

Submission to ACCC Digital Platforms Inquiry - Issues Paper

5th April 2018

By email: platforminquiry@accc.gov.au

Dear Secretariat,

Re: Digital Platforms Inquiry: Issues Paper

Submission and attachments to remain in confidence until 14th May 2018

The Consumer Policy Research Centre (CPRC) would like to thank you for the opportunity to respond to the Digital Platforms Inquiry Issues Paper.

CPRC is an independent, not-for-profit consumer research organisation. CPRC undertakes interdisciplinary and cross-sectoral research to inform policy reform and practice change. Consumer data is a central research priority for the organisation due to the rapidly growing online marketplace, early adoption of digital technology by Australians, and the emerging benefits and risks to consumers of 'big data' amalgamation.

In this submission CPRC has drawn on internal research, as well as recently commissioned market research completed by Roy Morgan Research into *Consumer Knowledge and Understanding of Consent to Data Collection, Usage and Sharing in Australia*. We attach a copy of the quantitative market research to this submission (Attachment 1).

CPRC notes that this Inquiry and cited data practices are not occurring in isolation. One of the most significant challenges of data amalgamation and the impact on competition is that the collection, sharing and use of data is not happening within any one sector, but multiple at the same time. It is therefore important to consider not only the issues associated with genuine consent and control of over *collection* of data but also the *sharing* and *use* – by who and for what purpose.

While this Inquiry focusses on data collected by digital platforms, largely transacted for advertisement – the extent to which data is being shared between digital platforms and other commercial entities to which consumers may have unwittingly given consent remains unclear, and obfuscated by vague and lengthy privacy policies which consumers have little awareness of or control over.

We therefore encourage the Commission to consider the amalgamation of consumer data by digital platforms to include data amalgamated by the digital platform which may have been

generated by separate commercial entities in completely different sectors such as retail stores, technology providers or service providers.

We have raised similar concerns in relation to the need to view these matters holistically in relation to the Review into Open Banking and establishment of a Consumer Data Right in Australia. While the establishment of the Consumer Data Right is a useful first step to enable more accurate comparisons of products and services for consumers, we believe there to be significant benefit in ensuring that complementary protections are rolled out in parallel. In particular, ensuring consumers are empowered with more transparency and control over how their data is collected and used, along with a greater focus by regulators on the potential for discrimination and exclusionary practices.

CPRC supports effective competition in the online marketplace where:

- consumers are able to make genuinely informed choices about purchase decisions;
- consumers have genuine control and transparency over what data is collected, how it is used, shared and transacted;
- information (or data) asymmetry between buyers and sellers is minimised;
- adequate protections exist, especially for vulnerable or disadvantaged consumers.

Ensuring these settings are in place as the online marketplace evolves in Australia will be central to consumer confidence, fairness and good consumer outcomes.

Implications for consumers

3.18. Describe the nature of the impacts (positive and negative) that digital platforms are having on consumers? What causes these impacts? Are these impacts temporary or ongoing?

Digital platforms such as social networking sites facilitate interactions between users by allowing them to share information, opinions, and interests¹. They are also being used by organisations to disseminate information and foster collaboration. This can have a positive impact for consumers as digital platforms can be a useful source for information attainment and for exchanging ideas. However, these platforms also bring new challenges relating to privacy, security, data management, accuracy and diversity of information^{2 3 4}.

¹ Khan, G.F., Swar, B., Lee, S.K. Social Medial Risks and Benefits: A Public Sector Perspective. Social Science Computer Review. 2014; 32(5): 606-627

² ibid

³ Allcott, H. and Gentzkow, M. Social media and fake news in the 2016 election. Journal of Economic Perspectives. 2017; 31(2):211-236

⁴ Bozdag, E. and Van Den Hoven, J. Breaking the filter bubble: democracy and design. Ethics Information Technology. 2015; 17(4): p249-265

There have been a number of complaints against Google and Facebook in the US and Europe between 2011 and 2016 relating to privacy and data protection concerns⁵. The issues raised for Google included collection, use or sharing of information without user knowledge or consent. This ranged from user search queries to Wi-Fi data, placing cookies on users' computers without users' consent and more. Some of these complaints have resulted in large fines and penalties. Facebook complaints have included inaccuracy of information provided to users, lack of user ability to restrict access to their data, broader collection of data and tracking (e.g. web browsing and when logged off Facebook), sharing of information to third parties, and conducting experiments without user knowledge—some of which are under investigation. The use of digital platforms can have negative lasting impacts for consumer privacy due to the lack of adequate protection and control consumers have over their information. There is a view that consumers are being valued less as clients and more as 'groups of data that can be understood, and possibly manipulated to increase advertising revenues'⁶. CPRC strongly supports Australia following the European Union's (EU) lead by looking at privacy from a human rights perspective and providing tighter regulation on privacy—the EU's Charter of Fundamental Rights protects privacy and data protection as fundamental rights and the General Data Protection Regulation (GDPR), in force from 25 May 2018, will subject any company who is collecting information from data subjects in the EU to re-collect consent under new strengthened conditions⁷.

3.19. What are the advantages and disadvantages of using digital platforms for consumers?

In relation to news and journalistic content, an advantage of digital platforms is that they can facilitate consumer engagement in news and social issues—digital platforms allow users to consume, share, comment and react to information. Personalised display of information also means that consumers get access to items that are relevant or are of interest to them⁸.

One of the disadvantages of using digital platforms is the 'filter bubble' effect where algorithms filter and prioritise the content displayed so that it reflects the users' view, based on their prior interactions with the system and other factors, and consequently hides content with opposing viewpoints without the users' consent. By controlling the information accessible to consumers, it has been claimed that digital platforms are eroding the consumer's autonomy to be a judge of their own interest⁹. Bozdag and Van Den Hoven (2015) argue that 'filter bubbles can be seen as a form of market failure that diminishes user control and hence autonomy, hide available options and coerce people in such a way that they cannot get what they want. Users will not get the search results they were looking for, or do not receive the updates from friends they want to in a

⁵ Jorgensen RF. and Desai T. Right to Privacy meets online platforms: exploring privacy complaints against Facebook and Google. *Nordic Journal of Human Rights*. 2017; 35(2): 106-126

⁶ *ibid*

⁷ *ibid*

⁸ Bozdag, E. and Van Den Hoven, J. Breaking the filter bubble: democracy and design.(p3)

⁹ *ibid*

social networking platform.' For consumers who value diversity in content and product offerings, there is often little other option available to avoid heavily personalised and curated content.

Additionally, how this curation impacts display results both of information and certain products and services is unclear. The quality and source of data that is used by digital platforms to determine a 'consumer profile' remains obscure. Lack of transparency for consumers to understand how their profiles have been established and what they are based on leaves little options available for revision or dispute.

One proposed way of addressing this is designing tools to improve users' control over the filters: for example by increasing users' awareness of their own biases (e.g. [Balancer](#)), giving users exposure to diverse viewpoints (e.g. [ConsiderIt](#)), and informing users of the filters that are implemented online (e.g. [Bobble](#))¹⁰. However, this places a lot of effort on the individual to overcome algorithm bias.

3.20. What terms and conditions govern consumers' use of digital platforms? How do they differ from those which apply when consumers obtain news and journalistic content from other sources?

Consumers aren't subject to the same conditions when accessing news and journalistic content on digital platforms compared to other sources such as printed newspapers, radio or television. The difference with digital platforms is that they have the ability to collect a user's personal information and track their activities (and their social network's activities) to develop a detailed profile of who they are and their preferences.

Privacy Policies and Terms and Conditions allow companies to 'declare' and secure consent to practices around data collection, use, storage and sharing which are not necessarily identified by consumers in these lengthy documents.

CPRC recently commissioned a market research study conducted by Roy Morgan Research surveying a representative sample of 1004 Australians. The results show that 33% of Australians surveyed admit to not reading a Privacy Policy or Terms and Conditions at all when signing up for a product or service in the past 12 months. Only 6% have read their Privacy Policy and Terms and Conditions for all products they have signed up to in the past 12 months. Additionally, of the 67% who reported reading a Privacy Policy or Terms and Conditions at least once in the past 12 months, *two-thirds* 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%). These findings demonstrate that Australian consumers are currently lacking sufficient awareness and control over the type of data being collected and used. Consumers simply feel that they have

¹⁰ *ibid*

no choice but to accept the terms of service or otherwise face denial of access to the products or services.

3.21. Are consumers generally aware of these terms and conditions? Specifically, do Australian consumers understand the value of the data they provide, the extent to which platforms collect and use their personal data for commercial purposes, and how to assess the value or quality of the service they receive from the digital platforms?

Our research indicates that while Australians are aware of Privacy Policies and Term and Conditions, this does not necessarily translate to sufficient knowledge or control of how their information is being collected, used, stored or shared. 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.

A view expressed by consumers in CPRC's qualitative focus groups was that Terms and Conditions were written to satisfy legal requirements and do not really serve as a tool for effective communication with the customer.

"I actually read the Terms and Conditions. They're written to satisfy legal requirements, not to communicate with me, and can sometimes be hard to understand."

An Australian study by consumer advocacy group CHOICE, looked at the time it would take to read the Terms and Conditions of Amazon Kindle and found that it would take nine hours to read¹¹. This is consistent with other literature which suggests users do not read policy documents because the policy documents are too long, difficult to comprehend, difficult to find, or they perceive the cost to benefit ratio of reading to be too high^{12 13 14}. These findings highlight the importance of a significant focus by regulators on effective consent and privacy by design approaches to regulatory intervention, rather than ongoing reliance on consumers to wade through excessively lengthy policies with little ability to comprehend the information, let alone control over the outcome if they do not agree with what is being proposed.

¹¹ Hunt, E. (2017). Amazon Kindle's terms 'unreasonable' and would take nine hours to read, Choice says. The Guardian. Available at <https://www.theguardian.com/australia-news/2017/mar/15/amazon-kindles-terms-unreasonable-and-would-take-nine-hours-to-read-choice-says>. (Accessed on 18 Jan 2018)

¹² Solove, DJ. Introduction: Privacy self-management and the consent dilemma. Harvard Law Review. 2013, 126 (7): 1880-1903

¹³ Obar, JA., Oeldorf-Hirsch, A. The biggest lie on the internet: Ignoring the privacy policies and terms of services policies of social networking services (August 24, 2016). TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016. Retrieved from <https://ssrn.com/abstract=2757465>.

¹⁴ Marrtje, E. et al. (2016). Study on consumer's attitudes towards Terms and Conditions (T&Cs). European Commission. Retrieved from http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf

Focus groups also suggested that consumers are aware that their data has some monetary value.

"There's this other series of information which is inferred, largely through data mining processes, by which you could be profiled and your desires and expectations predicted with some degree of confidence, and that I think is the more scary part... that information is highly valuable."

"Big data is the most valuable thing in the world. They should pay us to collect it."

However, it is difficult for consumers to know the extent to which platforms collect, use, store and share their personal data for commercial purposes because the information is not transparent, and consumers do not have genuine control over their data.

"I confess, I sometimes wonder what I am agreeing to..."

"How can we achieve 'privacy' unless you cut yourself off from useful things?"

"I close my eyes and don't think about it"

Forty-four percent of consumers surveyed feel that it is not enough for companies simply to notify them about how they collect, use and share data in their Privacy Policies or Terms and Conditions alone.

Furthermore, our research 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. Furthermore, the majority of Australians (73%) expect that the Government should mandate companies to provide consumers options to opt out of certain uses and sharing of their data.

As an example of intervention in other jurisdictions, the EU takes an even more consumer-focused approach by ensuring that privacy is the default setting by design, meaning that consumers would have to opt in to sharing information rather than opt out and that there are conditions around consent to protect consumers^{15 16}. Consent can only be effective if users truly have real choice—e.g. if consent is given as a premise for using platforms and the boundaries to which data is collected, used, stored and shared is too broadly defined, then there is no real choice for consumers but to agree out of necessity or otherwise risk losing access to tools that

¹⁵ GDPR. Article 25 GDPR Data protection by design and by default. Available at <https://gdpr-info.eu/art-25-gdpr/>

¹⁶ GDPR. Article 7 GDPR Conditions for consent Available at <https://gdpr-info.eu/art-7-gdpr/>

have no alternatives¹⁷. Furthermore, the GDPR also provides consumers a 'right to erasure' or to be forgotten, which helps to address issues around unwanted data retention because data can still be stored without the users' knowledge even if they had 'deleted' the information¹⁸
¹⁹.

3.23. If you consider the collection of data part of the effective price paid by consumers for use of the digital platforms, to what extent are consumers aware of and provide informed consent for the collection and use of their data?

CPRC understands that consumers' access to some services for free is made possible through advertising revenue. However, advertising is becoming increasingly personalised and targeted to consumers through the use of their data. The level to which consumers are aware of and provide consent for the collection and use of their data is not extensive. Whilst 88% of consumers were aware that companies exchange information about them with third parties for purposes other than delivering the product or service, and 91% were aware that companies today have the ability to follow their activities across many sites on the web, more detailed discussion from recent focus groups suggest that consumers are concerned because they do not know exactly where their data goes and how it is used.

"Once you share your information, you cannot trace it."

It is evident that the ability to control, track and know what their data is being used for is important to consumers.

Australians value the privacy of their information. Majority of Australians do not want companies sharing their information for secondary purposes. At least two-thirds of Australians indicated they were uncomfortable with most types of information being shared with third parties:

- Phone contacts (87%)
- Their messages (86%)
- Their 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%)

¹⁷ Jorgensen RF. and Desai T. Right to Privacy meets online platforms: exploring privacy complaints against Facebook and Google. *Nordic Journal of Human Rights*. 2017; 35(2): 106-126

¹⁸ *ibid*

¹⁹ GDPR. Article 17 GDPR Right to erasure ('right to be forgotten'). Available at <https://gdpr-info.eu/art-17-gdpr/>

- Purchase/transaction history (69%)
- Email address (67%)
- Name (61%)

Another finding of our research suggests that consumers' openness to sharing information depends on which organisation is collecting the information (preference for reputable companies), the type of data being collected (consumers are more open to sharing data that does not identify them), and purpose for which the data will be used (they do not want the data to result in their detriment).

Consumers are also relying on companies they trust to protect their personal information – with trust and brand effectively being used as a proxy for privacy and good data practices. CPRC's quantitative study suggests that 96% of Australians have (at any time in the past) used products or services provided by major companies they trust as a strategy to protect their data or information. Our research indicates that consumers typically do not currently read Privacy Policies or Terms and Conditions if they are accessing products or services from an organisation they trust. Furthermore, consumers perception of trust is often guided by the size of the company or if they have heard of the company.

"I don't read them for some of the bigger kinds of companies..."

Consumers clearly have a desire to protect their information. Australians surveyed indicated that they have (at any time in the past) taken the following actions as means to protect their data:

- Denied apps permission to access information after installing them (86%)
- Chosen not to use the product or service collecting their data/information (90%)
- Adjusted privacy settings on social networking sties (82%)
- Cleared their browsing history (90%)
- Deleted cookies on internet browsers (85%)
- Checked their mobile/tablet app 'permissions' before downloading (80%)
- Adjusted ad settings on online accounts to reduce targeted ads (72%)
- Read Privacy Policies and Terms and Conditions documents (82%)
- Used incognito browsers in order to protect their information (55%).

3.25. How do consumers value digital platforms' access to their data? Do consumers see it as a cost or a benefit (e.g. it enables customisation of the content displayed)? How does the access to or control over user data impact the relationship between digital platforms and consumers?

The value consumers place on digital platforms' access to their data depends on the level of awareness and purpose for which the data is used.

A small proportion of consumers find the use of their data for customisation of content displayed to be of benefit. Twenty-seven percent of Australians believed it is acceptable for companies to monitor their online behaviour to show relevant advertising. However the majority, 52% of Australians surveyed found such use unacceptable.

Our qualitative research suggests that some consumers appreciate relevant advertising based on their interest. Furthermore, participants generally value the use of their data where it would benefit them or society as a whole. These situations generally included getting birthday discounts, receiving relevant recommendations or deals:

"If I get a discount on my birthday, that is good use. Anything that is of personal benefit to me."

"I don't mind it if things pop up about travel deals, just in case I'm interested."

"Product development, predict preferences (e.g. Spotify)... simplifying life."

However, many participants believe that the data provided to a company should not be shared. Participants also expressed a view that they should have greater ownership and control over their own data and how it is shared.

"It should be my data. I should have rights to it."

"...It's just they are all connected. So that's when I started to worry a bit coz the stuff that I search for is like moving companies."

"Anything identifiable, anything that can be traced back to you [should not be shared]."

"I'm not comfortable with them having any of my information, but if you want to be involved in whatever the site is about, you don't get options..."

Furthermore, use of information which can disadvantage certain consumers and reduce consumer choice is overwhelmingly rejected by the Australians surveyed as being a reasonable use of data. Generally, Australian consumers do not find it acceptable if their data is being used to:

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

In an evolving environment ensuring online markets retain consumer confidence and trust is crucial. Companies and policymakers that do not keep up with community expectations around appropriate collection, sharing and use of data will ultimately impact the long-term sustainability and growth and uptake of new technologies and digital platforms.

In line with public expectations, a greater focus on how consumer data and digital platforms can be used by organisations to unfairly price or exclude consumers from certain products and services (particularly where essential) requires additional resources for regulators for monitoring activities as these markets expand.

Lastly, better access to and control over user data by consumers can help to re-balance the growing information asymmetry and build better relationships between digital platforms and consumers²⁰.

If you have any questions or would like further information regarding this submission, please don't hesitate to contact Senior Research & Policy Officer, 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-focused 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.

²⁰ Jorgensen RF. and Desai T. Right to Privacy meets online platforms (p3)

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

Contents

1. INTRODUCTION	2
1.1 RESEARCH BACKGROUND	2
2. RESEARCH OBJECTIVES	2
3. METHODOLOGY	3
3.1 QUESTIONNAIRE DESIGN AND EXECUTION	3
3.2 SAMPLE	3
4. THIS REPORT	3
4.1 BREAKDOWN OF SAMPLE	3
5. MAIN FINDINGS	4
5.1 PRODUCT AND SERVICE USAGE	4
5.2 TERMS AND CONDITIONS/PRIVACY POLICY ACCEPTANCE	4
5.3 KNOWLEDGE OF DATA COLLECTION, USE AND STORAGE	5
5.4 ATTITUDES ABOUT USING DATA FOR MARKETING AND PERSONALISED PRICING	6
5.5 GOVERNMENT’S ROLE	7
6. Appendix A: Questionnaire	8

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 consumers 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 _____