Consumer Policy Research Centre

Consumer data and the digital economy

Emerging issues in data collection, use and sharing

Phuong Nguyen & Lauren Solomon

ABOUT CONSUMER POLICY RESEARCH CENTRE (CPRC)

An independent think-tank established by the Victorian Government in 2016, CPRC produces evidence-based research to inform government policy and business practice reform. We work collaboratively across the government, regulatory, business and community sectors. We also conduct, support and promote interdisciplinary consumer research. Our goal is to deliver a fair outcome for all consumers. To find out more, visit: cprc.org.au

Acknowledgements

We would like to acknowledge Roy Morgan Research who were commissioned to conduct a national survey and focus group study on behalf of CPRC.


MINIMUM
eftpos

Introduction

Australians are spending more of their lives online. 87% were active internet users in 2017[1], more than 17 million use social networking sites[2], and 84% of Australians are now buying products online[3].

With this growing digital life, large volumes of data about consumers are being collected at an unprecedented rate — in 2013 it was reported that approximately 90% of the world's data was collected in two years[4]. Collected information is now being amalgamated by sophisticated computing tools and techniques to generate what is called Big Data.

Big Data is defined as *"high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation"*[5, 6]. High-volume refers to large amounts of data; high-velocity refers to how quickly large amounts of data is accumulated, thereby requiring high processing capacity to manage and keep up-to-date; and high-variety refers to the mixing of heterogeneous data types in meaningful ways[7].

Marketing companies estimate the Big Data software market revenue to be worth $42b in 2018[8], with 79% of Big Data users suggesting that companies risk being at a competitive disadvantage if they do not utilise Big Data to inform their business practices[9].

Many benefits can arise from Big Data, including improved public health, stronger fraud detection, improved efficiencies and processes, relevant advertising, and access to more suitable products. However, emerging issues have also been identified, such as consumer profiling and business practices that place consumers at risk of discrimination and exclusion from accessing products and services.

This report discusses some of the known practices of data collection, sharing and amalgamation, the benefits and the potential detrimental impacts for consumers without complementary protections. It also explores opportunities to give consumers greater control over their personal information and ways to preserve their right to privacy.

In particular, we examine the benefits of improving conditions for obtaining genuine consent, implementing Privacy by Design, developing better tools for consumers to manage their data and privacy, including revising consumer protection and privacy legislation.

Research on Australians' knowledge and attitudes about how their data is collected, used and shared[3, 10-13] is limited. Consumer Policy Research Centre (CPRC) has built on existing evidence by commissioning Roy Morgan Research to survey a nationally representative sample of 1004 Australians and conducting two focus group studies.

Our research explored Australian consumers' understanding of consent to data collection, use and sharing when accessing products and services. Consumers were asked questions relating to their online behaviour, knowledge and attitudes regarding data collection practices, and their expectations around consumer protection and data control.

The findings were clear, with participants indicating that consumers:

- Did not fully understand specifically what types of information were being collected and shared about them;
- Experience barriers to reading Privacy Policies; and/or
- Lacked genuine consent over the terms upon which they provide their information.

The majority of those surveyed also indicated that they did not want companies to use their data in ways that could disadvantage them or other customers, and that they wanted more options over what data is collected and how it is used. Furthermore, participants wanted the government to have a role in improving consumer control over data as well as protecting them from data misuse.

This report draws on the results of this market research, provides an analysis of international and Australian consumer experiences, business practice and policy settings, and explores policy implications relating to consumer data collection, use and sharing. Policy recommendations are provided with a focus on reforms to facilitate trust so that both businesses and consumers are well-placed to reap the benefits of the digital economy.

What is consumer data?

In 2017, the Productivity Commission broadly defined consumer data as[14]: "*personal information (as defined in the Privacy Act 1988 [Cth]) that is in digital form; files posted online by the consumer; data created from consumers' online transactions, Internet-connected activity or digital devices; data purchased or obtained from a third party that is about the identified consumer; and other data associated with transactions or activity that is held in digital form and relevant to the transfer of data to a nominated third party*".

In Australia, the definition of consumer data is being determined through reforms to establish a Consumer Data Right[15].

The Consumer Data Right flowed from one of 41 recommendations in the Data Availability and Use, Productivity Commission Inquiry Report in March 2017[14] which sought to review the benefits and costs of increasing the availability, and improving the use of, public and private data by individuals and organisations.

The Consumer Data Right aims to provide consumers with rights to access and transfer certain types of data about themselves to accredited third parties in a machine-readable form[15]. The Right is slated to be implemented in the financial sector through Open Banking in July 2019, followed by energy, telecommunications, and other sectors as determined by the Australian Competition and Consumer Commission (ACCC)[15]. Opening up greater access for consumers to their own data is hoped to enable greater competition, more accurate product comparisons and innovation in product offerings.

The Review into Open Banking has suggested that only data provided directly by the consumer (customer-provided data) and transaction data be included as consumer data in the Open Banking framework[16]. With the Consumer Data Right still in development, it's unclear if the original 2017 Productivity Commission definition of consumer data will apply in its entirety to the reform, such as the inclusion of data purchased or obtained from a third party.

Importantly, both reports suggest that data which has been 'imputed' by a data holder about a consumer, through application of insights or analysis, may not necessarily be considered the consumer's data[14,16]. One simple example of 'imputed' data is where a company has acquired one or more consumer datasets, transforming them to develop a profile of a consumer, or to allocate a consumer to a particular class or segment. It's these profiles, segments, or transformed data that may not necessarily be included in the data that can be accessed or transferred by a consumer, as currently flagged by the Consumer Data Right.

This exclusion has implications — especially if that score, profile or segment is used by a company to target or restrict certain kinds of products and services — something explored further in Chapter 6. It also has implications if consumers have no right to transparency around how profiles or scores have been designed, or the right to correct the record if the data, analysis or algorithms are wrong.

Furthermore, the very large volumes of consumer data identified by the Productivity Commission currently being collected, shared and used by organisations around Australia will not be automatically governed by the Consumer Data Right. The Consumer

Data Right is voluntary and opt-in for Australian consumers, meaning that data collected, shared and used outside this Right can and will continue to occur, ongoing, without the protections that a complementary broader economy-wide reform would deliver.

Further consideration of the definition of consumer data is needed. Withholding consumer access to imputed data will enable industries to maintain and increase *data asymmetry*, that is, where companies hold greater information about consumers and the conditions under which they are offered or excluded from products or services.

This topic is discussed further in the section *'Emerging risks for consumer detriment and discrimination'.*

Defining personal information

As identified by the Productivity Commission 2017, a key component of consumer data is personal information. In Australia, personal information is defined in the Privacy Act as:

"[…] information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable."[17]

Clear examples of personal information provided by the Office of the Australian Information Commissioner (OAIC) include information such as an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, and commentary or opinion about a person, racial or ethnic origin, political opinion, religious beliefs, sexual orientation, criminal record, health information, credit information, employee record and tax file number information[18].

Of note is that information or opinion inferred about an individual from their activities *"such as their tastes and preferences from online purchases they have made using a credit card, or from their web browsing history"* were considered examples of personal information[18].

When assessing if information is 'about' an identified individual or an individual who is reasonably identifiable, the OAIC states that *"information will be 'about' someone where the person is a subject matter of the information or opinion"*[18]. Furthermore, when determining if a person is 'reasonably' identifiable, consideration is required as to whether other information can be reasonably linked to identify the individual based on the nature and amount of information, who will hold and have access to that information, and what other information is available that can practicably be used to identify an individual[18].

A court decision in 2017 on a case between the Privacy Commissioner and Telstra demonstrated the challenges to interpreting the definition of personal information[19]. Telstra argued that network data – geo-location data, which is based on the longitude and latitude of mobile phone towers connected to the customer's phone – was not considered identifiable information because the data at face value was anonymous[19]. The Privacy Commissioner argued that it could be cross-matched with different datasets to identify the customer[19].

It was the term 'about' in the definition of personal information, however, which led to the Administrative Appeals Tribunal (AAT) to make a decision in Telstra's favour[19]. The argument was that the geo-location data was not considered 'about an individual' because the data was 'about connection between mobile devices' as it was created for that primary purpose[19].

Legal expert Anna Johnston suggested that the AAT's interpretation undermines Privacy laws, and that the information could still be about an individual even if it was collected about something else, for example *"that metadata could be 'about' both the delivery of a network service and the customer receiving that service"*[19].

A new law since passed states that metadata kept by telecommunication companies under data retention rules is regarded as personal information[19]. It's unclear, however, what this means for metadata collected and retained by non-telecommunication companies.

By contrast, in Europe, an economy-wide General Data Protection Regulation (GDPR) has been established by the European Union (EU) which defines personal data as:

"[…] any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[20]

It is this broader definition of 'any information relating to' that allows the inclusion of broader types of data to be considered personal information, rather than using the term 'about' an individual[19]. This consideration is important because most data collected does not obviously match 'traditional' descriptions of personal data but can still be used to identify and profile consumers[21]. It is this evolution of privacy laws in line with technological advancement which we are yet to see in Australia.

The relationship between consumer data and privacy

The Privacy Act regulates how personal information is handled. It applies to most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers, and some small businesses[17]. Small businesses in Australia with a turnover of $3 million or less are generally *not* liable data holders under the Act. This is a significant portion of businesses as the Australian small business and family enterprise ombudsman suggests that majority (approximately 9 in 10) of Australian businesses are small businesses, defined in their report as having a turnover less than $2 million or employing fewer than 20 people[22].

The Consumer Data Right definition outlined above covers more than just 'personal information' and thereby offers better protection than the existing Privacy Act alone, but it only applies when consumers choose to access or port specific types of data (covered in the Consumer Data Right Framework) to an accredited third party of their choice. It is a voluntary right expressly for the purpose of acquiring the data as defined, or transferring the data as defined, leading to some advocates arguing it would be more accurately defined as a 'Data Portability Right'.

Essentially, the Right gives consumers the authority to provide a third-party service provider access to certain types information that is being held by their current provider to potentially offer them a better service (for example, to track their spending across banks, compare mortgages, or find better energy offers)[15]. The Right is also meant to give consumers greater control over how their nominated third party collects, uses or shares their ported data.

However, as highlighted earlier, the existing data sharing practices outlined in Privacy Policies or Terms of Service which allow companies (e.g. their current provider) to exchange consumer data with third parties for a variety of purposes can still operate outside of the Consumer Data Right Framework, as long as these companies fulfil their obligations under the Privacy Act.

While the law requires companies to provide Privacy Policies outlining how they manage personal information, privacy experts argue that these documents are often too long

and complex for consumers to read and understand[23]. Individuals who clicked 'I agree' to notices about the collection, use or sharing of their personal data may not have freely 'consented' to these terms and do not have the ability to negotiate the terms[23].

We reviewed Privacy Policy documents of a major online company which suggest that they share 'non-personal information' with third parties, *"we may share non-personally identifiable information publicly and with our partners"*, as well as 'personal information' in some circumstances (e.g.*"with your consent, with domain administrators, for external processing, [and] for legal reasons"*[24].

Google has suggested that personal information is information that personally identifies an individual, such as *"name, email address and billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account"*[25]. Facebook states that *"we don't share information [to advertisers] that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission"*[26].

A variety of other data, however, is being collected about individuals when using Google services such as their device information, search queries, browsing history, call and SMS logs, location information, who they contact/interact with online, purchase information and more[24]. Similarly, when using Facebook products, information about individuals such as their location, interaction with people/pages/groups, call/SMS log if the individual imported/synced contact information, type of content viewed, purchases, device, and more are collected[26]. Very little guidance in Australia has been provided as to whether this data is considered personal or non-personal information.

This is important because recent evidence has suggested that de-identified data can be used to re-identify people. Su *et al.* (2017) were able to link anonymised web browsing histories to social media profiles to correctly re-identify 70% of individuals[27]. Another study shows that datasets where the location of an individual is specified hourly can be used to uniquely identify 95% of individuals[28]. It is critical, therefore, that those who release data and regulate the release of data also consider the potential privacy breaches and uses before allowing transfers of what, in isolation, they might have considered to be 'anonymised' data.

The UK Information Commissioner's Office states that it is the first European data protection authority to develop an anonymisation code of practice[29]. It defines 'anonymised data' as *"data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data"*[29].

More operational advice is provided in the UK's Anonymisation Decision-Making Framework[30], which has been adapted by CSIRO Data 61 and the Office of the Australian Information Commissioner to develop the De-Identification Decision-Making Framework in Australia[31]. The framework recommends reviewing use cases and ethical obligations among other measures before sharing or releasing data.

Privacy advocates have argued, however, that it is not enough for companies to dismiss privacy concerns by claiming they are using 'anonymised' data if they are still able to 'single out' or identify users as the same person in various situations to deny access to services, alter prices, or target ads, even if they do not know their name or address[21,32].

This highlights the complexity of navigating a new era of data collection, sharing and use. No longer can we rely on old frameworks and assumptions. Greater consideration must be given by Australian policymakers, regulators and businesses to the potential innovations in technology, applications and use of personal information and consumer data in the digital economy.

Recent evidence has suggested that de-identified data can be used to re-identify people. Su et al. (2017) were able to link anonymised web browsing histories to social media profiles to correctly re-identify 70% of individuals. Another study shows that datasets where the location of an individual is specified hourly can be used to uniquely identify 95% of individuals.

Consumer data collection practices

This chapter explores some of the types of data currently being collected and their modes of collection.

Data can generally be obtained in three different ways[5]:

- **Declared data***: data consumers offer voluntarily through registration or transactions with a service.*
- **Observed data***: data consumers generate and supply passively such as social media interactions and tracked browser history.*
- **Generated data***: data generated by first and third parties through analysis, or in combination with other data.*

Many companies are collecting information about who individuals are (i.e. identifiable information), their social network, what they do online (e.g. browser history, interests and preferences), and even what they do offline (e.g. offline purchases, location tracking, microphone recording on mobile devices)[5, 33].

This information can be compiled internally through inbound email/website contact forms, customer records, inbound telephone inquiries, social media, surveys and competition entries[34]. When companies use internally compiled consumer data, approximately a third use the provision of contact details as consent to be contacted for marketing purposes[34].

Companies can also however, collect additional data that has been externally compiled by other parties such as obtaining data through public sources (e.g. public databases, data scraping), purchasing from third parties (e.g. data brokers), receiving consumer data through business partnerships, or swapping lists[34]. An identified advantage of obtaining externally compiled data is that it can be used to enhance the company's existing customer information.

Increasingly, companies are collecting observed data about consumers through tracking mechanisms. Consumers are also likely unaware of the extent of tracking online. It has been reported that the top 100 most widely-used sites are monitored by over 1,200 firms[35]. More data is also being collected about mobile users (100 data points per user) compared to desktop users (50-70 data points per user)[35].

Modes of passive data collection

A few examples of how companies can collect data about consumers (often through consent to lengthy complex Privacy Policies) are detailed below.

Cookies

In the online environment, users are being tracked through cookies, which are small text files that store information about the user's interaction with the sites[35]. Cookies are used to recall information about the user when they return to a web page, for example remembering user preferences on the site, and to personalise their experience[32, 35].

Cookies are necessary for some website functions for example displaying contents in the user's online shopping basket[32, 35]. Third-party cookies are cookies set by companies other than the website being visited[35]. They are often used for advertising and to track users across different sites[32, 35].

Web beacons/pixel tags

Web beacons or pixel tags are small invisible images that can be placed on a web-page or email and used in combination with cookies to track when users have opened emails or loaded a particular webpage[35]. Web beacons can be used for collecting information such as what users click on and their movements across websites[32].

Device information and tracking

User's device information such as hardware model, operating system version, unique device identifier, mobile network information, battery level, IP address and more, can be collected when individuals use online services[24,26]. Third parties can often gain access to device information and functions through app permissions that are granted at the point of installation[32].

Various technologies can be used to track a user's location through their mobile device. The most obvious is GPS (Geo-location tracking via satellites). However, users' location can also be tracked when their GPS is turned off, for example through Wi-Fi network sensors using the phones media access control (MAC) address, or through radio signals to mobile antennas[35]. Companies can use these technologies to track customer's movements near or around a store[35].

Companies can also track how many devices a user owns through known data (e.g. email address or log ins used on multiple devices, and other methods (e.g. audio beaconing played from one device and picked up by the other device)[35].

'Fingerprinting'

Companies can use a combination of specific data from devices or browsers as 'fingerprints' to recognise users (e.g. browser type, font preference, operating system, battery status, and more)[32, 35]. Fingerprinting can be used to recognise the same device across multiple online sessions even if cookies are deleted, user login changes, or IP addresses are hidden[32, 35].

Facial recognition

Companies can use biometric software to identify individuals through facial recognition. Facial recognition is increasingly being used in stores[35] and online (e.g. Facebook).

Payment cards & loyalty cards

Even in the offline environment, a customer's purchasing behaviour can be tracked at a store without having to scan their loyalty card. For example, Woolworths Rewards Privacy Policy indicate that they can still track customer's transaction history when the customer chooses not to scan their Woolworths Rewards card at the point of sale[36].

"We also collect Members' transaction history from the use of their payment card, which is matched to their Woolworths Rewards account. Our systems render payment card numbers unreadable (through the use of cryptographic hashing or encryption algorithm) and replace it with a randomised token number, which protects such details from unauthorised access or disclosure. Linking this token number with a Member's account enables us to collect the Member's transaction history even when they do not scan their Woolworths Rewards card at the point of sale. The collection of this information enables Woolworths to continue to provide Members with personalised and more engaging and relevant offers than they would otherwise receive."[36]

Data collection from third parties

Another way companies collect data about consumers is through the use of third parties. This can occur through data brokers, or by 'partnering' with third-parties to enable data sharing between companies.

Another way companies collect data about consumers is through the use of third parties. This can occur through data brokers, or by 'partnering' with third-parties to enable data sharing between companies.

Data brokers hold large amounts of information about consumers globally; for example, Acxiom's databases contain information about 700 million consumers worldwide and 3000 data segments for nearly every consumer in the United States (US)[32,37].

In 2012, the US Federal Trade Commission (FTC) initiated a study of nine data brokers and subsequently published a report calling for greater transparency and accountability by data brokers[37]. A bill for a Data Broker Accountability and Transparency Act of 2017 was introduced and referred to the Committee on Commerce, Science, and Transportation by the Senate in the United States in September 2017[38].

The nine data brokers involved in the 2012 study were Acxiom, CoreLogic, Datalogix, eBureau, ID Anlaytics, Intelius, PeekYou, Rapleaf, and Recorded Future. This sample of data brokers provided a 'cross-section' of large, mid-sized and small data brokers[37]. The report indicated that data brokers collect information about consumers for a variety of purposes, but generally do not interact directly with consumers. As such, consumers are largely unaware that data brokers are collecting or using their information[37].

Data brokers collect information from commercial, government and other publicly available sources (*see Figure 1*), where they can also derive inferred data about consumers, such as interests, loyalty or other characteristics[37].

The FTC 2014 found that data brokers also obtain information from other data brokers that hold commercially sourced data, sourced from telephone companies, car dealers, other merchants, and data consumers provided through surveys, warranty registrations and contests[37].

The FTC (2014) found that data brokers resell or share information they have collected about consumer data with other companies and data brokers[37]. They typically offer three main types of products: marketing products, risk mitigation products, and people search products[37].

In 2012, the nine data brokers generated a combined total of approximately $426 million in annual revenue, where over $196 million was made through offering marketing products[37].

In terms of product offerings, these vary from firm to firm. Experian's website states, for example, that they provide *"businesses like yours with a deeper understanding of consumers' characteristics by overlaying demographic information and Mosaic USA household lifestyle segmentations on to your file any time day or night: define unique attributes of your best and most profitable customers; anticipate likely future behaviours and buying trends; [and] identify prospects most like your best customers for new growth opportunities"*[39].

To get started, Experian provided the following instructions[39]:

1. *Select from one of the pre-defined data packages or build your own set of data.*
2. *Upload your customer list to Experian. Don't worry, your data is 100% secure and we never share or sell this information.*
3. *Experian will match your customer records to the data elements in your package and notify you as soon as your file is complete*
4. *Log back in to complete your registration, purchase, and download your appended file"*

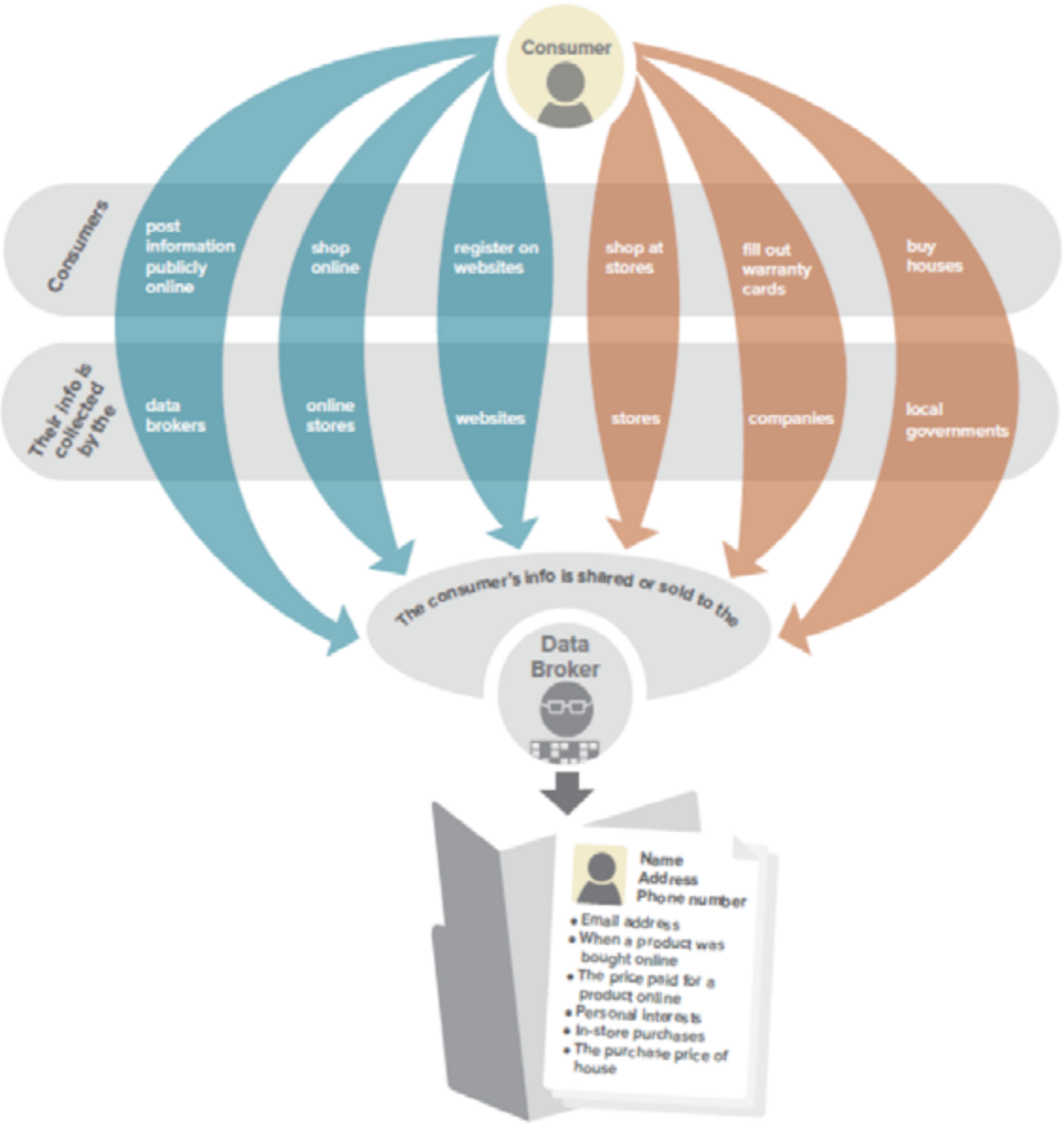

Figure 1: Original figures of online and offline data collection by data brokers. Source: Federal Trade Commission, 2014

'Data append' is a service provided by data brokers to provide companies with an enhanced view of their customers[37]. Data brokers can also use a process called 'on-boarding' which combines online and offline data for advertisers to better target consumers[37].

For example, the Head of Marketing at CoreLogic, a large provider of property information and management services in Australia, indicated that the database company Quantium could overlay CoreLogic's property data with datasets from NAB, Foxtel, Woolworths and News Corp through a partnership model, to more accurately identify people whom they could target as potential vendors[40]. Davis gave examples of how information about an individuals' spending patterns and how long they have owned the property could be overlaid to indicate that the owner may be looking to downsize their property: *"using big data to identify four bedroom, two bathroom home owners who have owned their home for more than 10 years near your target property on Facebook with additional data elements that signal their children are leaving home. This might be that their grocery bill has significantly reduced in past months, that they're spending more on entertainment and dining out, or at hardware stores sprucing up the place"*[40].

Whilst some might argue that this level of detail may improve the consumer experience by enabling them to receive more relevant offers, the clear lack of transparency and choice provided to consumers about how consumer data is being collected, used and shared remains ongoing. Individuals who have provided data to these separate entities may not have reasonably expected that their data could be amalgamated to profile and target them with this level of detail. Individuals might not make the connection at the point of providing information how their data could be used for profiling as this does not tend to be a visible process for data subjects[41].

Lastly, in relation to these sharing and amalgamation practices, consumers might not be aware that the provision of data to one company for one purpose can quickly end up being used for purposes different from those it was originally collected for — a person using grocery shopping loyalty cards for shopping deals may not typically expect their data to be used to monitor and predict if they were going to sell their home, even though this activity might still hold true to the clause, for 'marketing purposes'.

The need for protections to evolve to better reflect consumer expectations is clear and explored further in Chapter 7.

Consumers might not be aware that the provision of data to one company for one purpose can quickly end up being used for purposes different from those it was originally collected for.

How is consumer data collection and sharing enabled?

The primary way in which consumer data collection and sharing is enabled is when consumers 'consent' to Privacy Policies and Terms & Conditions when signing up or using products and services.

Vague terminology in companies' Privacy Policy documentation often enables the collection, combination or sharing of data about their customers from partners and third parties to improve their services[42].

The following examples are direct extractions from various Privacy Policies accessed in the past few months and available on company websites.

Woolworths Rewards Privacy Policy[36] states under the section *'Collection from others'*:

"We collect personal information about Woolworths Rewards Members from other persons or entities. For example, we collect personal information for marketing purposes from other suppliers of goods or services who, like us, have an existing relationship with Woolworths Rewards Members. Such entities include our strategic partners, Earn Businesses, affiliated programs, suppliers of publicly available information and digital services used by Woolworths Rewards Members (including social media platforms).

"For purposes other than marketing, we collect personal information from persons and entities that assist or partner with us in supplying our goods and services to Woolworths Rewards Members, administering and improving the Woolworths Rewards program and conducting our business generally. These entities include insurers, providers of publicly available sources of information, delivery service companies, possible business sellers and buyers, third party data providers and our related bodies corporate. At times, we combine different sets of data to add to the personal information we hold. An example of this is a history of a Member's transactions from use of the same payment card."

Google Privacy Policy[24] states under the section *'When Google shares your information'*:

"For external processing: We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures"

Facebook recently updated its Privacy Policy, which is now more explicit than the previous version about how it collects and combines data from partners and third parties[26]; under the section '*What kinds of information do we collect?*':

"Advertisers, app developers and publishers can send us information through Facebook Business Tools that they use, including our social plugins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook – including information about your device, websites you visit, purchases you make, the ads you see and how you use their services – whether or not you have a Facebook account or are logged in to Facebook...We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information."

Some company policies might contain reassuring statements in the Privacy Policies such as *"We will only disclose personal information to others if you've given us permission…"*. However, this may not provide adequate protection if access to their services is conditional to providing permission to share with others at the point of signing up, particularly if the initial consent provides a 'free pass' to all uses and there is no optionality to choose between different types of uses and sharing.

Research suggests that consumers often blindly agree to Privacy Policies and Terms of Services without being aware of the risks[43]. Experts argue that many people simply give consent whenever they are shown a consent request[41].

A study observing the online behaviour of users accessing a fictitious social networking site found that 74% did not read the Privacy Policy and 98% missed a clause in the Terms of Services about giving up their first-born child[43]. Of those who did read the Privacy Policy and Terms of Services, they spent less than a minute reading either documents, which should have taken approximately 15 and 30 minutes respectively to complete.

Typically, users do not read policy documents because they are too long, difficult to comprehend, difficult to find, or because users perceive the cost to benefit ratio of reading to be high[41, 43, 44, 45].

An Australian study by consumer advocates Choice, found it would take nine hours to read the Terms and Conditions of Amazon Kindle[46]. Another study estimated that it would take an individual 244 hours a year to read Privacy Policies for each new website they visited—an average of 40 minutes a day[47].

Choice raised concerns that companies are forcing consumers to agree to contracts that they cannot reasonably be expected to have read, and that consumers can miss unfair clauses that are embedded in these long contracts[46]. Furthermore, despite expressing concerns about privacy, people often provide their personal information because of convenience, discounts, other incentives, or a lack of understanding of the consequences[41].

Consumers are often unaware of the conclusions which can be drawn from their data[32]. Furthermore, even if consumers are aware, they have little ability to negotiate with the privacy terms outlined by the company if they want to access products or services[23]. The power imbalance in negotiations and the lack of ability to detect these practices may leave consumers with little protection or opportunity for redress[32].

It is clear that the current method of 'informed consent' through Privacy Policies and Terms of Services alone is ineffective. More work is needed to provide consumers greater transparency, control and choice over how their data is collected, used and shared.

Benefits of consumer data

Many innovations have been made possible because of access to Big Data. The opening up of data can enable greater competition between providers, innovation in products which are more relevant to the needs of consumers and efficiency improvements in service delivery. It can result in reductions in cost to services, improvements in consumer experience and utility, and enhancements in everything from well-being, infrastructure investment and safety.

The responsible opening up of access to consumer data with adequate protections unquestionably has the ability to drive improvements in our quality of life. A few emerging applications and benefits are explored below in this chapter.

Improved public health

Perhaps one of the most significant benefits of greater collection and access to personal information and consumer data is the ability to develop better medical technologies to improve public health. For example, artificial imaging technology has been developed to detect skin cancer with greater accuracy (95%) compared to manual methods (75%-84%)[48].

Technological advancements are also enabling greater equity and inclusion for people with disabilities, such as smart-glasses to assist the visually impaired, hearing artificial intelligence to assist the hearing impaired[49], and real-time feedback from sensors in prosthetics to improve the experience of those with physical disabilities[50].

Fraud detection

In 2016, The Australian Payments Network (formerly the Australian Payment Clearing Association) reported that Australians transacted $1,869,357 million using cards and cheques; of this total, fraud accounted for $540 million*[51]. In the 2017 Australian Community Attitudes to Privacy Survey, one in ten Australians reported they had previously been a victim of fraud and 69% were concerned about identity fraud or theft[3].

One benefit of collecting more granular data on consumer purchases, locations and interaction is to better identify suspicious activity and detect fraud, thereby protecting consumers and businesses from financial loss[35,37]. This is particularly important as approximately 80% of Australian consumers are now banking online and over 70% now making purchases online[52].

Improved efficiencies and processes

When we have more knowledge about what products and services are demanded, and where, both businesses and government can make more efficient investment decisions. For example, datasets can inform urban planning or improve public transport[53], improve access to healthcare services[14], make processes more efficient by stocking products in locations according to demand[35], and monitor the use of resources such as energy and water[14].

*Statistics updated from previous version of CPRC report (updated 17th July 2018)

More relevant advertising

Businesses are using data to better understand what consumers want and how they respond to goods and services[5]. This can be both beneficial to businesses and consumers, for example, personalisation of advertisements or products means that the businesses are targeting the right people and reducing costs while the consumer is receiving relevant offers and products/services that better match their needs[5, 37].

Access to more suitable products

Improved access to their consumer data and information about different product offerings may assist consumers in comparing and switching to an alternative provider that better meets their needs[14, 54]. For example, the Victorian Government uses data provided by the consumer to compare suitable energy offers so consumers may find cheaper deals[55]. Access to more diverse data can also improve the accuracy of algorithms and potentially promote more inclusive access to benefits[56].

Improved access to their consumer data and information about different product offerings may assist consumers in comparing and switching to an alternative provider that better meets their needs.

Consumer data as a competition enabler

Companies with an ability to amalgamate and collect significant amounts of consumer data are at a competitive advantage when compared to companies without such capability. Sometimes, this capability difference has emerged due to the breadth of data collection abilities that a company can have across multiple markets and platforms at the one time, or due to the organisation historically being required or regulated to be the data collector.

Additionally, if only one firm has full access to data about a consumer, then only they are able to target a product or service in full knowledge of what will or will not best suit that individual. By giving consumers a right to their own data, and an ability to share that data with other providers, this can incentivise competitors to tailor and design products that better suit consumer needs.

The benefits to flow to consumers from greater data collection and analysis are significant. Ensuring data can be opened up to drive innovation and competition with the appropriate protections is key to a vibrant and productive digital economy.

Emerging risk for consumer detriment and discrimination

Greater amounts of data collection enables more detailed knowledge to be acquired about who we are as consumers, and as individuals. As highlighted in prior chapters this can deliver significant benefits, however, without complementary protections and evolutions of the policy framework these same practices and technologies can result in detrimental and discriminatory outcomes for consumers.

One obvious avenue for detriment to consumers in relation to increased data collection and sharing is the increased risk of identity or financial theft if the data is not stored or transferred securely[35]. Less obvious, however, is how consumer profiles can be developed and used in ways which may result in discrimination or exclusion.

Consumer profiles, scores and segments

With increased digitisation, data generation, data storage and data processing, it is now becoming common for companies to use statistical methods to profile, rate people (e.g. credit score), or predict their personality and behaviour[32].

One example is using data for personality prediction. The 'Big Five' model is a leading model of personality psychology, used to predict users' characteristics—innovations have now enabled this to be conducted based on digital data[32]. The model measures five personality dimensions which include extroversion, agreeableness, conscientiousness, neuroticism, and openness[32]. Numerous studies that have looked at how different types of data such as a person's call log, text message log, apps most frequently used, Facebook likes, or websites visited, can be used against the Big Five to predict personality traits with varying degree of accuracy[32].

Similarly, other predictive analysis might also be possible via Facebook likes to predict sensitive personal attributes such as ethnicity (95%), religious (82%) and political views (85%), sexual orientation (75% to 88%), and consumption of alcohol (70%), cigarettes (73%) and drugs (65%) with varying degrees of accuracy[32]. Seemingly harmless release or user generation of data can reveal much more about a person than one would typically expect.

Christl and Spiekermann (2016) reported that start-up companies are collecting and/or purchasing data from third parties, such as data brokers, to predict an individual's creditworthiness and are providing their credit scoring technology to other companies. The researchers suggested that companies are using proxies, such as how they fill an online application form, online shopping behaviour, number of times they have moved homes, social connections, and even variables such as battery levels, to generate a credit score for a user[32].

There is also some evidence to suggest health or life insurance companies are purchasing information from data brokers traditionally used for marketing (e.g. occupation, education, income level and sports activities) to predict disease and health risks[32].

As highlighted in previous chapters, consumers may not make rational decisions or be fully aware of the consequences of giving away their information, because the benefits are presented upfront while harms are often hidden[57]. The release of data for one purpose within a specific context, but its use in another unrelated context, makes the relevance of the data and proxies being used for the context important. Not only can profiles be built on incorrect information and data, they can also be built on wilfully

incorrect information provision – some 46% of the population admit to providing false personal details in order to protect their information[3]. We will explore some of the issues with the development of profiles using algorithms later in this section.

Personalised pricing and product offerings

While companies often require data from consumers to assess financial or insurance risk (for example due to responsible lending obligations under the National Consumer Credit Protection Act 2009)[58], consumers may not be aware of the data companies are using to create profiles of them to determine their access to products or services, or to price discriminate[59, 60]. There are different degrees of price discrimination[59]:

- **First degree**: when consumers are charged an *individual price* based on the *maximum price they are willing to pay*.
- **Second degree**: when there is a pricing scheme based on the *quantity bought* rather than consumer characteristics. For example, the prices of individual goods or services might be cheaper if purchased in larger quantities/bulk, than if they were purchased individually.
- **Third degree**: when the 'price-to-marginal-cost-ratios' are different between *groups* or *types of buyers*. For example, charging people different prices based on their characteristics such as location, age, etc.

Price discrimination isn't always considered unfair – it depends on the product and the market. It is argued that third degree price discrimination could potentially benefit the disadvantaged if it is used to lower the prices for those who can only afford to pay less (for example pensioner, concession and student discounts for movie tickets). However, Borgesius & Poort (2017) suggest that the closer personalised pricing approaches first-degree price discrimination, the worse off consumers will be compared to producers[59]. As Plunkett (2017) highlights, price discrimination is by no means new, but it is being enabled and super-charged by technology and data collection in a way we've not seen before.

Online retailers can use Big Data to facilitate first degree price discrimination by steering consumers to products and services that closer match what they are willing to pay in real-time, based on behaviours or attributes, such as what they previously purchased, if they are a high spender, and what they have browsed and not purchased[32, 59, 60].

The Wall Street Journal, for example, reported that a company called Orbitz advertised more expensive hotels to Mac-users than PC-users based on data that suggests Mac-users spent 30% more on hotel bookings[35].

Some researchers suggest that two individuals may be presented different prices for the same product or service based on the information the company has about the customer[59, 60]. A study conducted by Mikians *et al.* (2012), for example, found evidence of online price differences based on the customer's geographical location, whether they were considered affluent or budget conscious customers, and if they visited a vendor site directly or if they were re-directed to a vendor site via a discount aggregator site[61].

This clearly presents risks for vulnerable or disadvantaged consumers if profiling practices are used to identify 'high value' and 'low value' consumers, particularly in essential service markets. While interventions and reforms around the world into competitive markets are aiming to deliver fairer prices for consumers, one area attracting little attention is the extent to which price monitoring powers are being extended to regulators, to better assess the extent to which profiling is resulting in more vulnerable consumers being offered higher-priced products, or excluded.

Although personalised pricing and discrimination does not appear to be a widespread practice online, the potential is certainly there for business to exploit[59, 62, 63]. Comprehensive information on business practices is often limited and undisclosed, making it difficult to detect harmful practices[32]. Algorithms used for business practices remain opaque because they are considered to be trade secrets[32].

Christl and Spiekermann, in their research of data sharing networks, argue that *"users are often informed incompletely, inaccurately or not at all about which data is being collected and shared with third parties"*[32].

The imbalance of information about the product and trade between companies and consumers presents a clear information and data asymmetry. Without corresponding reforms to rebalance the information asymmetry or ensure vulnerable consumers are not targeted with inappropriate products, or excluded from markets, inequality will rise and place increasing pressure on hardship and social support measures.

Although personalised pricing and discrimination does not appear to be a widespread practice online, the potential is certainly there for business to exploit. Comprehensive information on business practices is often limited and undisclosed, making it difficult to detect harmful practices. Algorithms used for business practices remain opaque because they are considered to be trade secrets.

Exclusion from access to products and services

Tools that allow targeting based on consumer attributes, interests and behaviour may also result (unintentionally or otherwise) in unfair exclusion to accessing products and services. A range of examples of such practices include:

- Money, CNN News in March 2018 reported that Facebook was being sued for allegedly allowing landlords and brokers to exclude ads from being displayed based on the user's gender, family status, and interest categories such as 'disability parking permits'[64]. This case is still before the courts[65].
- CNN Tech News reported that lenders are using data on social networks to determine the creditworthiness of potential clients to grant or reject their loan applications[66]. Lenddo, for example, allegedly takes into account if an applicant's Facebook friends had made late repayments when considering whether to approve or reject a loan application[66].
- Wired News reported that it is possible for companies to use basic information such as the type of device someone is using, their operating system (iOS vs Android), how they got to the site (e.g. if clicked on an ad), type of email provider (Hotmail or Yahoo vs. others) as proxies to predict if a user is likely to default on a loan[67]. Although the practice is not widespread, the researchers suggest that some retail companies are already using data for this purpose[67].

In Australia, the Government is enforcing mandatory comprehensive credit reporting. Consumer groups have raised concerns that mandatory comprehensive credit reporting data may be used by non-credit licensees, such as telecommunications and utilities services, to make it harder for consumers with poor credit ratings to access these essential services[68]. Aside from possible exclusion, there are also concerns about the risk of profiles being developed for 'vulnerability-based marketing'. One example of this is consumers experiencing hardship potentially being targeted with exploitative loans[42].

Problems with using unchecked algorithms for decision-making

A common misconception is that technology is neutral[32]. Technology, machine learning and coding practices are all increasingly enabling detailed algorithms to develop profiles and determine outcomes for consumers.

What data goes into the algorithms and profiles is therefore of significance. The quality of data, the appropriateness of the proxies being used, and the extent to which there is transparency all have the ability to impact consumer choice. Part of the challenge here is that the people building the algorithms and scores often have no expertise in the field for which the data and tools are being deployed. As recently highlighted by Bank of England Chief Economist Andrew Haldane, this also highlights the difference of relying on inductive as opposed to deductive reasoning when analysing a problem[69].

Deductive reasoning, Haldane argues initially uses a theoretical framework, before making measurements to test and deduce if a hypothesis is true or not[69]. Inductive reasoning, the primary method for data scientists, in contrast does not depend on a theoretical framework but relies on the mining and observed correlation of data to inform choices and models of behaviour[69]. Haldane suggests that the approaches should complement rather than substitute each other because deductive reasoning alone may limit new insights to be made, and inductive reasoning alone may create unreliable predictive models if untested against theories and causality. Therefore, it may be beneficial for data scientists and theoretical experts to collaborate in the fields which the data and tools will be used.

Globally, data experts are raising concerns around the potential harms of algorithms in perpetuating discrimination of marginalised groups. Data scientist Joy Buolamwini, for example, found that generic facial recognition software recognised a white mask as a human face over her dark-skinned face[56]. Buolamwini argued that the lack of diversity in training datasets meant that these technologies do not accurately recognise diverse faces, which can result in exclusionary experiences or discriminatory practices[56]. This meant that some groups may not be able to fully participate in the benefits of some technologies or, conversely, be disproportionally affected by inaccurate recognition, such as in law enforcement regimes[56, 70].

Another data scientist, Cathy O'Neil, has sparked an international conversation in her book *Weapons of Math Destruction* by describing how opaque algorithms can lead to unfair outcomes[71]. O'Neil highlighted how biases in algorithms have contributed to unfair scoring of teachers' performances, unfair recruitment for jobs, and longer prison sentences for minority groups[72].

Another identified problem is the lack of gender and cultural diversity among data scientists who develop algorithms[73]. Just as greater diversity has been shown to improve performance and decision-making of companies[74], this lack of diverse viewpoints in the data science field can make algorithms more prone to bias. The issue has led to the emergence of organisations such as O'Neil Risk Consulting & Algorithmic Auditing, Algorithmic Justice League, and Information Ethics and Equity Institute, which aim to raise awareness about algorithmic bias, provide a platform for people to voice their concerns, and provide businesses with guidance on how to develop ethical algorithms that are inclusive and fair[56, 75, 76].

There are significant learnings for the policy-making and business communities in the evolution of technology and data analysis – many different fields of expertise have a role to play – data ethicists, social scientists, psychologists, behavioural and legal experts all can make a valuable contribution. Now more than ever before, adopting a diverse, flexible and open approach to the evolving policy & regulatory landscape is critical.

Greater transparency of algorithms, profiles and scores can also play an important role both to ensure that companies are complying with laws and regulation, and to ensure fair outcomes for consumers.

Australian's knowledge, behaviour and attitudes about data collection, use and sharing

Ensuring that policy, regulations and practice are consistent with community and consumer expectations is central to the operation of sustainable markets and businesses in the new digital economy.

To build the Australian knowledge base of current consumer knowledge, behaviour and attitudes about data collection, use and sharing practices, CPRC engaged Roy Morgan Research to conduct a nationally representative survey of 1004 Australians throughout February and March 2018, along with two complementary focus groups. Comparisons with other studies, are also drawn, where relevant.

A supplementary summary table of results from the survey is provided in *Appendix B*.

Knowledge of data collection and sharing

By and large, Australians surveyed understood that companies have the ability to follow their activities across many websites (91%). Participants also had some understanding that their information was being shared with third parties (*see Table 1*). Despite general knowledge of data collection and sharing, focus group feedback revealed that consumers do not fully understand specifically what types of information are being collected and shared about them.

> *I'm, aware that it happens, but not to what extent*

> *I confess, I sometimes wonder what I am agreeing to… .*

> *Once you share your information, you cannot trace it.*

> *I don't know how I can decipher where my data goes and how it's used. It concerns me, but it's not transparent to me.*

> *I don't see how or why they are using the data, and I'm more frustrated with this.*

Table 1. Australian consumer knowledge about data collection and sharing.

	True	False	Don't know	Correct answer
Companies today have the ability to follow my activities across many sites on the web*	91%	2%	7%	True
In store shopping loyalty card providers like Flybuys and Everyday Rewards have the ability to collect and combine information about me from third parties	73%	4%	23%	True
Some companies exchange information about their customers with third parties for purposes other than delivering the product or service the customer signed up for	88%	2%	10%	True
All mobile/tablet apps only ask for permission to access things on my device that are required for the app to work	26%	47%	27%	False
When a company has a privacy policy, it means the site will not share my information with other websites or companies*	19%	59%	22%	False

*Questions derived from Turow et al (2005)

Survey participants were less knowledgeable about the ability of mobile applications (apps) to access information on their device unrelated to the app's function, with only 47% currently identifying that mobile apps often have the capacity to collect device data unrelated to the app's function. This lack of knowledge about apps was consistent with findings from OAIC's 2017 Community Attitudes to Privacy survey, where only 3% considered smartphones/apps as a way their personal information could be lost[3]. This suggests that Australians are largely unaware that apps can be granted access to more information than is required for them to operate[77].

Another study by privacy enforcement authorities found 31% of 1,200 popular apps accessed data not required for functionality[32]. One example of unnecessary access is a Flashlight-Torch LED Light app gaining permission to user's location for 'market/customer analysis' and audio via microphone for 'delivering targeted advertisement'[32].

There are also reports to suggest that many mobile phone apps transfer data to third parties in general[32]. A study of 110 popular apps found they shared the following sensitive information with third parties[32]:

- 45%: email address
- 40%: location data
- 34%: name
- 15%: gender, and
- 11%: information on friends.

The Norwegian Consumer Council recently launched a campaign called #appfail to raise awareness on this issue, but we are not aware of any similar activities in Australia[78].

CPRC's survey also revealed a lack of knowledge about Privacy Policies. 19% of Australians wrongly believed that if a company had 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 (*see Table 1*). Australians, however, fared much better than Americans in this respect; research in the US reported that 75% of Americans believed that a website with a privacy policy would not share their information with others,

however, we do note that this study was conducted in 2005 and digital literacy would likely have improved significantly since that time[79].

Notice and choice – opinions and behaviour relating to Privacy Policies and Terms

The majority of Australians admitted they do not read Privacy Policies or Terms & Conditions frequently, with only 6% reported reading the documents for *all* the products or services they signed up to in the past 12 months (*see Figure 2*). This is consistent with other research that suggest the majority of people do not normally read Privacy Policies or Terms[3, 41].

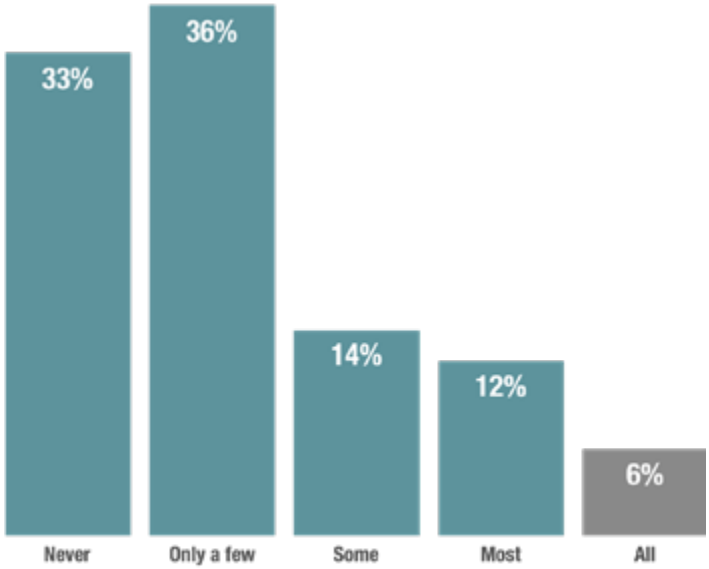

Figure 2. Percentage of Australians who read a Privacy Policy or Terms & Condition when signing up for a product or service in the past 12 months. Where percentages add to 101%, this is due to rounding error; percentages are rounded to the nearest whole number.

Some focus group participants indicated that they do not read Privacy Policies for larger and more reputable companies.

> *"It depends on who or what it is. I don't read them for some of the bigger kinds of companies, but for the kind of smaller companies that I've never heard of, I would do because I don't know any of their information.*

> *"It depends on the company… if it's a reputable company, it tells a story… If it's a company I haven't heard of, I wouldn't sign up.*

Others suggest that they might read the terms depending on the service they are accessing.

> *It depends on what I am signing up for. Like if I am order [sic] food online, I wouldn't look at terms and conditions, but big companies I might, depending on the relationship I have with the company.*

> *If money is involved, I might look, but if there's something else… I can't think of an example, but I tend not to read the terms and conditions.*

The focus groups may have revealed part of the reason why some consumers readily 'consent' to sharing their data, because they assume the laws would protect them against misuse or want to believe that companies would not misuse their data.

> *I expect the law to deal with that.*

> *I'd like to think that they're using it for good and not evil.*

Another reason may be because participants feel they have no control over how their data is collected, used or shared.

> *I think it's unethical, but it's the digital world we live in.*

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

> *I just close my eyes and don't think about it.*

Of the 67% of Australians who reported reading a Privacy Policy or Terms and Conditions for one or more services/ products they signed up to 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.

These sentiments echo those of EU participants in another study who suggested they did not read online policy documents because they assumed the law would protect them, or because they felt a sense of helplessness[41].

It is evident that Privacy Policies and Terms & Conditions currently do not allow consumers to give genuine consent.

Of the 67% of Australians who reported reading a Privacy Policy or Terms and Conditions for one or more services/products they signed up to 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. The most common reason was that it was the only way to access the product or service (73%) (*see Figure 3*).

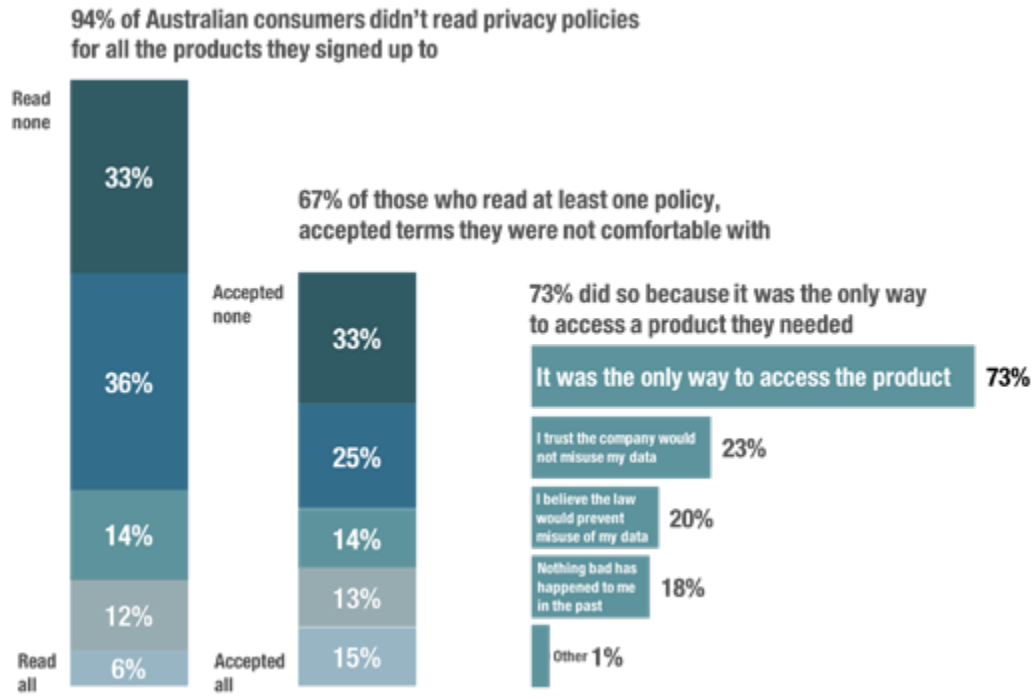

Figure 3: Reasons why Australian consumers accepted policies despite feeling uncomfortable. Where percentages add to 101%, this is due to rounding error; percentages are rounded to the nearest whole number.

Another study of EU participants also suggests a lack of genuine consent to Privacy Policies. 31% of respondents who were dissatisfied with a site's Privacy Policy indicated they would still proceed to using the website, and 22% indicated they don't know what they would do[41]. Experts also argue that consumers have no real choice because consent is often framed as 'take-it-or-leave-it offer'[80].

Focus group participants suggest that company policy documents currently do not serve as an effective tool for 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.*

> *I skim through them, read any text that is interesting, highlighted in red, but even then, I don't understand what it means, and I don't get much out of reading it.*

Attitudes to data sharing and use

The 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 (*see Figure 4*). This is consistent with findings from OAIC's 2017 Community Attitudes to Privacy survey which suggests that 79% are uncomfortable with businesses sharing their information with other businesses[3].

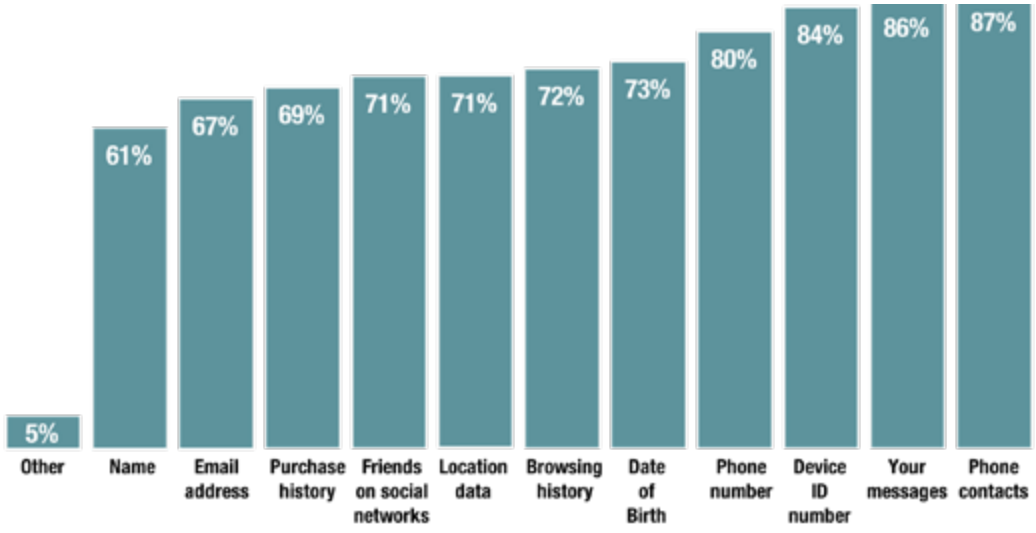

Figure 4. Types of data Australians are uncomfortable sharing with third parties for secondary purposes.

Several focus group participants expressed concern about what companies are tracking and profiles companies may be generating about them.

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

> *I feel uncomfortable with this modern-day technology and these privacy laws now… . How does one company happen to be the company you're with, then all these other companies (say power) get your information on that company. How can they do that and get away with it?*

> *They can look at your browsing history and get a better picture of yourself than you have. People are not quite aware of the extent of data trawling that happens.*

> *There is overt info e.g. date of birth, bank account numbers…There's other information that's inferred from that information. So, there's two things going on, there's the stuff you don't want to share, which is overt (marital status, address, phone number, bank account details), and that's simple in a way. There's this other series of information which is inferred, largely though 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 scarier part. No one is ever going to give the PIN number to their bank account, but other bits of information which are far more valuable, that can be inferred… that information is highly valuable.*

One participant also questioned if they are receiving enough value in return for their data.

> *Big Data is the most valuable thing in the world. They should pay us to collect it.*

The level of comfort to data sharing varied depending on the purpose of use and the degree in which participants felt they had control over how their data was used and where it is shared.

> *I'm more concerned about the on-selling than the company I gave it to using it. If I'm not offered anything, then whatever, but… if all my information is in one place, and they are hacked, then I'm more worried about someone using my data for illegal things.*

> *Have no problem with data being merged, but not misused.*

> *It's okay if it's not used to shame me... .*

> *Some things, like my contact details and medical records. I don't want someone to use that data against me to get insurance or something when I didn't give them that information. I don't want that to be mixed."*

Focus group participants expressed concern of how data about them could be obtained without their knowledge to put them at a disadvantage or put their safety at risk.

> *Employers do internet searches, and people share way too much information and can lead to losing or not getting a job.*

> *Harassment or physical threats are a possibility. The idea of stalking freaks me out, so I try to never share my postcode.*

Furthermore, participants raised concerns about the potential negative impacts of unregulated data collection, use and sharing on children.

> *There is a risk to children if they share information and they don't understand what they are sharing, and why they shouldn't share that information.*

> *Students over share, and that puts them at risk. Students are at risk of reputational damage as they are documenting more of their lives. For example, if they get into a fight, someone puts the video of it up online which is always there. This may prevent them getting a job in future; but then it can also be helpful to have it if they later on do [sic] other crimes.*

With regard to the use of their data for personalized pricing or product offerings, majority of survey participants did not find it acceptable if it meant some customers would be disadvantaged (*see Figure 5*). More than four in five Australian consumers did not find it acceptable if their data was 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%).*

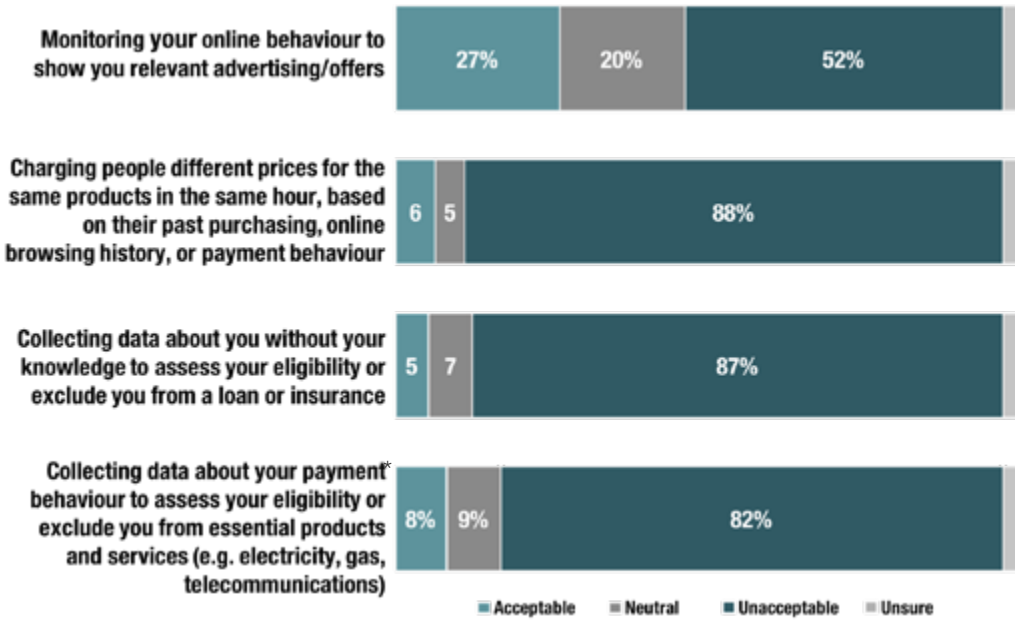

*Figure 5. Consumer acceptability of certain uses of their data. *Question adapted from Turow et al (2005). Where percentages add to 101%, this is due to rounding error; percentages are rounded to the nearest whole number. Categories were collapsed for ease of interpretation, refer to Appendix B for full detail.*

However, focus group participants identified that differential pricing can be fair in some cases, where it can enable better access to products for certain groups such as pensioners.

> *It can be very fair. For example, if you're a pensioner and you get discounts. I'd like to think that when I'm a pensioner I'll be able to get discounts on things I've paid full price for all my life.*

It was also considered appropriate to some extent for assessing risk and eligibility to some risk-based products, but not for essential products.

> *Not a big thing if they are using it for the determination of eligibility. It is okay to withhold services if for a legal reason, or about risk, but not in retail.*

> *What happens if it's an electricity supplier or gas supplier or water supplier? You're talking here about a fundamental human right. It isn't just if you buy Mars bars or Kit Kats. I think in that area there's a problem if you're being denied services when it's a fundamental service that every human being needs.*

Approximately half of Australians surveyed did not find it acceptable for companies to monitor their online behaviour to show them relevant advertising and offers (*see Figure 5*). These findings are similar with OAIC's 2017 Community Attitudes to Privacy survey where nearly two thirds of respondents were uncomfortable with search engines and social media sites targeting advertising based on their online activities[3].

Survey results and focus group feedback suggest that not all consumers are against the use of their information to receive targeted ads; approximately one quarter of survey participants found it acceptable to use consumer data to inform relevant advertising and offers. Some focus group participants said they appreciated relevant advertising and improved offers based on their interest. These situations generally included getting 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.*

This is consistent with OAIC's 2017 Community Attitudes to Privacy survey which suggests, 33% of Australians would trade personal information for rewards and benefits, 32% for better customer service, and 20% to win a prize[3].

Use of data protection strategies

Survey responses indicate that consumers have a desire to protect their information and are aware of some strategies to protect their information.

96% of Australians surveyed have used products or services provided by major companies they trust as a strategy to protect their data or information (*see Figure 6*). Other common strategies include selecting 'opt out' when available (94%), clearing their browsing history (90%), and choosing not to use the product/service (90%). Australians are less familiar with strategies like using incognito and adjusting ad settings, with 21% and 15% respectively reporting that they did not know how to access these options.

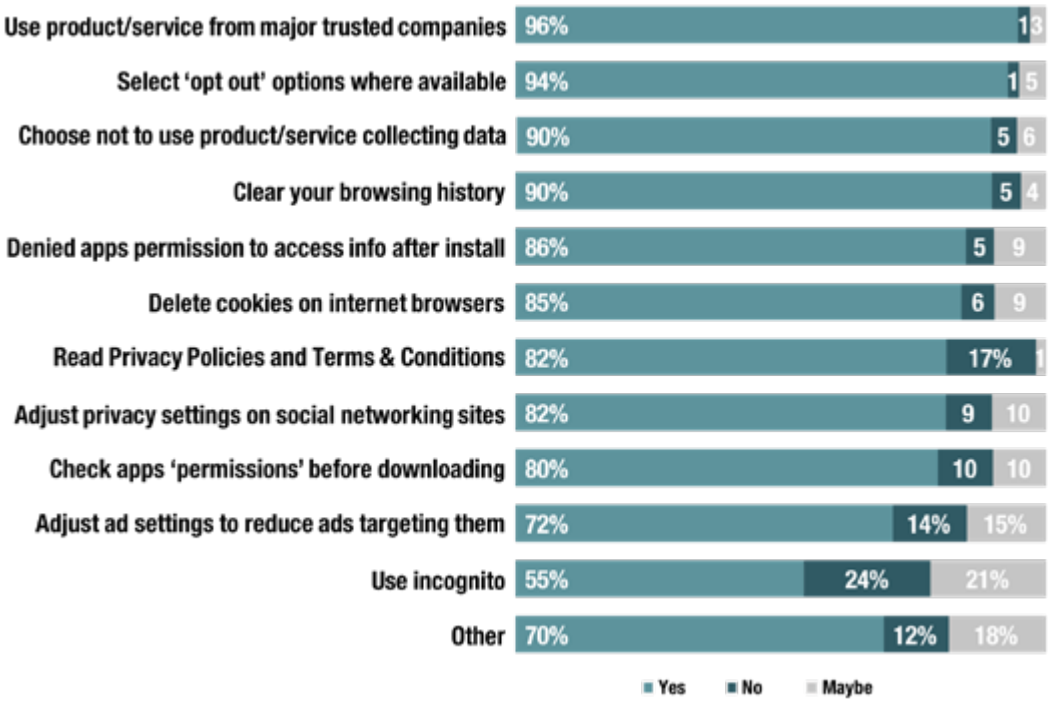

Figure 6. Strategies consumers have ever taken to protect their data. Question adapted from OAIC's survey (OAIC, 2017a). Where percentages add to 101%, this is due to rounding error; percentages are rounded to the nearest whole number. Categories 'always, often, sometimes and rarely' were collapsed as 'Yes' for ease of interpretation, refer to Appendix B for full detail.

Expectations of businesses and government

Survey results indicated that consumers want greater transparency and more control on how companies collect, use and share their data. 44% of respondents did not think it was enough for companies just to notify them about data collection, use and sharing in the Privacy Policy and Terms and Conditions.

The majority of survey respondents wanted companies to give them options to 'opt out' of certain types of data collection, use and sharing (95%), only collect data that is essential for the delivery of their service (91%), and to be open about how they use their data to assess their eligibility or exclude them from services or products (92%) (*see Figure 7*).

Focus group feedback further suggested that consumers want companies to provide more consent options that are easily accessible.

> "*If there was an option there with a box I could click saying 'I don't want my data to go any further', then I would use that. But because there is not that default, yes, I've given it to them—they own it.*

> "*If I see that box, I would always tick the box not to share, but that's when they are being honest and open and saying they want to share [your information]*

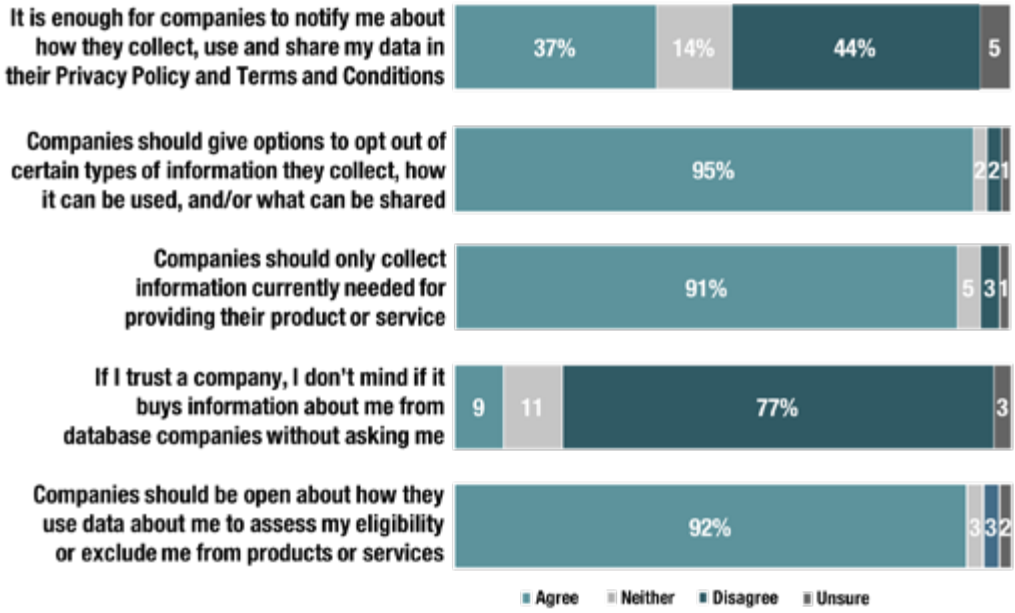

*Figure 7. Consumer expectations on how companies handle their data. *Question adapted from Turow et al (2005). Where percentages add to 101%, this is due to rounding error; percentages are rounded to the nearest whole number. Categories were collapsed for ease of interpretation, refer to Appendix B for full detail.*

Survey results also indicated that consumers expect the government to have a role in regulating companies by mandating companies give opt out options on how their data can be collected, used and shared (73%). Respondents also wanted the government to protect consumers so that they are not unfairly excluded from essential products or services based on their data (67%) (*see Figure 8*).

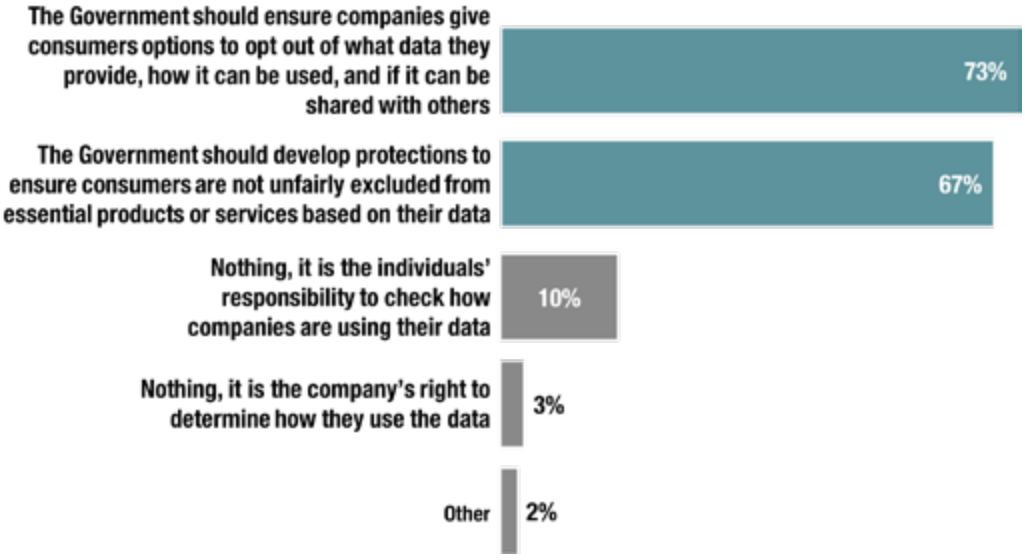

Figure 8. Consumer expectations of Government's role in data protection.

Focus group participants wanted legal protection that was supported by a strong

regulatory body and with penalties for misconduct.

> *If the government mandated for an 'opt out' button on each site…that'd be great…but then how are they going to monitor that?*

> *What would enforcement of that look like anyway?… Fine the company that's selling the data?*

> *They need to be a strong body to follow up on the laws. Make sure the policies are updated as well."*

Participants wanted greater ownership and control over their data and how it is shared.

> *It should be my data. I should have rights to it.*

> *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… .*

These findings highlight the current gap in public expectation when it comes to data collection, sharing and use practices in Australia and the current practice and regulatory framework. Policymakers, businesses and regulators developing systems, guidelines and principles for consumer data use and management should ensure consumer research and opinions are central to the design and implementation of relevant technologies and reforms if public confidence is to be retained and the benefits of innovation are to be delivered.

Policy implications

Building consumer trust and confidence to participate in the digital economy

The UK Competition & Markets Authority's (CMA) report into the commercial use of consumer data highlighted that consumers must be able to trust businesses in order to continue to provide data[5].

This trust is often based on the extent to which regulations and business practices are consistent with community expectations. As Roy Morgan Research has highlighted with their Net Trust Score rating, it is ultimately distrust which is driving significant community concern and consequently regulatory intervention across a range of markets[81].

The CMA report also suggests that consumer data can be used to support well-functioning markets if[5]:

1. *Consumers know when and how their data is being collected and used; and have some control over 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 are protected through the regulation of data collection and use.*
5. *There are effective ways to fairly manage non-compliance with regulation.*

Ensuring policy protections are in place to deliver these outcomes are central to ensuring collective benefits are derived from the opening up of consumer data and ensuing use practices. The next sections explore some of these concepts in more detail.

Consumers need to be provided with genuine choice & control over collection, sharing and use

For consumers to have greater confidence over the collection, management and use of their data they also need to comprehend from the outset what they are consenting to when releasing data to providers. As outlined in Chapter 7 it is clear that the current consent model is inadequate for modern-day technologies and practices.

How notice and consent systems are designed to deliver consumer comprehension of what they are agreeing to requires significant focus from policymakers. Additionally consumer and behavioural research which demonstrates the levels of comprehension are critical in the design of systems and regulations, cognisant of a broader shift in the regulatory community from solely looking at information disclosure requirements to comprehension testing of consumers[54].

Further research is much-needed on how best to provide meaningful notice and choice to consumers, to deliver greater control over their data. Some research has been done to look at what informed consent should look like for social media. Custers *et al.*, (2014) for example, developed a set of criteria for consent based on some existing EU legal provisions and the literature[41] (*see Table 2*).

Table 2. Set of Consent Criteria by Custers et al., (2014)

Criteria regarding the decision to consent		**Criteria regarding the person who consents**
	C1.1	Is the person who consents an adult? If not, is there parental consent?
	C1.2	Is the person who consents capable to consent? If not, is there a legal representative who consents?
	C.1.3	Is the person who consents competent to consent?
		Criteria on how to give consent
	C 2.1	Is the consent written? (Physical document or electronic format, possibly including check-boxes)
	C 2.2	Is the consent partial or full? In case of partial consent, does the consent cover the purpose?
	C 2.3	Is the consent reasonably strong?
	C 2.4	Is the consent an independent decision?
	C 2.5	Is the consent up to date?
Criteria regarding the well-consideredness of the decision to consent		**Criteria regarding what information should be provided**
	C 3.1	Is it clear which data are collected, used, and shared?
	C 3.2	Are the purposes clear?
	C 3.3	Is it clear which security measures are taken?
	C 3.4	Is it clear who is processing the data and who is accountable?
	C 3.5	Is it clear which rights can be exercised? Is it clear how these rights can be exercised?
		Criteria regarding how information should be provided
	C 4.1	Is the information provided specific and sufficiently detailed?
	C 4.2	Is the information provided understandable?
	C 4.3	Is the information provided reliable and accurate?
	C 4.4	Is the information provided accessible?

Custers *et al.* (2014) suggest that all criteria must be met to achieve consent on social media[41]. However, they observed that the interpretation and implementation of these criteria vary greatly in the literature and in practice. Therefore, their research was limited to assessing whether the criteria were mentioned in Privacy Policies, rather than assessing the extent to which Privacy Policies met these criteria.

For instance, *"a privacy policy mentioning that parental consent for minors is not required means that this criterion is addressed, but it also implies that this criterion is not fulfilled"*[41]. This means those policies checked against the list in their research study were considered to have covered legal perspectives but were not necessarily assessed for fairness or ethical perspectives.

More research is needed to explore how to obtain genuine consent and achieve fairer and more ethical outcomes for consumers. As a starting point, Australia can look to elements of the EU GDPR regime for provisions to improve consent[82], where consent must be:

- **Expressed** (the controller must be able to demonstrate that consent was given)
- **Specific** to purpose (unbundled with other matters)
- **Easy to understand** (written in clear and plain language)
- **Easily accessible**
- **Able to be withdrawn** (as easily as it is to give consent)
- **Freely given** (not conditional if the data is not necessary for the provision of the service)

The last point is important. Privacy expert Solove suggested that 'opt-in' consent is likely to fail if companies find ways to generate high opt-in rates by making it conditional to accessing products or services, and the consumer has no bargaining power or choice[45]. Another problem with the consent process is that it often implies perpetual consent[80]. Custers (2016) argue that rapid changes in Big Data and data analysis means that consent may get outdated and no longer reflect a user's preferences. Therefore, Custers recommend consent to be time limited and renewed after expiry dates to reflect user preferences over time[80].

A secondary way to provide greater control to consumers about what data is being collected, shared and used is to provide greater optionality of the differing types and uses of data. This could include requiring companies to specify categories of data use, such as 'data used only for the purpose of delivering the service', 'data shared or sold to third parties' or 'data used to assess eligibility or exclusion for products and services'. Of course, the nuances in the wording will still need to be tested. Enabling such options to be provided to consumers can provide greater transparency and also build understanding about what and how data is being used, while delivering some genuine choice over the end use.

An example of this is the US FTC's proposal to legislate how data brokers inform consumers and provide consumers with meaningful access to their data and 'opt out' options[37]. It also recommended that if a company used a data broker's product which adversely impacted a consumer's ability to complete a transaction or obtain a benefit, that the company be required to inform the consumer about which data broker supplied them with the information. The data broker should in turn provide the consumer access to the results generated by their product with explanations and description of how the results were developed to help consumers dispute or correct any misinformation[37].

While mandating 'opt out' provisions may be what consumers want, it might only provide a small degree of control for consumers if poorly designed. The FTC, for example, suggested that while some data brokers provided consumers with options to 'opt out' of their personal information being used for marketing purposes, it was not clear how consumers would learn about these rights and if consumers can 'opt out' of all uses of their data[37].

The FTC recommended legislative change to give consumers more meaningful access to their data and 'opt out' options[37], and a centralized internet portal where the largest group of data brokers could provide information about their data collection and use practices, and tools for opting out[37]. It also suggested that data brokers should give consumers notice if they derive inferences from their data and give consumers access to the categories which they have collected or inferred about them, including any sensitive data (e.g. information about a health condition)[37].

Furthermore, the FTC proposed that data brokers should clearly disclose the names and/or categories of their data sources, so there is greater transparency for consumers to

know about and correct original data sources. Likewise, companies that share consumer data with the data broker industry should clearly inform consumers about which data brokers they share the information with, provide them with links to the centralized website, and information on data access and 'opt out' rights[37].

The FTC states that while not all consumers may necessarily utilise these tools or understand the nuances of how their data is used, it will enable other stakeholders such as regulators, policy makers, academics, industry and consumer advocates to assess if data brokers are accurately informing consumers about their practices[37]. For consumers who wish to access these tools, the extent to which they are effective in providing consumers with better control over their data depend on its design. Systems could be better designed to make control options easily accessible and protect the consumer's privacy by default. In the next section we discuss Privacy by Design.

As a starting point, Australia can look to elements of the EU GDPR regime for provisions to improve consent, where consent must be: expressed, specific, easy to understand, easily accessible, able to be withdrawn, and freely given.

Ensuring consumers' right to privacy is adequately protected

As highlighted earlier in Chapter 7 Australians clearly value their privacy, with at least two thirds of the population surveyed thinking that it would be unacceptable for most types of their information to be shared with third parties for secondary purposes.

Balancing self-management

Professor Daniel Solove, a privacy legal expert has argued that relying on privacy self-management alone does not provide people with meaningful control over their data[45].

Solove presents several reasons for this. Firstly, social research has shown that there are *"cognitive problems that impair individuals' ability to make informed, rational choices about the cost and benefits of consenting, use, and disclosure of their personal data"*. Secondly, there are too many entities collecting and using personal data which can make it impractical for people to manage their privacy separately for each entity. Thirdly, it is not possible for people to accurately weigh the costs and benefits of providing their data or consent to the transfer of data because it is difficult to predict how their data could be aggregated over time to make privacy harms possible. Furthermore, many privacy notices are vague about future uses of the data collected[45].

Consumers are also not well informed about privacy; CPRC's research and international research show that people often do not read policies and terms, and some believe that they are protected from data sharing if there is a Privacy Policy[79]. Even those consumers who read policies often lack the expertise to make a judgment on the consequences of use or disclosure of their data[45].

Strategies to shorten Privacy Policies or make the policies easier to find have not been shown to significantly improve informed consent[43, 45]. Solove argues that privacy is a complex matter to understand and therefore there is 'a trade-off between providing a meaningful [privacy] notice and providing a short and simple one'[45]. Custers *et al.* (2014) argued that companies may feel inclined to have lengthy Privacy Policies to cover all legal aspects in case of dispute, rather than providing users with brief policies in everyday language[40].

More research and testing are needed to identify how best to improve consumer awareness and comprehension of their rights, as well as how their data is collected, used and shared, to improve informed consent.

Beyond the barriers of being able to understand policy documents, however, there is also the problem of being able to manage personal data with entities consumers know

about and those which have received information without consumers' knowledge[45].

Furthermore, an individual might provide one entity with a small amount of information that is considered 'non-sensitive' data without realising the implications to their privacy if 'non-sensitive' data from various entities are aggregated to reveal more identifiable and complete knowledge about the individual, so as to 'predict' behaviours and risks[45].

Solove argues that there is a tension between self-management and paternalism as approaches to privacy[45]. The paternalistic approach would provide individuals less power to consent by mandating privacy, so that it cannot be waived, and the law would override individual consent. Proponents of paternalistic approaches argue the problem with the self-management approach is that individuals do not necessarily make informed consent, and *"activities that would otherwise be illegitimate are made legitimate by consent"*[45]. Paternalistic approaches, however, would limit people's freedom to choose how and with whom they would like to share their data – some might want to share their data for social good or receive personally recommended products and services[45].

The challenge is finding the right balance in approaches for managing privacy. Solove suggests a number of ways to improve privacy[45]:

1. *Have a definition for valid consent. This needs to take into consideration the complexities of human decision-making and inequality in knowledge and power. Consent can be paired with paternalistic approaches such as nudges to change people's behaviour without removing their choices.*
2. *Develop mechanisms for 'partial privacy self-management', to make the process more manageable without the individuals having to be experts on privacy or be across the data collection, use or sharing for every entity separately. For example, developing a way for people to manage their privacy globally for all entities rather than having to micro-manage their privacy with one entity at a time.*
3. *Adjust time and focus in privacy law decisions, where the law can provide guidance about the types of uses at the time they are proposed (i.e. whether the uses should be restricted, be limited, require new consent, or allow the revocation of consent), rather than heavily focusing privacy laws at the time of initial collection when there is limited understanding of future privacy implication. Solove proposes an agency to review proposals for new uses.*
4. *The law to develop a code of basic privacy norms, where basic rules cannot be waived.*

Implementing Privacy by Design

Privacy by design is a proactive approach to protecting privacy during the design phase, and throughout the life-cycle of any project[83]. Under the GDPR it is now called data protection and design by default, and is a legal requirement[83].

Privacy by Design is not a new concept. It was developed in the 1990s by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian[84]. Commissioner Cavoukian reasoned that actually *"Privacy is good for business"*, and by responding to consumers' right to privacy, businesses can build consumer trust and confidence in their brand and have a competitive advantage over other companies[84]. Furthermore, Privacy by Design can reduce the likelihood of fines and penalties, and minimise compliance risks for businesses[83].

There are seven foundational principles of Privacy by Design[84]:

1. **Proactive not reactive; preventative not remedial**
   Be proactive rather than reactive, to anticipate and prevent privacy problems in advance.

2. **Privacy as the Default Setting**
   Personal data is automatically provided with the maximum degree of privacy protection in IT systems or business practices.

3. **Privacy Embedded into Design**
   Consider how to embed privacy in the design and architecture of IT systems and business practices rather than a treating privacy protection as a subsequent add-on feature

4. **Full functionality – Positive-sum, not Zero-Sum**
   Accommodate all legitimate interests and objectives in a win-win manner, where privacy and security can both be achieved without unnecessary trade-offs.

5. **End-to-End Security – Full Life-cycle Projection**
   Ensuring strong security measures prior to collecting the first element of information, as well as securely retaining data, and destroying data at the end of the process.

6. **Visibility and Transparency – Keep it Open**
   Businesses practices and technology involved should be subject to independent verification, to assure stakeholders they are operating according to stated promises and objectives.

7. **Respect for User Privacy – Keep it User-Centric**
   Take a user-centric approach by protecting the interest of individuals, for example: offering strong privacy defaults, appropriate notice, and user-friendly options.

These concepts may also help to tackle 'dark patterns' employed by businesses which make it difficult for consumers to manage their privacy. Dark patterns are interface design strategies used in websites or apps to steer consumers to behave in ways that may not be in their best interest[85,86]. For example, websites could be designed to make it onerous for users to locate where to opt out, or to become aware of the option to opt out, despite an option being made available[85]. Other examples of dark patterns include having intrusive privacy default settings, misleading wording, giving users false sense of control, hiding privacy-friendly choices and more[86]. Privacy by Design may help to combat this issue.

It has been argued that people gravitate to organisations that protect their personal information[84]. Therefore, businesses which can demonstrate that they respect their consumers' personal information by offering greater security and privacy protections will likely retain and gain new customers. Consumers also win by gaining better security and privacy protections.

Greater transparency of and access to data and profiles

Reforms underway in Australia to establish a Consumer Data Right aimed at providing consumers greater access to and portability of their own data are welcome, however, as highlighted earlier in this report, they apply only to certain types of data and where a consumer opts to have data transferred via the Consumer Data Right process.

The vast amount of consumer data currently being collected, transferred and used outside the establishment of the Consumer Data Right are not currently subject to the same protections. Thus significant economy-wide reform that takes into consideration the policy implications outlined in this chapter is critical to deliver greater confidence, access to, and transfer of consumer data.

For example, in the EU, the GDPR provides data subjects with greater rights to their data. The GDPR gives data subjects the rights to data access, data portability, object to certain uses, rectify incorrect information, and the right to erasure (to have their data deleted)[87].

Similarly, the risks of emerging profiling, pricing and exclusionary practices are significant. The design and application of algorithms and profiles, to determine the price or products for which consumers pay are marketed, eligible for or excluded from should be an emerging focus for policymakers.

As flagged earlier, the potential data and information asymmetry between buyers and sellers is increasing, and without knowledge of, or access to, the information or profile upon which organisations might be making decisions about product eligibility or pricing, consumers are not only unable to correct incorrect records, they are not able to change behaviour to increase their ability to acquire the product.

As flagged by Cathy O'Neil, Joy Boulamwini and Safiya Umoja Noble, there is also significant risk of assumptions being made that are simply incorrect, due to poor input data, or the data being inherently biased, opening the door to discrimination and exclusion.

The major concern raised by companies when asked to open up and make this transformed data or profiles public is the 'intellectual property' associated with the development of the profile and algorithms. This presents a major challenge for policymakers: without access to such information consumers have little to no ability to acquire insight into who companies think they are (rightly or wrongly). Similarly, regulators have little transparency or line of sight as to whether practices are exclusionary or discriminatory.

Assessment of algorithms for bias and discrimination is something that needs much greater policy consideration. Whether this is through a model such as that established by Cathy O'Neil with ORCAA[75], where algorithms can be submitted for auditing, or through a similar process undertaken by government regulators, such options should be explored as a matter of priority, especially where the impact of an incorrect decision could be significant for a consumer. This algorithm assessment could be an effective way to check that companies are complying with ethical standards on how they profile, offer or exclude consumers from products and services (particularly when it is considered an essential service or product).

As another example of opportunities for reform, recently the European Commission established a High-Level Expert Group on Artificial Intelligence; the 52 experts consist of representatives from academia, business and civil society to make recommendations and draft ethics guidelines to address fairness, safety, transparency, the future of work, fundamental rights, privacy and personal data protection, dignity, consumer protection and non-discrimination[88].

Strengthening regulatory monitoring and intervention powers

To maintain Australians' confidence in the government to protect them against data misuse, there needs to be better ways for regulators to detect and penalise companies who breach anti-discrimination, consumer protection, competition, and privacy laws.

Evolution of technology and machine-learning practices require a significant shift in capability, skills and monitoring powers within regulators in order to identify price discrimination or predatory lending behaviours, based on profiling practices. This will require investment in new skills, systems and people to keep pace with a fast-moving commercial environment.

Similarly, effective environment scanning and drawing on the latest research from the academic and research communities more regularly in policy development and consultation processes can strengthen the knowledge base and build greater shared-understanding of the challenges.

For example, CPRC this year established the Consumer Data Research Network with founding advisory members from QUT, UNSW, Western Sydney University, University of Melbourne, and 3A Institute to build a stronger community of Australian researchers working across multiple disciplines such as data ethics, consumer behaviour, privacy, computing science, competition & consumer law. As consumer data is an emerging field, providing space for interdisciplinary research and exploration of policy issues is critical. Through the Network, Australian researchers can have greater access to and knowledge of the policy development and regulatory processes to maximise the impact of their research. Greater collaboration across all sectors in this fast-moving field will help to develop more robust and sustainable regulatory and policy frameworks.

Lastly, Australia also could look at gaps in our existing laws to adapt and improve data rights for Australians. In addition to this, small businesses in the Privacy Act should also be included as liable data holders to ensure there is adequate protection in line with consumer expectations. The Australian government could also consider increasing penalties to disincentivise companies from being non-compliant. For example, companies who breach the GDPR would face penalties of up to 4% of annual turnover or €20 million (whichever is greater)[89].

To maintain Australians' confidence in the government to protect them against data misuse, there needs to be better ways for regulators to detect and penalise companies who breach anti-discrimination, consumer protection, competition, and privacy laws.

Conclusion

With increasing digital transformation and business dependency on consumer data, companies need to demonstrate that they are operating fairly and in the interest of their customers, lest they risk a backlash where consumers may withhold or provide inaccurate information in the future[90].

Providing consumers with greater transparency when it comes to how their data is being used can help to facilitate trust and make the market more fair and equitable.

Our research finds that improving transparency and the rights of consumers can be enabled by:

- Providing consumers with genuine options over what data is collected, shared and used
- Delivering greater transparency to enable consent, using elements of the GDPR as a starting point
- Making privacy management easier for consumers – for example, by designing a single portal for consumers to monitor data flows between third parties
- Implementing Privacy by Design in business IT systems or practices
- Reviewing potential gaps in current law and regulation to ensure basic data rights and protections are adequate, and reflect changing technologies
- Investing in regulatory bodies to audit unlawful discriminatory practices, and
- Increasing penalties to disincentivise companies from non-compliance.

Big Data has enabled rapid innovation in the digital economy which can bring benefits to both businesses and consumers. Consumer data is undoubtedly a rich resource for innovation. Responsible business practices and regulation centred around good consumer outcomes can work towards enshrining trust and enabling ongoing data sharing for continued innovation and economy-wide benefit.

References

1. Statista. (2018a). Active internet users as percentage of the total population in Australia from 2015 to 2017. Statista. Available at https://www.statista.com/statistics/680142/australia-internet-penetration/ (Accessed on 24 January 2018)

2. Statista. (2018b). Number of social network users in Australia from 2015 to 2022 (in millions). Statista. Available at https://www.statista.com/statistics/247946/number-of-social-network-users-in-australia/ (Accessed on 24 January 2018)

3. Office of the Australian Information Commissioner (OAIC). (2017a). 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

4. Science Daily. (2013). Big Data, for better or worse: 90% of world's data generated over last two years. Science Daily. Available at https://www.sciencedaily.com/releases/2013/05/130522085217.htm (Accessed on 17 April 2018)

5. 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

6. Gartner IT. (2018). IT Glossary: Big Data. Available at https://www.gartner.com/it-glossary/big-data (Accessed on 19 January 2018)

7. Lagoze, C. Big Data, data integrity, and the fracturing of the control zone. Big Data & Society. 2014; 1(2):1-11

8. Columbus, L. (2018). 10 Charts that will change your perspective of Big Data's Growth. Forbes. Available at https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#41666c329268 (Accessed 30 May 2018)

9. Accenture. (2014). Big Success with Big Data. Accenture. Retrieved from: https://www.accenture.com/t00010101T000000Z__w__/mx-es/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_7/Accenture-Big-Data-POV.ashxla=es-LA

10. Australian Communications and Media Authority (ACMA). (2013). Privacy and personal data: emerging issues in media and communications. Occasional paper 4. Australian Communications and Media Authority. Retrieved from https://www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/privacy-and-digital-data-emerging-issues

11. Research Australia. (2017). Australia Speaks! Research Australia Opinion Polling 2017. Available at https://researchaustralia.org/reports/public-opinion-polling-2017/ (Accessed on 15 January 2018).

12. Centre for Internet Safety (CIS). (2013). Privacy and the Internet: Australian attitudes towards Privacy in the online environment. Centre for Internet Safety. Available at http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf

13. Goggin, G., Vromen, A., Weatherall, K., Martin, F., Webb, A., Sunman, L., Bailo, F. (2017). Digital Rights in Australia. The University of Sydney. Retrieved from https://ses.library.usyd.edu.au/bitstream/2123/17587/7/USYDDigitalRightsAustraliareport.pdf

14. Productivity Commission. (2017). Data Availability and Use, Report No. 82. Productivity Commission, Canberra, Australia. Retrieved from https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

15. The Treasury. (2018). Consumer Data Right. Australian Government. The Treasury. Available at https://treasury.gov.au/consumer-data-right/ (Accessed 28 May 2018)

16. The Treasury. (2017). Review into Open Banking: giving customers choice, convenience and confidence. Australian Government. The Treasury. Retrieved from https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

17. Office of the Australian Information Commissioner (OAIC). (2018). Privacy Act. Office of the Australian Information Commissioner. Available at https://www.oaic.gov.au/privacy-law/privacy-act/ (Accessed on 12 April 2018)

18. Office of the Australian Information Commissioner (OAIC). (2017b). What is personal information. Office of the Australian Information Commissioner. Available at https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information (Accessed on 12 April 2018)

19. Johnston, A. (2017). Mobiles, metadata and the meaning of 'personal information'. Salinger Privacy. Available at https://www.salingerprivacy.com.au/2017/01/19/federalcourtdecision/ (Accessed 25 May 2018).

20. Intersoft consulting. (n.d.a). Art. 4 GDPR Definitions. Intersoft consulting. Available at https://gdpr-info.eu/art-4-gdpr/ (Accessed 6 April 2018).

21. Edwards, L. Data Protection: Enter the General Data Protection Regulation (May 21, 2018). To appear in L Edwards ed Law, Policy and the Internet (Hart Publishing, 2018). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182454

22. The Australian Small Business and Family Enterprise Ombudsman. (2016). Small Business Counts. Small Business in the Australian Economy. The Australian Small Business and Family Enterprise Ombudsman. Retrieved from https://www.asbfeo.gov.au/sites/default/files/Small_Business_Statistical_Report-Final.pdf

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

24. Google. (2018a). Google Privacy Policy. Google. Available at https://policies.google.com/privacy?hl=en&gl=au (Accessed 20 June 2018).

25. Google. (2018b) Personal Information. Google. Available at https://policies.google.com/privacy?hl=en&gl=au#footnote-personal-info (Accessed 20 June 2018).

26. Facebook. (2018). Facebook Data Policy. Facebook. Available at https://www.facebook.com/about/privacy/update (Accessed 23 April 2018)

27. Su, J., Shukla, A., Goel, S., Narayanan, A. De-anonymizing web browsing data with social networks. Proceedings of the 26th International Conference on World Wide Web. 2017. Pages 1261-1269

28. De Montjoye, Y., Hidalgo, C.A., Verleysen, M., Blondel, V.D. Unique in the crowd: the privacy bounds of human mobility. Nature. 2013; Scientific Reports 3, Article number 1376

29. Information Commissioner's Office (ICO, 2012). Anonymisation: managing data protection risk code of practice. Information Commissioner's Office. Available at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf (Accessed 9 May 2018)

30. Elliot, M., Mackey, E., O'Hara, K., Tudor, C. (2016). The Anonymisation Decision-Making Framework. UKAN. Retrieved from http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf

31. O'Keefe, C.M., Otorepec, S., Elliot, M., Mackey, E., O'Hara, K. (2017). The De-identification Decision-Making Framework. CSIRO Reports EP173122 and EP175702. Retrieved from https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS2

32. Christl, W. and Spiekermann, S. (2016). Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Vienna, Austria: Facultas Verlags- und Buchhandels AG

33. Maheshwari, S. (2017). That game on your phone may be tracking what you're watching on TV. The New York Times. Available at https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html (Accessed on 19 Jan 2018)

34. Australian Communications and Media Authority (ACMA). (2016). Data driven marketing practices: Australian industry participants survey results December 2016. Australian Communications and Media Authority, Melbourne, Australia. Retrieved from https://www.acma.gov.au/theACMA/data-driven-marketing-practices

35. Citi GPS. (2017). ePrivacy and Data Protection. Who watches the watchers? How regulation could alter the path of innovation. Citi GPS: Global Perspectives & Solutions. Retrieved from https://www.citibank.com/commercialbank/insights/assets/docs/ePrivacyandData.pdf

36. Woolworths Rewards. (2018). Woolworths Rewards Privacy. Woolworths Rewards (Updated January 2018). Available at https://www.woolworthsrewards.com.au/privacy.html (Accessed 13 February 2018)

37. Federal Trade Commission. (2014). Data Brokers. A Call for Transparency and Accountability. Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

38. Congress. (2018). All Information (Except Text) for S.1815- Data Broker Accountability and Transparency Act of 2017. Available https://www.congress.gov/bill/115th-congress/senate-bill/1815/all-info (Accessed 23 May 2018)

39. Experian. (2018). Introducing Consumer view now. Experian's data appending services for small businesses- now even better. Experian. Available at http://www.experian.com/small-business/data-appending-services.jsp (Accessed 17 April 2018)

40. Davis, K. (2016). Big Data Agents. Core Logic. Available at https://www.corelogic.com.au/news/big-data-agents#.WtWObH8RW72 (Accessed 17 April 2018)

41. Custers, B., van der Hof, S., Schermer, B. Privacy expectations of social media users: the role of informed consent in privacy policies. Policy & Internet. 2014; 6(13): 268-295

42. Kemp, K. and Vaile, D. (2018). Soft terms like 'open' and 'sharing' don't' tell the true story of your data. The Conversation. Available at https://theconversation.com/soft-terms-like-open-and-sharing-dont-tell-the-true-story-of-your-data-95521 (Accessed 1 May 2018)

43. 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

44. 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

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

46. 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 January 2018)

47. McDonald, A.M. and Cranor, L.F. The cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society. 2008; Privacy Year in Review, 4(3). Available at http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf

48. Jackson, J. (2014). IBM detects skin cancer more quickly with visual machine learning. Computer World. Available at https://www.computerworld.com/article/2860758/ibm-detects-skin-cancer-more-quickly-with-visual-machine-learning.html (Accessed 31 May 2018)

49. The Institute. (2017). Three Life-changing innovations for people with disabilities. The Institute. The IEEE news source. Available at http://theinstitute.ieee.org/technology-topics/consumer-electronics/three-lifechanging-innovations-for-people-with-disabilities (Accessed 30 May 2017)

50. The Working Group on Disability and Digital Societies. (2016). How can digital information contribute to achieving the SDGs for persons with disabilities? 9th Conference of States Parties to the UN Convention on the Rights of Persons with Disabilities. Retrieved from http://www.un.org/disabilities/documents/desa/digital_society_white_paper.pdf

51. Australian Payments Network. (2017). Australian Payments Fraud 2017. Jan-Dec 2016 Data. Australian Payments Network. Retrieved from https://www.auspaynet.com.au/sites/default/files/2018-01/australian_payments_fraud_details_and_data_2017.pdf

52. ABS. (2018). 8146.0- Household use of information technology, Australia, 2016-2017. Australian Bureau of Statistics. Available at http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0 (Accessed 20 June 2018)

53. OPI. (2018). Using Open Data to deliver Public Services. Open Data Institute. Retrieved from: https://www.scribd.com/document/372783776/Using-Open-Data-to-Deliver-Public-Services-report#from_embed

54. Solomon, L. and Martin-Hobbs, B. (2018). Five preconditions of effective consumer engagement- a conceptual framework. Product information, consumer choice and market engagement. Consumer Policy Research Centre. Retrieved from http://cprc.org.au/research-areas/making-consumer-decisions-easier-and-fairer/report-release-five-preconditions-effective-consumer-engagement/

55. Victorian Energy Compare. (2018). Welcome to Victorian Energy Compare. Victorian Energy Compare, Victoria State Government. Available at https://compare.switchon.vic.gov.au/ (Accessed 30 May 2018).

56. Algorithmic Justice League. (2017). Algorithmic Justice League. Available at https://www.ajlunited.org/ (Accessed 30 May 2018)

57. KPMG. (2016). Creepy or cool: staying on the right side of the consumer privacy line. KPMG International. Retrieved from https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/creepy-or-cool.pdf

58. ASIC. (2013). Responsible lending. Australian Securities & Investments Commission. Available at https://asic.gov.au/regulatory-resources/credit/responsible-lending/ (Accessed 20 June 2018)

59. Borgesius, FZ., Poort, J. Online Price Discrimination and EU Data Privacy Law. Journal of Consumer Policy. 2017, 40(3): 347-366.

60. Plunkett, J. (2017). The future of shopping: pricing gets personal. Prospect: The leading magazine of ideas. Available at https://www.prospectmagazine.co.uk/magazine/the-future-of-shopping-pricing-gets-personal (Accessed on 18 January 2018).

61. Mikians, J., Gyarmati, L., Erramilli, V., Loaoutaris, N. (2012). Detecting price and search discrimination on the Internet. Universitat Politecnica De Catalunya. Available at http://upcommons.upc.edu/handle/2117/19247 (Accessed on 31 January 2018).

62. Mattioli, D. (2012). On Orbitz, Mac Users Steered to Pricier Hotels. Wall Street Journal. Available at https://www.wsj.com/articles/SB10001424052702304458604577488822667325882 (Accessed on 31 January 2018)

63. Merler, S. (2017). Big data and first-degree price discrimination. Bruegel. Available at http://bruegel.org/2017/02/big-data-and-first-degree-price-discrimination/ (Accessed on 31 January 2018)

64. Fiegerman, S. (2018) Facebook sued for allegedly allowing housing discrimination. Money CNN. Available at http://money.cnn.com/2018/03/27/technology/facebook-housing-lawsuit/index.html (Accessed 9 April 2018)

65. PacerMonitor. (2018). National Fair Housing Alliance et al v. Facebook, Inc. PacerMonitor. Available at https://www.pacermonitor.com/public/case/24045944/National_Fair_Housing_Alliance_et_al_v_Facebook,_Inc (Accessed 20 June 2018)

66. Lobosco, K. (2013). Facebook friends could change your credit score. CNN tech. Available at http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html (Accessed on 31 January 2018)

67. Matsakis, L. (2018). Your smartphone choice could determine if you'll get a loan. Wired. Available at https://www.wired.com/story/your-smartphone-could-decide-whether-youll-get-a-loan/ (Accessed 11 May 2018)

68. Choice. (2016). Public Inquiry: Data Availability and Use-Draft report: Post-draft submission No.DR328. Available at https://www.pc.gov.au/__data/assets/pdf_file/0018/212364/subdr328-data-access.pdf

69. Haldane, A.G. (2018). Will Big Data Keep its Promise? Bank of England. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/will-big-data-keep-its-promise-speech-by-andy-haldane.pdf

70. Karp, P. (2018). Facial matching system is racist, Human Rights Law Centre warns. The Guardian. Available at https://www.theguardian.com/technology/2018/may/30/facial-matching-system-is-racist-human-rights-law-centre-warns (Accessed 30 May 2018)

71. O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. USA, New York: Crown Random House.

72. TED. (2017). Cathy O'Neil: The era of blind faith in Bi Data must end. TED. Available at https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end#t-634526 (Accessed 30 May 2018)

73. Priceonomics. (2017). The Data Science Diversity Gap. Forbes. Available at https://www.forbes.com/sites/priceonomics/2017/09/28/the-data-science-diversity-gap/#1929de1b5f58 (Accessed 30 May 2018)

74. Hoogendoorn, S., Oosterbeek, H., van Praag, M. The Impact of Gender Diversity on the Performance of Business Teams: Evidence from a Field Experiment. Management Science. 2013; 59(7): 1514-1528

75. ORCCA. (n.d.). O'Neil Risk Consulting & Algorithmic Auditing. ORCAA. Available at http://www.oneilrisk.com/ (Accessed 30 May 2018)

76. IEEI. (2018). Information Ethics & Equity Institute. IEEI. Available at https://ethicsequity.org/ (Accessed 30 May 2018)

77. Gutermuth, L. (2017). How to understand what info mobile apps are collecting about you: it takes a little work, but it's worth it. Slate. Available at http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile_apps_collect_about_you.html (Accessed on 24 January 2018)

78. Forbrukerradet. (2018a). #appfail. Forbrukerradet. Available at https://www.forbrukerradet.no/appfail-en/# (Accessed 21 June 2018)

79. Turow, J., Feldman, L., Meltzer, K. (2005). Open to Exploitation: America's Shopper Online and Offline. Annenberg Public Policy Center of the University of Pennsylvania. Retrieved from http://repository.upenn.edu/asc_papers/35

80. Custers, B. Click here to consent forever: Expiry dates for informed consent. Big Data & Society. 2016; 3(1): 1-6

81. Roy Morgan, (2018). Roy Morgan Net Trust Score (NTS). Roy Morgan. Available at http://www.roymorgan.com/findings/7521-roy-morgan-net-trust-score-nts-201802270643 (Accessed 21 June 2018)

82. Intersoft consulting. (n.d.b). Art. 7 Conditions for Consent. Intersoft consulting. Available at https://gdpr-info.eu/art-7-gdpr/ (Accessed 17 April 2018).

83. Information Commissioner's Office (ICO). (2018). Data Protection by design and by default. Information Commissioner's Office Available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed 6 July 2018).

84. Information and Privacy Commissioner of Ontario (IPC). (2013). Privacy by design. Information and Privacy Commissioner of Ontario. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf (Accessed 8 May 2018).

85. Dark Patterns. (n.d.). What are Dark Patterns? Dark Patterns. Available at https://darkpatterns.org/ (Accessed 30 May 2018)

86. Forbrukerradet. (2018b). Deceived by Design. Forbrukerradet. Retrieved from https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

87. Intersoft consulting. (n.d.b). Rights of the data subject. Intersoft consulting. Available at https://gdpr-info.eu/chapter-3/ (Accessed 1 June 2018)

88. European Commission. (2018). Commission appoints expert group on AI and launces the European AI Alliance. European Commission. Available at https://ec.europa.eu/digital-single-market/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance (Accessed 29 June 2018)

89. EU GDPR. (n.d.). GDPR Key Changes. EU GDPR. Available at https://www.eugdpr.org/key-changes.html (Accessed 17 April 2018)

90. Kemp, K. (2018) The need for boundaries: respecting privacy in financial consumer data practices. Dvara Research. Available at https://www.dvara.com/blog/2018/03/09/the-need-for-boundaries-respecting-privacy-in-financial-consumer-data-practices/ (Accessed 1 May 2018

Appendices

Appendix A:
Research methodology

In February 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 methodology outline provided by Roy Morgan Research for this study is included in this section.

Roy Morgan conducted an online survey and two focus groups with Australian consumers.

Focus groups

The overall objectives of the focus groups were to determine:

- The individual's awareness of and sensitivity towards different type of information collection (both type of information and collection methods);
- The individual's awareness of how data is used; and
- Perceived risks around data usage and methods of risk mitigation.

Participants were recruited from Roy Morgan Research's consumer panel. We aimed for an even mix of male and female respondents.

Selection criteria:

- Participants lived within 30kms of the Melbourne CBD; and
- They had previous accessed or signed up to a product or service that collected data.

For each focus group, 10 people were recruited, with the expectation that some participants would not be able to attend. Two focus groups were conducted in Melbourne on February 15, 2018, with the group breakdowns, as follows:

- Group 1: Men and women age 45+ years (8 respondents attended)
- Group 2: Men and women age 18-45 years (7 respondents attended)

Each focus group was an hour long, with groups beginning at either 5:30pm or 7:30pm. A discussion guide was prepared by the Roy Morgan project team in collaboration with CPRC. A $100 incentive was paid to participants after completing the session, and sessions were viewed by CPRC staff and audio recorded with participant consent.

Survey

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 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.

The online survey was conducted from 27 February to 6 March 2018. Sample for the survey was sourced through Roy Morgan Research's online consumer panel.

Selection criteria:

- Participants lived in Australia, and
- They were aged 18 years or older.

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

The questionnaire consisted of 16 questions. The average time taken to complete the questionnaire was 9 minutes.

As an incentive, participants were eligible to enter in Roy Morgan's monthly cash prize draw.

Appendix B:
Weighted summary tables of survey results

Table 1: Demographics of survey participants

Gender	**(%)**
Male	48.7
Female	51.3

Age (years)	**(%)**
18-24	12.1
25-34	19.1
35-49	25.5
50-64	23.0
>=65	20.3

State*	**(%)**
ACT	3.4
NSW	30.6
VIC	26.3
QLD	19.9
SA	7.2
NT	0.5
TAS	1.8
WA	10.1

*Derived from postcodes

Region*	(%)
Metro	65.9
Regional	34.1

*Derived from postcodes

What is the highest level of education you have completed?	(%)
Primary school or lower	0.3
Secondary school	18.7
Technical or further education	30.4
Undergraduate university degree	32.5
Post graduate university degree	17.7
Other	0.3

Approximately how much income do you usually receive in a year (includes wages and government payments)?	(%)
≤$19,999	13.4
$20,000-$49,999	28.4
$50,000-$79,999	21.5
$80,000-$109,000	13.7
≥$110,000	10.6
Can't say	2.5
Prefer not to say	10.0

Table 2. Language and self-assessed level of English spoken

Speak language other than English at home?	(%)
Yes	14.6
No	85.4

How well do you speak English?	(%)
Well	6.4
Very well	93.6

Table 3. Use of social media, loyalty rewards, online shopping, apps & mobile payment technology

In 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 (%)
Facebook	18.7	5.8	4.8	12.4	58.3
Google products and services (including Google search engine, Gmail, Google maps, etc.)	1.2	2.2	3.0	20.5	73.0
Flybuys or Everyday Rewards supermarket loyalty card	22.2	7.1	12.8	50.7	7.2
Online shopping websites	11.2	32.1	35.0	17.4	4.3
Apps on a mobile phone or tablet	11.3	5.2	5.1	13.3	65.1
Tap and Pay with your phone	72.1	5.5	3.9	10.2	8.2

Table 4. Behaviour relating to Privacy Policies or Terms and Conditions among survey participants

In the past 12 months, how often did you read a Privacy Policy or Terms & Conditions when signing up for a product or service?	(%)
Never	33.2
For only a few	35.5
For some	13.6
For most	11.6
For all	6.1

Of those who did read (67%):

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?	(%)
Never	32.9
For only a few	25.3
For some	14.0
For most	13.2
For all	14.7

Of those who did answered for only a few, for some, for most and for all in the previous question:

Why did you 'accept' the Privacy Policy or Terms and conditions even though you did not feel comfortable with the policies) (tick all that apply)	(%)
It was the only way to access the product or service	73.2
I trust that the company would not misuse my data	23.2
I believe that the law would prevent the company from misusing my data	19.5
Nothing bad has happened to me in the past	17.7
Other, please specify	1.1

Table 5. Knowledge of data collection, use and sharing among survey participants

Choose True, False or Don't Know for the following statements as best reflects your opinion	True (%)	False (%)	Don't know (%)	Correct answer
Companies today have the ability to follow my activities across many sites on the web*	90.5	2.1	7.4	True
When a company has a privacy policy, it means the site will not share my information with other websites or companies*	18.6	59.2	22.2	False
In store shopping loyalty card providers like Flybuys and Everyday Rewards have the ability to collect and combine information about me from third parties	73.0	4.1	22.9	True
Some companies exchange information about their customers with third parties for purposes other than delivering the product or service the customer signed up for	88.3	2.1	9.6	True
All mobile/tablet apps only ask for permission to access thing on my device that are required for the app to work	25.7	47.3	26.9	False

*Questions borrowed from Turow et al. (2005)

Table 6. Data/information survey respondents did not feel comfortable sharing with third parties

What data/information would you be uncomfortable with companies sharing with third parties for purposes other than delivering the product or service? (tick all that apply)	(%)
Phone contacts	86.6
Your messages	85.7
The unique ID number on your device	83.7
Phone number	79.5
Date of birth	72.6
Browsing history	71.9
Who you are friends with on your SNS	71.2
Location data	70.7
Purchase/transaction history	68.8
Email address	67.3
Name	60.9
Other, please specify	5.1

Table 7. Measures taken to protect data/information by survey participants

In order to protect your data/information, how often do you…	Always (%)	Often (%)	Some times (%)	Rarely (%)	Never (%)	I don't know how (%)
Use products or services provided by major companies you trust?	18.3	51.4	22.0	3.8	1.6	2.9
Use incognito	4.5	14.1	21.2	15.0	24.0	21.1
Read Privacy Policies and Terms & Conditions documents?	6.3	16.7	33.3	25.6	16.8	1.3
Not to use the product or service collecting your data/information?	8.8	25.1	42.2	13.9	4.6	5.5
Adjust privacy settings on social networking sites?	24.3	21.7	22.6	13	8.5	9.9
Adjust ad settings on your online accounts to reduce ads targeted at you?	15.8	18.5	23.2	14.1	13.8	14.6
Check your mobile/tablet apps 'permissions' before downloading the app to see what you are giving it access to on your device?	21.3	20.6	23.5	14.9	10.1	9.7
Deny apps permission to access information from your mobile after installing and opening the app?	18.2	34.0	27.1	6.4	5.0	9.3
Delete cookies on internet browsers?	11.3	25.2	29.3	18.7	6.2	9.3
Clear your browsing history?	13.9	26.0	29.6	20.8	5.4	4.3
Select 'opt out' options where available, denying companies permission to share your data with third parties?	32.6	32.8	23.4	5.2	1.3	4.6
Other	29.3	18.2	20.6	1.7	12.1	18.1

Table 8. Survey participants acceptability of how companies use their data

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 (%)
Monitoring your online behaviour to show you relevant advertising and offers	2.4	24.6	19.8	22.8	29.2	1.2
Charging people different prices for the same products in the same hour, based on their past purchasing, online browsing history, or payment behaviour *	2.2	3.6	4.6	11.2	76.9	1.5
Collecting data about you without your knowledge to assess your eligibility or exclude you from a loan or insurance	2.1	3.1	6.6	11	75.7	1.3
Collecting data about your payment behaviour to assess your eligibility or exclude you from essential products and services (e.g. electricity, gas, telecommunications)	2.0	6.0	8.8	14.2	67.5	1.4

*Adapted from Turow et al., 2005

Table 9. Survey participants opinion on how companies should handle their data

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 (%)
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	6.1	31.1	13.7	29.5	14.8	4.7
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	64.4	30.6	1.8	0.7	1.2	1.2
Companies should only collect information currently needed for providing their product or service	55.3	36.1	4.6	1.7	1.1	1.1
If I trust a company, I don't mind if it buys information about me from database companies without asking me *	1.7	7.0	11.3	33.6	43.8	2.7
Companies should be open about how they use data about me to assess my eligibility or exclude me from products or services	63.7	28.5	2.7	1.3	2.2	1.6

*Adapted from Turow et al., 2005

Table 10. Survey participants expectations of government

What role do you think government has in regulating how companies are use your data?	(%)
Nothing, it is the individuals' responsibility to check how companies are using their data	9.8
Nothing, it is the company's right to determine how they use the data	3.4
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	72.6
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	66.7
Other	1.5

Level 14, 10-16
Queen Street

Melbourne
Victoria 3000

T 03 9639 7600
F 03 9639 8966

cprc.org.au
ACN 100 188 752

Consumer
Policy Research
Centre