 3. METHODOLOGY

## 3.1 Questionnaire Design and Execution

The questionnaire was designed collaboratively by CPRC and Roy Morgan Research, based on insights identified through the qualitative focus groups conducted in the first phase of the research.

The online survey was conducted from 27 February to 6 March 2018 with Australians aged 18 years or more.

The average questionnaire length was 9 minutes.

A copy of the questionnaire is appended to the end of this report.

## 3.2 Sample

Sample for the survey was sourced through Roy Morgan Research's online consumer panel.

Quotas were set, and weighting applied where appropriate, to ensure a representative sample of Australians by age, gender and region.

# 4. THIS REPORT

This report outlines findings from the online quantitative survey. Results from the qualitative research have been delivered in a separate report.

## 4.1 Breakdown of Sample

As shown below, the data represented a broad range of respondents from a range of different ages, locations, educational qualifications and income brackets. All respondents indicated that they spoke English either well or very well.

- Gender
    - 49% Male
    - 51% female
- Age
    - 12% aged 18-24 year
    - 19% aged 25-34 years
    - 26% aged 35-49 years
    - 23% aged 50-64 years
    - 20% aged 65 years or more
- Location
    - 66% metro areas
    - 34% regional or rural areas

- Education
    - 19% secondary or lower
    - 30% TAFE
    - 33% undergraduate degree
    - 18% postgraduate degree
- Income
    - 45% earned under $50,000 p/a
    - 51% earned $50,00 or more p/a
- Language:
    - 15% speak a language other than English at home
    - 85% only speak English
    - 6% speak English well
    - 94% speak English very well

# 5. MAIN FINDINGS

## 5.1 Product and Service Usage

In the past 12 months, only one respondent indicated that they had not used any of the products or services lists. Almost all Australians (99%) had used Google products and services at least once in the past 12 months.

Over three-quarters of Australians indicated that they had most other products and services listed in the past 12 months—the only exception being Tap and Pay, where less than one in three Australians has used this feature in the past 12 months.

- Online shopping websites (89%);
- Apps on mobile phones or tablets (89%);
- Facebook (81%);
- Flybuys or Everyday Rewards supermarket loyalty cards (78%); and
- Tap and Pay with their mobile phone (28%).

## 5.2 Terms and Conditions/Privacy Policy Acceptance

In the past 12 months 67% of respondents indicated having read a Privacy Policy or Terms and Conditions at least once when signing up for a product or service, with the majority (35%) having only read them for a few products/services they signed up for. In contrast, one-third (33%) indicated that they never read Privacy Policies or Terms and Conditions.

Of those who read a Privacy Policy or Terms and Conditions document, one-third (33%) indicated that they did not accept the terms if they felt uncomfortable with them. In contrast, two-thirds (67%) indicated that they still signed up for one or more of the products/ services, with 15% indicating that they agreed to the T&Cs or Privacy Policies

for all products and services they signed up for, even if they did not feel comfortable with the policies.

When asked why they still accepted the Privacy Policies or Terms and Conditions, the most common response was that it was the only way to access the product or service (indicated by 73% of Australians). Less than one in four indicated other reasons:

- I trust the company would not misuse my data (23%);
- I believe that the law would prevent the company from misusing my data (20%); and
- Nothing bad has happened to me in the past (18%).

### 5.3 Knowledge of Data Collection, Use and Storage

Almost all respondents understand that companies can follow their activities across the internet (90%) and exchange information about them with third parties for purposes other than delivering the particular product or service (88%). Almost three-quarters (73%) were also aware that in store shopping loyalty card providers have the ability to collect and combine information about them from third parties.

Around half of Australians did not believe that when a company has a privacy policy, it means they will not share information with other websites or companies (59%), or that all mobile/tablet apps only ask for permission to access things on their device that are required for the app to work (47%).

At least two-thirds of Australians indicated that they were uncomfortable with most types of information being shared with third parties (as shown below). The exception being their name, where only 61% of Australians indicated that they were uncomfortable with their name being shared.

- Phone contacts (87%);
- Messages (86%);
- The unique ID number on their mobile or other device (84%);
- Phone number (80%);
- Date of birth (73%);
- Browsing history (72%);
- Who they are friends with on social networking sites (71%);
- Location data (71%);
- Purchase/transaction history (69%);
- Email address (67%);
- Name (61%);
- Other information raised included their home address, medical information, financial information, passwords and photos.

The above suggests that Australians are most uncomfortable sharing information about others (i.e. the phone contacts and messages), or information directly related to their personal device (i.e. phone numbers and unique IDs).

In order to protect their data, most Australians indicated that they at least sometimes use products or services provided by major companies they trust (92%) or select 'opt out' options where available (89%), suggesting that they prefer to stick to companies they know and trust, or those that are open and transparent about their desire to share data.

At least half of Australians also indicated that they:

- Deny apps permissions to access information after installing them (79%);
- Choose not to use the product or service collecting their data/information (76%);
- Adjust privacy settings on social networking websites (69%);
- Clear your browsing history (69%);
- Delete cookies on internet browsers (66%);
- Check mobile/tablet app 'permissions' before downloading (65%);
- Adjust ad settings on online accounts to reduce targeted ads (57%);
- Read Privacy Policies and Terms and Conditions documents (56%); and

Less than half of Australians (40%) use incognito browsers. In contrast, 24% indicated that they never do this as a means of protecting their data.

### 5.4 Attitudes about Using Data for Marketing and Personalised Pricing

At least eight in ten Australians found the following uses of their data to be somewhat or very unacceptable:

- Charging people different prices for the same product in the same hour, based on their past purchasing, online browsing history or payment behaviour (88%);
- Collecting data about them without their knowledge to assess their eligibility or exclude them from a loan or insurance (87%);
- Collecting data about their payment behaviour to assess their eligibility or exclude them from an essential product or service (82%); and

However, only around one in two (52%) felt that monitoring online behaviour to show relevant advertisements and offers was very or somewhat unacceptable. In contrast, 27% found this to be very or somewhat acceptable. This suggests that Australians are most concerned about fairness, and do not want their data to be used in any fashion that could be construed as unfair to either themselves or others.

With respect to how companies use their data, Australians were most likely to agree that companies should be open, honest and transparent, and:

- Give them options to opt out of certain types of information they can collect, use and/or share (95%);

- Be open about how they use data to assess my eligibility (92%); and
- Only collect information currently needed for providing their product or service (91%).

Correspondingly, very few agreed that:

- It is enough for companies to notify them about how they collect, use and share data in Privacy Policies or Terms and Conditions (37% agreed, and 44% disagreed); and
- If they trust a company, they don't mind if it buys information about them from database companies without asking them (only 9% agreed, and 77% disagreed with this statement).

### 5.5 Government's Role

Finally, with respect to the role of Government, most Australians felt that the Government should take some active role in helping to protect their data with:

- 73% indicating that Government should ensure companies give consumers options to opt out of what data they provide, how it can be used and if it can be shared; and
- 67% indicated that Government should develop protections to ensure consumes are not unfairly excluded from essential products or services based on their data and/or profile.

Less than one in ten believed that Government's should do nothing, agreeing that:

- It is the individual's responsibility to check how companies are using their data (10%); or that
- It is the company's right to determine how they use the data (3%).

# 6. APPENDIX A: QUESTIONNAIRE

## SCREENING AND QUOTA BUILDING

**PLEASE IMPUTE GENDER FROM SAMPLE INTO <DUMGEN>**

[Single]

<DUMGEN>

1. Male
2. Female

[Ask all] [Single]

Q1. AGE

What is your age?

1. 17 years or under
2. 18-24 years
3. 25-34 years
4. 35-49 years
5. 50-64 years
6. 65 years or older
99. Prefer not to answer

**IF SDAGE = 1 OR 99 TERMINATE**

[Single]

Q2. What is your postcode?

_____

**IF INVALID POSTCODE, END SURVEY**

**RECODE RESPONSE FROM Q2 INTO DUMVARIABLE <DUMSTATE>**

[Single]

<DUMSTATE>

1. Australian Capital Territory
2. Sydney
3. NSW excluding Sydney
4. Melbourne
5. Victoria excluding Melbourne
6. Brisbane
7. Queensland excluding Brisbane
8. Adelaide
9. South Australia excluding Adelaide
10. Northern Territory
11. Hobart
12. Tasmania excluding Hobart
13. Perth
14. Western Australia excluding Perth

**IF RESPONDENT DOES NOT QUALIFY BEYOND SCREENING, SKIP TO SCREENOUT MESSAGE**
**IF RESPONDENT FALLS INTO A FULL QUOTA, SKIP TO QUOTA FULL MESSAGE**
**IF RESPONDENT QUALIFIES, CONTINUE**

## CONSUMER CHARACTERISTICS

[Ask all] [Single]

Q3. What is the highest level of education you have completed?

1. Primary school or lower
2. Secondary school
3. Technical or further education (e.g. Trade, certificate, diploma)
4. Undergraduate university degree (e.g. Bachelor degree, Honours)
5. Post graduate university degree (e.g. Master degree, PhD)
97. Other, please specify _____

[Ask all] [Single]

Q4. Approximately how much income do you usually receive in a year (includes wages and government payments)

1. Less than $6000
2. $6,000 - $9,999
3. $10,000 - $14,999
4. $15,000 - $19,999
5. $20,000 - $24,999
6. $25,000 - $29,999
7. $30,000 - $34,999
8. $35,000 - $39,999
9. $40,000 - $44,999
10. $45,000 - $49,999
11. $50,000 - $59,999
12. $60,000 - $69,999
13. $70,000 - $79,999
14. $80,000 - $89,999
15. $90,000 - $99,999
16. $100,000 - $109,999
17. $110,000 - $119,999
18. $120,000 - $129,999
19. $130,000 Or More
98. Can’t Say
99. Prefer not to answer

**IF Q4=98 OR 99, ASK SDINRR**

[Ask if Q4 = 1-19] [Single]

SDINRR. STANDARD DEMOGRAPHIC QUESTION
Could you please tell me whether your income would be over $50,000 or under $50,000 per annum?

1. Under $50,000
2. $50,000 Or More
98. Can't Say
99. Prefer not to answer

[Ask all] [Single]

Q5. Do you, yourself, speak a language other than English at home?

1. Yes
2. No

[Ask all] [Single]

Q6. How well do you speak English?

1. Not at all
2. Not well
3. Well
4. Very well

[Ask all] [Single response per statement] [Grid]

Q7. In the past 12 months, how often did you use…?

| | NEVER | LESS OFTEN THAN ONCE A MONTH | AT LEAST ONCE A MONTH | AT LEAST ONCE A WEEK | DAILY |
|---|---|---|---|---|---|
| a. Facebook | | | | | |
| b. Google products and services (including Google search engine, gmail, Google maps, etc.) | | | | | |
| c. Flybuys or Everyday Rewards supermarket loyalty card | | | | | |
| d. Online shopping websites | | | | | |
| e. Apps on a mobile phone or tablet | | | | | |
| d. Tap and Pay with your phone | | | | | |

## INTERACTION WITH PRIVACY POLICIES AND TERMS AND CONDITIONS

[Ask all] [Single]

Q8. In the past 12 months, how often did you read a Privacy Policy or Terms & Conditions when signing up for a product or service?

1. Never
2. For only a few products/services I signed up for
3. For some products/services I signed up for
4. For most products/services I signed up for
5. For all products/services I signed up for

**IF Q8=1, SKIP TO Q11**

[Ask if Q8 = 2-5] [Single]

Q9. In the past 12 months, how often did you 'accept' a company's Privacy Policy or Terms and Conditions to use a product or service, even though you did not feel comfortable with the policies?

1. Never
2. For only a few products/services I signed up for
3. For some products/services I signed up for
4. For most products/services I signed up for
5. For all products/services I signed up for

**IF Q9=1, SKIP TO Q11**

[Ask if Q9 = 2-5] [Multiple] [Randomise statements 1-4]

Q10. Why did you 'accept' the Privacy Policy or Terms and Conditions even though you did not feel comfortable with the policies? (Select all that apply)

1. It was the only way to access the product or service
2. I trust that the company would not misuse my data
3. Nothing bad has happened to me in the past
4. I believe that the law would prevent the company from misusing my data

97. Other, please specify _____

## KNOWLEDGE OF DATA COLLECTION, USE AND SHARING

[Ask all] [Single response per statement] [Grid] [Randomise statements]

Q11. Choose True, False or Don't Know for the following statements as best reflects your opinion.

| | TRUE | FALSE | DON"T KNOW |
|---|---|---|---|
| a. Companies today have the ability to follow my activities across many sites on the web. | | | |
| b. When a company has a privacy policy, it means the site will not share my information with other websites or companies. | | | |

| | TRUE | FALSE | DON"T KNOW |
|---|---|---|---|
| c. In store shopping loyalty card providers like Flybuys and Everyday Rewards have the ability to collect and combine information about me from third parties. | | | |
| d. Some companies exchange information about their customers with third parties for purposes other than delivering the product or service the customer signed up for. | | | |
| e. All mobile/tablet apps only ask for permission to access things on my device that are required for the app to work. | | | |

[Ask all] [Multiple] [Randomise statements 1-11]

Q12. What data/information would you be uncomfortable with companies sharing with third parties for purposes other than delivering the product or service? (Select all that apply)

1. Name
2. Phone number
3. Email address
4. Date of birth
5. Your messages
6. Browsing history
7. Purchase/transaction history
8. Phone contacts
9. Who you are friends with on social networking sites
10. The unique ID number on your mobile phone or other device
11. Location data

97. Other, please specify _____

[Ask all] [Single response per statement] [Grid] [Randomise statements a-k]

Q13. In order to protect your data/information, how often do you…

| | ALWAYS | OFTEN | SOMETIMES | RARELY | NEVER | I DON'T KNOW HOW |
|---|---|---|---|---|---|---|
| a. Use products or services provided by major companies you trust | | | | | | |
| b. Use incognito browsers | | | | | | |
| c. Read Privacy Policies and Terms & Conditions documents | | | | | | |
| d. Choose not to use the product or service collecting your data/information | | | | | | |
| e. Adjust privacy setting on social networking websites | | | | | | |
| f. Adjust ad settings on your online accounts (e.g. Google or Facebook) to reduce ads targeted to you | | | | | | |
| g. Check mobile/table app 'permissions' before downloading the app to see what you are giving it access to on your device | | | | | | |

| | ALWAYS | OFTEN | SOMETIMES | RARELY | NEVER | I DON'T KNOW HOW |
|---|---|---|---|---|---|---|
| h. Deny apps permission to access information from your mobile after installing and opening the app | | | | | | |
| i. Delete cookies on internet browsers | | | | | | |
| j. Clear your browsing history | | | | | | |
| k. Select 'opt out' options where available, denying companies permission to share your data with third parties | | | | | | |
| l. Other, please specify _____ | | | | | | |

## ATTITUDES ABOUT USE OF DATA FOR MARKETING AND PERSONLISED PRICING

[Ask all] [Single response per statement] [Grid]

Q14. How acceptable or unacceptable do you find it for companies to use your data in the following ways?

| | VERY ACCEPTABLE | SOMEWHAT ACCEPTABLE | NEUTRAL | SOMEWHAT UNACCEPTABLE | VERY UNACCEPTABLE | UNSURE |
|---|---|---|---|---|---|---|
| a. Monitoring your online behaviour to show you relevant advertisements and offers | | | | | | |
| b. Charging people different prices for the same product in the same hour, based on their past purchasing, online browsing history, or payment behaviour | | | | | | |
| c. Collecting data about you without your knowledge to assess your eligibility or exclude you from a loan or insurance | | | | | | |
| d. Collecting data about your payment behaviour to assess your eligibility or exclude you from essential products and services (e.g. electricity, gas, telecommunications) | | | | | | |

[Ask all] [Single response per statement] [Grid]

Q15. How strongly do you agree or disagree with the following regarding how companies should handle your data?

| | STRONGLY AGREE | AGREE | NEITHER | DISAGREE | STRONGLY DISAGREE | UNSURE |
|---|---|---|---|---|---|---|
| a. It is enough for companies to notify me about how they collect, use and share my data in their Privacy Policy and Terms and Conditions | | | | | | |

| | STRONGLY AGREE | AGREE | NEITHER | DISAGREE | STRONGLY DISAGREE | UNSURE |
|---|---|---|---|---|---|---|
| b. Companies should give me options to opt out of certain types of information they can collect about me, how it can be used, and/or what can be shared with others | | | | | | |
| c. Companies should only collect information currently needed for providing their product or service | | | | | | |
| d. If I trust a company, I don't mind if it buys information about me from database companies without asking me | | | | | | |
| e. Companies should be open about how they use data about me to assess my eligibility or exclude me from products or services | | | | | | |

[Ask all] [Multiple]

Q16. What role do you think government has in regulating how companies use your data? (Select all that apply)

1. Nothing, it is the individuals' responsibility to check how companies are using their data
2. Nothing, it is the company's right to determine how they use the data
3. The Government should ensure companies give consumers options to opt out of what data they provide, how it can be used, and if it can be shared with others.
4. The Government should develop protections to ensure consumers are not unfairly excluded from essential products or services (e.g. electricity, gas, telecommunications) based on their data and/or profile

97. Other, please specify _____