Australian Government

Office of the Australian Information Commissioner

Australian Community Attitudes to Privacy Survey 2020

Prepared for the Office of the Australian Information Commissioner
by Lonergan Research

September 2020

OAIC

Report prepared by

LONERGAN.

Document Retrieval Information:

Publication date September 2020

No of Pages: 121

ISBN: 978-1-877079-74-0

Publication Title: Australian Community Attitudes to Privacy Survey 2020

Office of the Australian Information Commissioner
Website: www.oaic.gov.au
Access our online enquiry form on our website for any general enquiry
Telephone: 1300 363 992

Lonergan
Website: www.lonergan.team
Email: chris@lonergan.team
Telephone: +61 2 9046 5600

If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au.

This study was conducted in compliance with quality and data privacy standards and legislation including ISO 20252, Privacy Act 1988 (Cth), The (Market and Social Research) Privacy Code 2014 and the AMSRS Code of Professional Behaviour.

Contents

Commissioner's foreword 4

Executive summary 6

Introduction and background 10

Methodology 11

Part 1: Introduction to privacy 14

- What 'privacy' means to Australians 14
- The importance of privacy 17
- Incidence of negative privacy experiences 20
- Incidence of data-driven advertising 23
- Perceived privacy risks 26
- Levels of comfort with data practices 27
- General acceptance of data practices 31
- Levels of comfort by purpose and organisation 32
- What Australians consider a misuse of personal information 36
- Sending data overseas 39
- Likelihood to take action to protect one's privacy 41
- Australians' levels of knowledge about privacy 43
- Actions Australians are taking to protect their privacy 45
- Levels of control over privacy 51
- Trust in organisations 55

Part 2: Privacy legislation 57

- Awareness of the Privacy Act 57
- Awareness of organisation types covered by the Privacy Act 58
- Organisations that should be covered by the Privacy Act 60
- Awareness of the Privacy Commissioner 61
- Entity to whom Australians would report a misuse of privacy 62
- Degree to which Australians feel their privacy is protected 64
- Demand for greater government protection 65
- Additional rights under the Privacy Act 67
- Vulnerable groups and the Privacy Act 68
- Privacy policies 69

Part 3: Location data 78

Comfort with the use of location data 79
Protection of location data 80

Part 4: Biometric information 81

Comfort with providing different types of biometric information 82
Trust in private and public sector organisations to collect biometric information 83
Comfort with providing biometric information for different purposes 83
Protection of biometric data 85

Part 5: Artificial intelligence 86

General attitudes towards AI 86
Right to know if AI is being used 87
Right to human oversight 88
Impact of organisation types on trust in AI 89

Part 6: Children's privacy 90

Children's access to and ownership of devices 92
Use of online accounts and services by children 93
Attitudes to children's privacy 94
Measures implemented by parents to protect their child's privacy 95
Measures to increase children's data privacy online 96
Perceptions of control over children's privacy 97
Reasons for not doing more to protect their child's privacy 99
The ideal age for children to take responsibility for their own privacy 100

Part 7: Attitudes to privacy in the context of the COVID-19 outbreak 102

Concerns over privacy in a COVID-19 environment 103
Perception of privacy risks 105
Change in behaviour in Australian households 107
Attitudes to protection of personal information while at home 108
Privacy concessions during the COVID-19 outbreak 110
Implications for trust in organisations 113
Attitudes to digital services during the COVID-19 outbreak 116

Figures and charts 118

Commissioner's foreword

In 2020, privacy is a major concern for 70% of Australians, and almost 9 in 10 want more choice and control over their personal information.

These are among the key findings of our Australian Community Attitudes to Privacy Survey (ACAPS), which for the first time in its 30-year history has been conducted entirely online.

It also measures the impact of the COVID-19 outbreak on our views towards privacy and provides critical insights into our nation's beliefs and concerns at a unique point in time.

The survey reveals data privacy is now our top consideration when we are choosing a digital service — ahead of reliability, convenience and price. In an ever-evolving digital environment, the actions we take to maintain our privacy are changing, while our trust in organisations to protect our personal information continues to decline.

Our concern about privacy is driven by experience. More than half of us experienced a problem with how our data was used during the 12 months leading up to the survey, such as unwanted marketing communications, or personal information being collected when it was not required.

Compared to 2017, when the survey was last conducted, Australians are more likely to view identity theft and fraud as the biggest risks to privacy, along with data security and data breaches.

We also have strong views on misuse of our information. This includes being asked for information that doesn't seem relevant or having information about the websites we visit recorded without our knowledge. In response, we are more likely to take certain actions to protect our privacy than in 2017 — such as deleting an app, denying permission to access our information, or clearing our browser history.

Our comfort with certain data practices depends on the type of information collected, the purpose behind it, and the level of trust in the organisation involved. Australians appear more comfortable with data practices where the purpose is clearly understood – for example, law enforcement using facial recognition and video surveillance to identify suspects.

But we are concerned about businesses tracking our location through mobiles or web browsers (62%) and are generally reluctant to provide biometric information (66%). Commercial profiling activities drive higher levels of discomfort than government data practices.

This is an area of focus for regulators, including the OAIC, which is working towards a new privacy code for social media and online platforms. The binding code will improve Australians' ability to manage privacy choices through transparent policies and better practices around consent, and will strengthen protections for children and other groups with particular needs.

As the survey shows, most Australian parents strongly support more restrictions on business and devices to protect the data privacy of children online. They want their children to be empowered to use the internet and online services, but their data privacy to be protected in the digital environment.

The COVID-19 pandemic has also influenced our views about privacy. While half of all Australians think privacy is more at risk generally during the pandemic, the majority are comfortable with personal information being shared to combat COVID-19 and expect it to be protected.

Across the board, there is a strong understanding of why we should protect personal information (85% agree) but Australians are less sure how they can do this (49% agree). The main reasons for not doing more to safeguard privacy are lack of knowledge, lack of time and the difficulty of the process.

While my office provides a range of resources on simple steps people can take to protect their privacy, there are strong signals here for regulated entities on how to build consumer trust and confidence.

Business use of personal information should be contextual and related to purpose. In response to perceived privacy risks, regulated entities need to strengthen measures to prevent data breaches, such as investing in systems and staff training. Making it easier for Australians to have more control and choice over the collection and use of their personal information will also differentiate a business from its competitors.

Australians are more likely to trust a website or service if they have read the privacy policy. However, only 20% read privacy policies and are confident they understand them. We want privacy policies that are easier to understand, and feature standard, simple language (87%), a plain English summary (86%), and use of icons as visual prompts (73%).

While there has been a decrease in trust in organisations to handle personal information, the survey points to other factors that increase trust and transparency, such as certification.

As well as greater control over their personal information, Australians want to be protected against harmful practices, with 84% believing personal information should not be used in ways that cause harm, loss or distress. Australians also want increased rights around certain issues such as asking businesses to delete information (84%).

These insights are important to consider as we embark on a review of the *Privacy Act 1988* led by the Attorney-General's Department. The Australian Government has also committed to a new system of fines and penalties for interferences with privacy.

Additional measures that enhance organisational accountability and facilitate meaningful self-management of privacy will be a focus of the reform process. It should also consider the need for global interoperability of laws to reduce regulatory friction for business and enable economic growth, and a framework that equips the OAIC with the right tools to operate as a contemporary regulator.

When our research on community attitudes to privacy began in the 1990s, the Privacy Act had limited application to the private sector. As we head into the 2020s, the Act's coverage is being reviewed, providing a further opportunity to ensure it is aligned with community expectations.

My office will use the findings of ACAPS 2020 to inform our input into the review of the Privacy Act, and our priorities for the coming years. We look forward to working closely with Australian Government agencies and other organisations to build greater trust and confidence in the community that their privacy and personal information is respected and protected.

Angelene Falk, Australian Information Commissioner and Privacy Commissioner

Executive summary

The Australian Community Attitudes to Privacy Survey (ACAPS) 2020 was conducted between February and March 2020 with a nationally representative sample of 2,866 unique respondents aged 18 years and over. Additional research was conducted in early April 2020 to measure changing attitudes to privacy issues following the COVID-19 outbreak. For the first time since the survey's inception in 2001, all data was collected online.

The main objectives of the 2020 survey were to:

- provide insight on Australian attitudes towards privacy
- understand the change in Australian attitudes and behaviours over time through the construction of longitudinal trend models
- identify awareness of and concern about emerging privacy issues, related to new technologies and to regulation, and
- collect data to assist the OAIC as the national privacy regulator across policy, compliance, and communications initiatives.

Main findings

Privacy is an important issue for most Australians. Seventy percent consider the protection of their personal information to be a major concern in their life. The biggest privacy risks identified by Australians in 2020 are:

- identify theft and fraud (76%)
- data security and data breaches (61%)
- digital services, including social media sites (58%)
- smartphone apps (49%), and
- surveillance by foreign entities (35%) or Australian entities (26%).

Three in 5 Australians (59%) have experienced problems with how their personal information was handled in the past 12 months. The majority involved unwanted marketing communications or having their personal information collected (with or without consent) when this was not required to deliver the service.

The behaviours Australians are most likely to consider a misuse are when:

- an organisation uses their personal information in ways that cause harm, loss or distress (84%)
- information supplied to an organisation for a specific purpose is used for another purpose (84%), and
- a personal device is listening to conversations and sharing this with other organisations without their knowledge (83%).

Concerns regarding data privacy are driven by a belief that many companies routinely use personal information for purposes that make Australians uncomfortable.

Levels of comfort with the data practices of online businesses including social media sites and other digital platforms are low. They vary according to the nature of the organisation involved, the purpose for collecting or using the data and the type of personal information collected:

- The Australian Government is generally more trusted than businesses with the protection of personal information. Certain purposes are considered more legitimate than others, such as public safety. Australians are slightly more comfortable with most instances of government use of personal information than they were in 2017.
- Australians are particularly uncomfortable with businesses tracking their location through their mobile or web browser (62% uncomfortable) and keeping databases of information on what they have said and done online (62% uncomfortable).
- Australians are increasingly questioning data practices where the purpose for collecting personal information is unclear, with 81% of Australians considering 'an organisation asking for information that doesn't seem relevant to the purpose of the transaction' as a misuse (up 7% since 2017).

Most Australians have a clear understanding of *why* they should protect their personal information (85% agree) but half say they don't know how (49% agree). Four in 10 rate their knowledge of privacy as fair to poor, while 23% say their knowledge is excellent or very good. One third (34%) feel they are in control of their privacy, however just as many (34%) do not. This is not through lack of desire, as 87% want more control and choice over the collection and use of their personal information.

In line with this, Australians are most likely to believe they should have:

- the right to ask a business to delete their personal information (84%)
- the right to ask a government agency to delete their personal information (64%)
- the right to seek compensation in the courts for a breach of privacy (78%)
- to know when their personal information is used in automated decision-making if it could affect them (77%), and
- the right to object to certain data practices while still being able to access and use the service (77%).

Compared to 2017, fewer Australians are taking measures to protect their privacy, in particular:

- asking public or private sector organisations why they need personal information (down 16%)
- choosing not to use an app on a mobile device because of concerns over handling personal information (down 13%)
- shredding documents (down 11%), and
- adjusting privacy settings on a social networking website (down 10%).

Privacy regulation and reform

Eighty-three percent of Australians would like the government to do more to protect the privacy of their data. A quarter (24%) feel the privacy of their personal information is well protected, while 40% feel it is poorly protected.

On a prompted basis, half (48%) of Australians know about the Privacy Commissioner, an increase of 4% since 2017. Australians are just as likely to report a misuse of privacy to the police (37%) as the Privacy Commissioner (38%). Two-thirds (64%) of those surveyed are unaware that they can request access to their personal information from business and government agencies. This has not changed since 2017.

Privacy policies

Only 1 in 5 Australians (20%) read and are confident they understand privacy policies on internet sites. The main reasons why Australians do not read privacy policies include the length and difficulty of the policies.

Those who read privacy policies are much more likely to actively take measures to ensure the protection of their privacy and personal information.

Australians strongly support measures to improve privacy policies to make them easier to read. They want to see standard, simple language (87% support) and a plain English summary at the start of every privacy policy (86% support). There is also support (73%) for the use of icons as indicators that certain activities are undertaken, for example, if data is stored overseas.

Children's privacy

Australian parents provide their children access to connected devices and digital services early in life and are more likely to be concerned about their children's privacy (91%) than their own (82%). They are particularly uncomfortable with businesses tracking the location of a child without permission (70%) and businesses obtaining personal information about a child and selling it to third parties (69%).

Parents are very supportive of measures to increase the protection of their children's privacy and educate children on these issues. The most appealing idea is that a company must provide important data privacy information to children in clear language that is not misleading (85% support, 60% strongly support).

Half of parents (47%) believe that they are doing everything they can to protect their child's personal information. Thirteen percent do not actively do anything to protect their child's privacy online. Lack of knowledge, time and difficulty are the main reasons given for not doing more.

On average parents believe children should be able to consent to handing over their personal information in exchange for an online service from the age of 13, which generally coincides with the acquisition of a mobile phone and more widespread use of social media.

Young Australians

Young Australians (18-24) are more likely than older counterparts to know *how* to protect their personal information (54%; cf. 49% overall, 43% aged over 50). However, they are less likely to understand *why* they should protect their personal information (78%; cf. 85% overall).

Young Australians are the least likely age group to believe protecting personal information is a major concern in their life (63% cf. 70% overall) and the most likely to believe it is too much effort to protect the privacy of their data (39%; cf. average 30%).

Three in 10 (29%) believe the privacy of information and data when choosing a digital service is extremely important, compared with the Australian average of 54%.

Compared to the average Australian, those aged 18-24 are more likely to take control of their privacy in the digital realm, but less likely to take control outside this environment. Young Australians are more likely to adjust settings on social media (51%; cf. average 46%), use ad blockers, VPNs and privacy-focused web search engines (40%; cf. average 32%) and change smartphone settings for a higher level of privacy (43%; cf. average 35%). They are less likely to shred documents (26%; cf. average 41%) or to ask public or private sector organisations why they need their information (20%; cf. average 27%).

As with control, young Australians are also more likely to take action to protect their privacy. A quarter (26%) of young Australians have changed a service provider due to privacy concerns (cf. average 13%). They are more likely to have deleted an app (61% cf. average 57%) and request that personal information is deleted (27% cf. average 23%).

Privacy and COVID-19

The main fieldwork for the 2020 ACAPS survey was conducted immediately prior to the COVID-19 outbreak in Australia. The outbreak had an impact on attitudes to privacy with half (50%) of Australians considering that their privacy is more at risk in a COVID-19 environment than usual and almost half (48%) being more concerned about the protection of their location information than they were before the outbreak. Overall, more Australians feel comfortable than uncomfortable with the protection of their personal information while using digital services at home during the COVID-19 outbreak, whether it is for work, studying or personal use.

The majority (60%) agree that some privacy concessions must be made to combat COVID-19 for the greater good. The same proportion agree that concessions should not be permanent. Consent is still important: more than half (54%) are comfortable with the government using phone data to help stop the spread of COVID-19 with consent, whereas 29% are comfortable with phone data being used without consent.

Introduction and background

The Australian Community Attitudes to Privacy Survey (ACAPS) is a longstanding study to evaluate the awareness, understanding, behaviour and concerns about privacy among Australians. The survey was first conducted in 2001. It is commissioned by the national privacy regulator, the Office of the Australian Information Commissioner (OAIC). It provides longitudinal information on the attitudes Australians hold regarding key privacy issues, their experiences and perspectives towards misuse of personal data, as well as actions taken to protect their privacy.

Rapid growth of online businesses, social media and other digital platforms has presented new privacy and personal data considerations. The past decade has seen a dramatic shift in the type of privacy risks Australians face and, in response, a change in the types of concerns Australians hold about privacy. The 2020 survey also provides insight into how Australians' views on privacy have changed over time.

Findings from the survey inform the OAIC's strategic direction in policy development, enforcement and education and awareness priorities.

The main objectives of the 2020 survey were to:

- provide insight on Australian attitudes towards privacy
- understand the change in Australian attitudes and behaviours over time through the construction of longitudinal trend models
- identify awareness of and concern about emerging privacy issues, related to new technologies or to regulation, and
- collect data to assist the OAIC as the national privacy regulator across policy, compliance and communications initiatives.

The 2020 survey has changed from earlier waves of the study and addresses a wide range of new concerns. This wave examines children's privacy issues for the first time, following a separate survey module that was solely answered by Australian parents. It also explores privacy-related topics such as biometrics, artificial intelligence and location data in more detail than before.

The main fieldwork for the 2020 survey was conducted immediately prior to the COVID-19 outbreak in Australia. The response to the COVID-19 pandemic was rapid and actions taken by government, businesses and individuals had implications for privacy. In response to the pandemic, an additional privacy survey was conducted in early April, several weeks after the first physical distancing rules were applied in all Australian states and territories, to understand the impact of these events on Australian attitudes to privacy.

Methodology

Overview

The 2020 survey is the fifth in a series of surveys initiated in 2001. The methodology has evolved over the past two decades to reach a representative sample of Australia's population. Between 2001 and 2013, all interviews were completed via Computer Assisted Telephone Interviewing (CATI). In 2017, the methodology shifted to a hybrid online/CATI methodology, where 800 surveys were conducted via CATI and 1,000 were completed online, reaching respondents via an online research panel. In 2020, all data was collected online, with 39% of the respondents recruited via telephone (including via human operator and SMS) to ensure it included respondents who are not members of paid, online market research panels.

Questionnaire development

The questionnaire was jointly developed by Lonergan Research and the OAIC. A comprehensive phase of cognitive and pilot testing was undertaken to evaluate the questionnaire from a respondent perspective and ensure that the questions were clear, unambiguous and interpreted in the manner intended.

Questionnaire length, sample size and modularisation

The 2017 survey was 30 minutes in length. It was split into 3 sections (modules) and each respondent was asked to answer 2 of those 3 modules. Average length of interview per respondent was 20 to 30 minutes.

In 2020, the total survey length was increased to 40 minutes. The shift to a completely online data collection methodology enabled quicker completion of the survey and the expansion of the questionnaire from 49 questions in 2017 to 76 in 2020.

The goal in 2020 was to replicate a sample size of n=1,500, but without the survey fatigue issues of a 40-minute survey. To achieve this, the survey was divided into 5 modules of questions, of which 4 could be answered by any adult 18 or over in Australia. The fifth was only answered by parents or carers of children aged 17 years and under. Each module was around 8 to 10 minutes in length. Respondents were encouraged and incentivised to answer multiple modules, however they were not permitted to answer more than 2 modules in any given day. Modules 1 and 2 were linked, as were modules 3 and 4. Respondents taking a break after the completion of one part of a linked module were required to complete the second part of that module as a priority. Beyond this, respondents were allocated to the module where their combination of age, gender and location had the fewest responses, or randomly allocated to a module if these were even.

Quotas were applied for the first 4 modules, representative of the general population in Australia, and a minimum sample size of 1,500 respondents was reached for each module. Quotas representative of the population of parents in Australia were applied for the fifth module.

	Total unique respondents	Module 1 & 2	Module 3 & 4	Module 5 (parents)
Recruited via phone	1,043	555	561	244
Recruited online	1,645	955	948	545
Total	2,688	1,510	1,509	789

Sampling

Due to the increasing ownership of mobile phones and the decline of landline phones, the mix of landline and mobile numbers has changed over time; 30% of numbers were mobile numbers in 2013, 80% in 2017 and 100% in 2020.

Data calibration of trend analysis

Data collection for the survey has migrated from pure CATI (2013) to mixed CATI and online (2017) to pure online (2020). This change in methodology can impact results. To allow fair analysis of trend data, a calibration of the data was applied to historic data to allow trend comparisons.

Trends from 2017 to 2020 are established by comparing online data to online data (with the 2017 online data reweighted to be representative by age, gender and location in isolation to the CATI data). Trends from 2013 to 2017 were established by comparing CATI data to CATI data (with a separate set of weights applied to the 2017 CATI data). Trends prior to 2013 were as reported.

Historic trend data may therefore differ from data published in previous years. Further calibrations should not be necessary for future waves of the survey, assuming an online data collection methodology is maintained.

Fieldwork

The survey fieldwork started on 17 February 2020 and was completed on 16 March 2020. The recruitment via phone was conducted by a combination of SMS and human interviewers. Human operators are essential to maximise response rates. Their role is to build rapport, explain the importance of the survey and maximise the trust respondents have in clicking on the SMS link. Where appropriate, they discussed the prize draw incentive associated with this study[1]. The interviewers had the capability to send (or resend) an SMS with a unique link or an email if the respondent preferred it. All telephone interactions with respondents were conducted by the fieldwork team at Lonergan offices in the Sydney CBD. The SMS and email contained broad information about the survey, the survey link and opt-out messaging. Responses to both were monitored by both an AI (to ensure opt-outs were actioned immediately) and a human to address any more complex queries.

[1] The prize draw incentive for this study was a cash prize of $1,000 (NSW Permit No. LTPS/20/42087)

Additional COVID-19 survey

The additional survey measuring attitudes to privacy specifically in the context of Australians adapting to COVID-19 social distancing and self-isolation measures was conducted among 1,004 members of a research panel between Tuesday 7 April and Thursday 9 April 2020. The data was weighted to the latest population estimate by the Australian Bureau of Statistics. This survey was conducted online, solely using an online research panel. This data is reported in Chapter 12 of this report.

Glossary

Statistics shown in this report are regularly compared across demographic groups. The standard format to compare these in this report is as in the following example, where 'cf.' is an abbreviation used to introduce the comparison.

- Example: The privacy of information and data when choosing a digital service is much more important to older Australians than younger ones (50+ years 90%; cf. 35-49 years 79%, 18-34 years 79%).

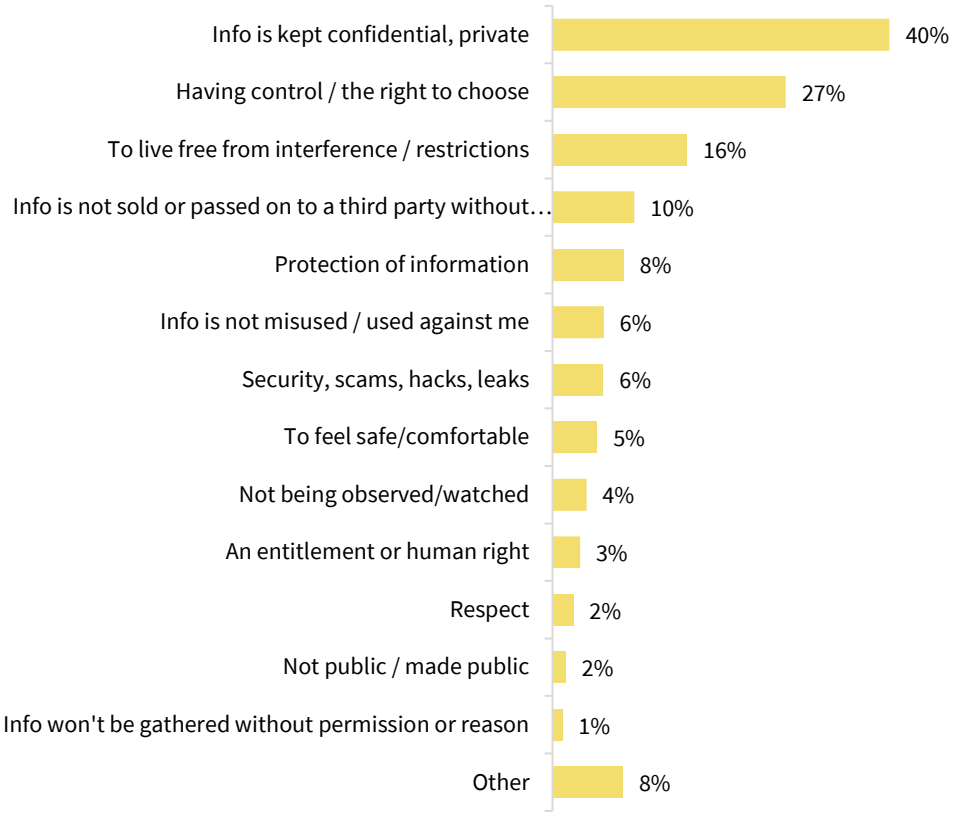
Part 1: Introduction to privacy

What ‘privacy’ means to Australians

Respondents were asked to describe in their own words what privacy means to them. Thematically, there are 6 main groups of responses:

1. the idea of keeping one’s information private and confidential (41%)
2. the idea of having control over one’s information (27%)
3. the concept of protection against harmful practices and security (19%)
4. the idea of living free from interference and maintaining one’s lawful right to be left alone (18%)
5. the idea of not having one’s information shared or sold without permission (11%), and
6. the right to security and respect (11%).

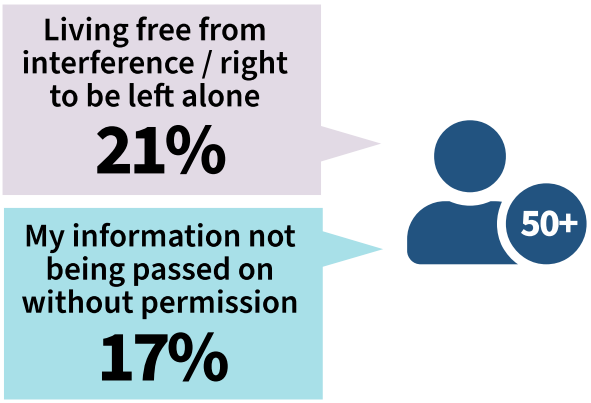
Figure 1: What privacy means to Australians (unprompted, categorised by researchers)



B1. In your own words, please tell me what ‘privacy’ means to you? Please be specific in terms of what this covers — unprompted. Base: Australians 18+ (n=1,451)

Privacy is more likely to mean having control over personal information to Australians with a higher level of education and higher income earners. For 1 in 3 (31%) Australians with a household income over $100k, privacy means having control over personal information; this compares with 28% of those earning $70-$99k and only 25% of those earning less than $70k.

Those in regional areas are also more likely to mention the idea of control (32%); only 25% of those in metropolitan areas mentioned the idea of control.



Privacy is more likely to evoke the right to be left alone to older Australians, as well as the idea of not having one's information shared or sold to a third party.

Twenty-one percent of Australians aged 50 and over feel that privacy means the right to be left alone, and 17% mentioned the idea of not having one's information shared or sold to a third party. Younger Australians are less likely to associate these ideas with privacy: 16% of those aged 35-49 and 17% of those aged 18-34 mentioned the right to be left alone; only 7% of Australians aged 35-49 and 5% of Australians aged 18-34 mentioned the idea of not having one's information shared or sold to a third party.

The most common words used by Australians in their response are information, personal, privacy and shared. However, the relatively high use of words like consent, disclose, permission, secure, access and right are evidence that Australians are considering many important concepts in their responses.

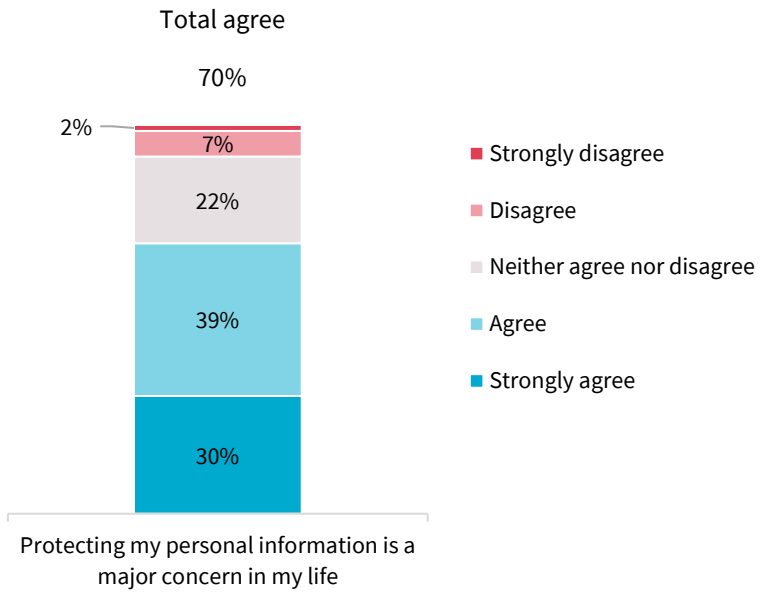
Figure 2: What privacy means to Australians (word cloud)

B1. In your own words, please tell me what 'privacy' means to you? Please be specific in terms of what this covers. Base: Australians 18+ (n=1,451)

The importance of privacy

The majority of Australians (70%) see the protection of personal information as an important issue and a major concern in their life. Although privacy is important across most demographic groups, there are variations by age and level of technology adoption. Older Australians are more likely to value protection of their personal information highly, with 73% of those aged 50 years and over feeling that this is a major concern in their life. This compares with 68% of those aged 35-49 and 66% of those aged 18-34 who feel that protection of their personal information is a major concern.

Figure 3: Percentage of Australians concerned about personal information protection



B2_1. Thinking about data privacy, to what extent do you agree or disagree with each of the following statements?
Base: Australians 18+ (n=1,506)

Early adopters of technology are the most likely to strongly agree that protecting their personal information is a major concern in their life – 2 in 5 (40%) early adopters strongly agree, which compares with an average of 30% among the Australian general population.

Early adopters of technology

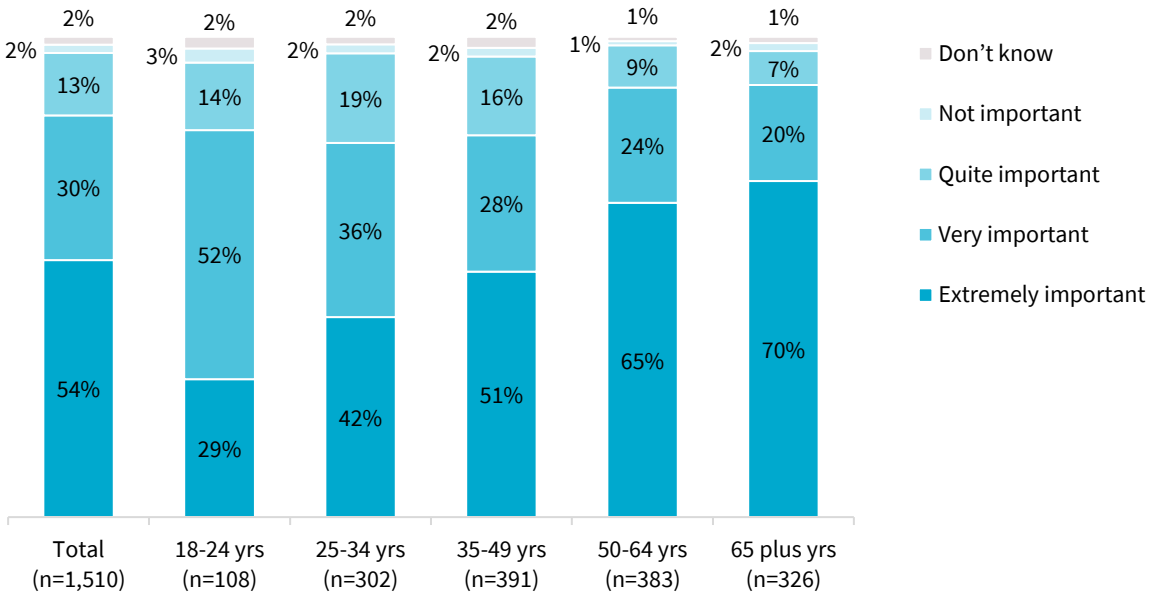
The speed at which Australians adopt technology often influences their attitude and behaviour towards privacy, particularly early adopters of technology. Five percent of the population are early adopters who are the first to try a new technology. Early adopters are the most likely to have a very good to excellent knowledge of data protection (53%); in contrast, 23% of the Australian general population rate their knowledge of data protection as 'excellent'.

The importance of privacy when choosing a digital service

Concerns around privacy of information are even more prevalent in the digital space. Eighty-four percent of Australians consider the privacy of their information to be extremely or very important when choosing a digital service (including 54% who say it is extremely important).

The privacy of information and data when choosing a digital service is more important to older Australians than younger ones. Younger Australians aged 18-34 are the least likely to feel this is 'extremely important' (29%), compared with the Australian average of 54% who feel that privacy is important when choosing a digital service.

Figure 4: Importance of privacy when choosing a digital service

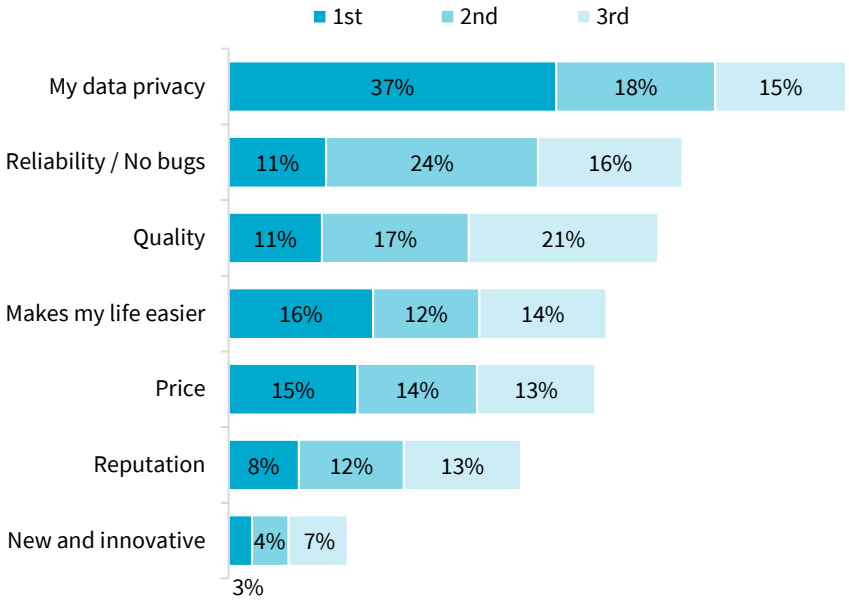


A2. Thinking of choosing a digital service, how important is the privacy of your information and data when choosing a digital service (e.g. any app or program on a phone or laptop)? Base: Australians 18+ (n=1,510)

At the time of choosing which app or program to download, Australians consider the privacy of their data to be more important than all other considerations such as quality, convenience or price. More than half of Australians (55%) rank 'my data privacy' as the most or second most important element at the time of choosing a digital service, making privacy far more important to Australians than the reliability of the service or app (35% rank this first or second).

Younger Australians, aged 18-24, are less likely to rank 'my data privacy' in the top 3 most important elements (54%). Older Australians, especially those aged 65 and over (80%), are much more likely to place 'my data privacy' in their top 3.

Figure 5: Importance of aspects when choosing an app or program to download



A1. Please rank each of the following in order of importance when choosing which app or program to download. Base: Australians 18+ (n=1,510)

On an unprompted basis, the top reasons for considering data privacy important at the time of choosing a digital service are privacy and protection of personal information (22%), ownership and control of access to the personal information (22%), concerns such as fear of scams, hacks and fraud (21%) and personal harm/security (11%).

Figure 6: Reasons privacy is important in digital services

A3. Why do you say that? - Unprompted (After levels of importance of privacy at the time of choosing a digital service). Base: Australians 18+ who consider the privacy of their information quite to extremely important (n=1,385)

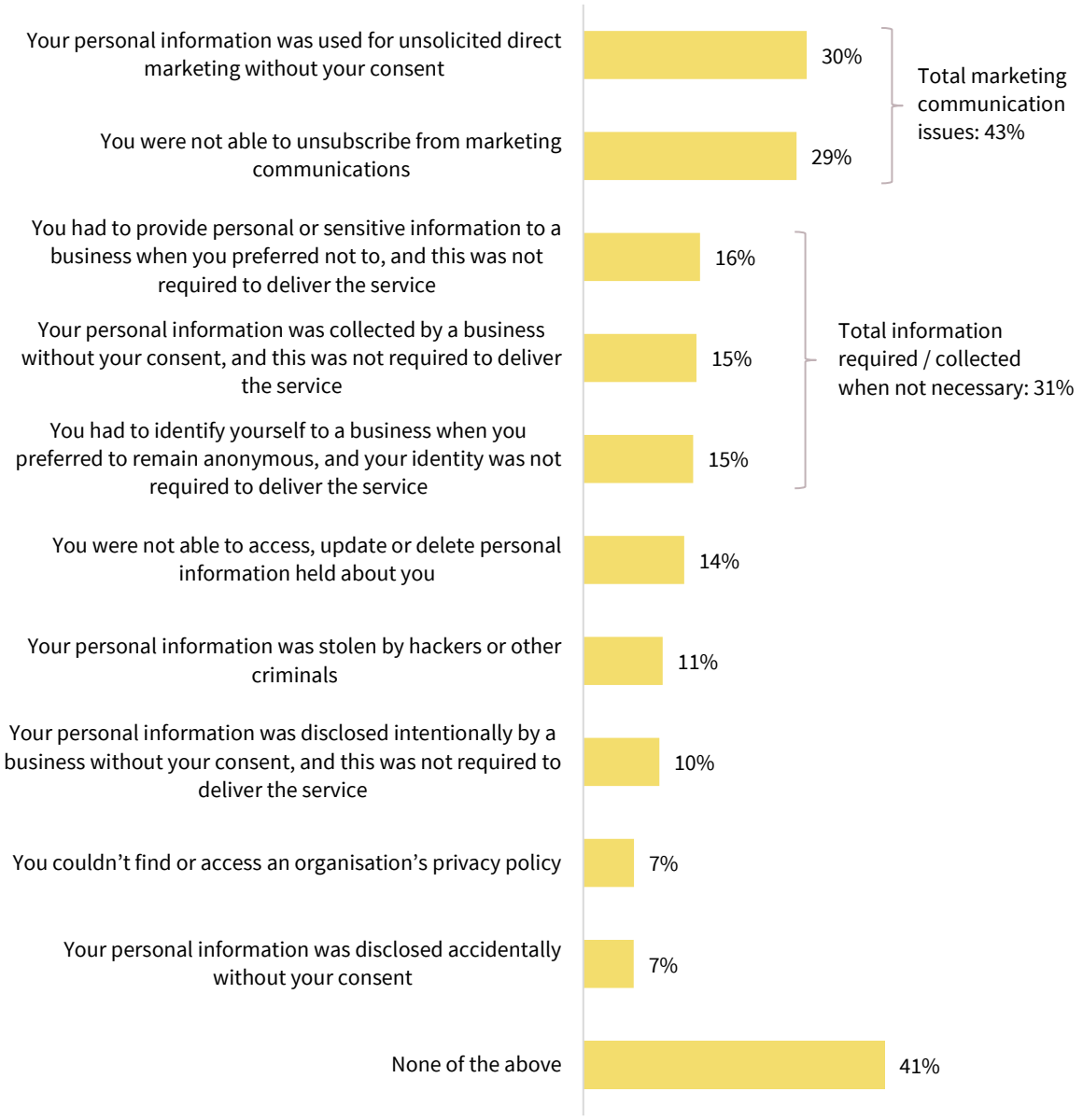
Incidence of negative privacy experiences

The majority of Australians (59%) have experienced problems with the handling of their personal information in the past 12 months. Most occurrences relate to unwanted marketing communications, with 43% receiving unsolicited direct marketing without consent or that they were not able to unsubscribe from. Thirty-one percent have had their personal information collected (with or without consent) when this was not required to deliver the service.

The majority of Australians (59%) have experienced problems with the handling of their personal information in the past 12 months.

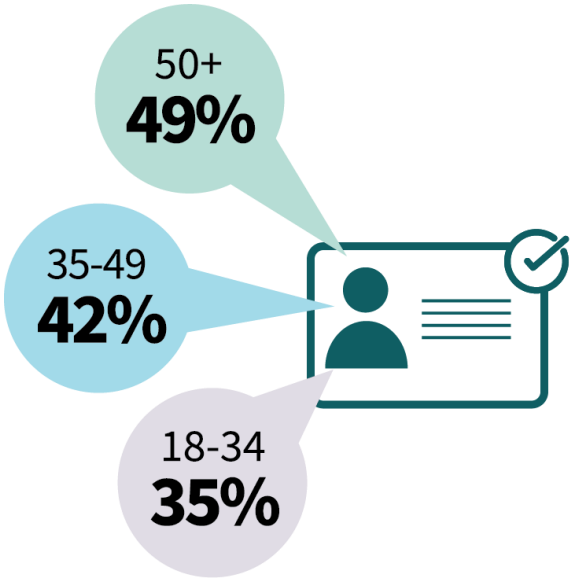
The majority of Australians (59%) have experienced problems with the handling of their personal information in the past 12 months

Figure 7: Percentage of Australians who experienced mishandling of personal information



A9. Have you experienced any of the following types of problems with how your personal information was handled in the past 12 months? Base: Australians 18+ (n=1,510)

Half of Australians aged 50 and over (49%) have experienced problems with how their personal information was handled because of unwanted marketing communications. This is only true of 2 in 5 (42%) Australians aged 35-49 and 35% of Australians aged 18-34.



Half of Australians aged 50 and over have experienced problems with how their personal information was handled as a result of unwanted marketing communications

Males (34%) and people aged 18-34 (35%) are the most likely to report that their information was collected when it was not required to deliver the service. Females (27%) are less likely to report this happening, as are those aged 35-49 (27%) and those aged 50 and over (30%).

One in 2 males (50%) experienced problems other than marketing, while only 2 in 5 (40%) females reported the same.

Early adopters of new technology are more likely to have experienced a problem with how their personal information was handled (79%), compared to 58% of those who adopt technologies later.

Digital data practices

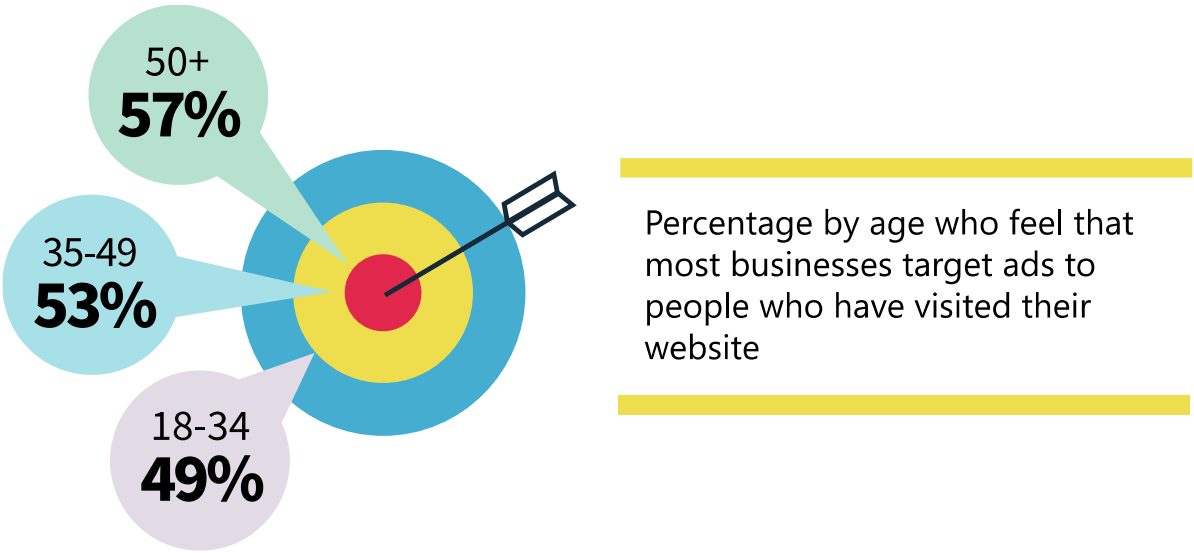
The term 'digital data practices' is used throughout the survey and this report to encompass a range of online activities involving personal information and user data, including location tracking, targeted advertising and selling or sharing information with third parties.

Incidence of data-driven advertising

Australians believe most businesses use a variety of data-driven advertising practices, which potentially have an impact on their privacy. The practices most commonly believed to be occurring include:

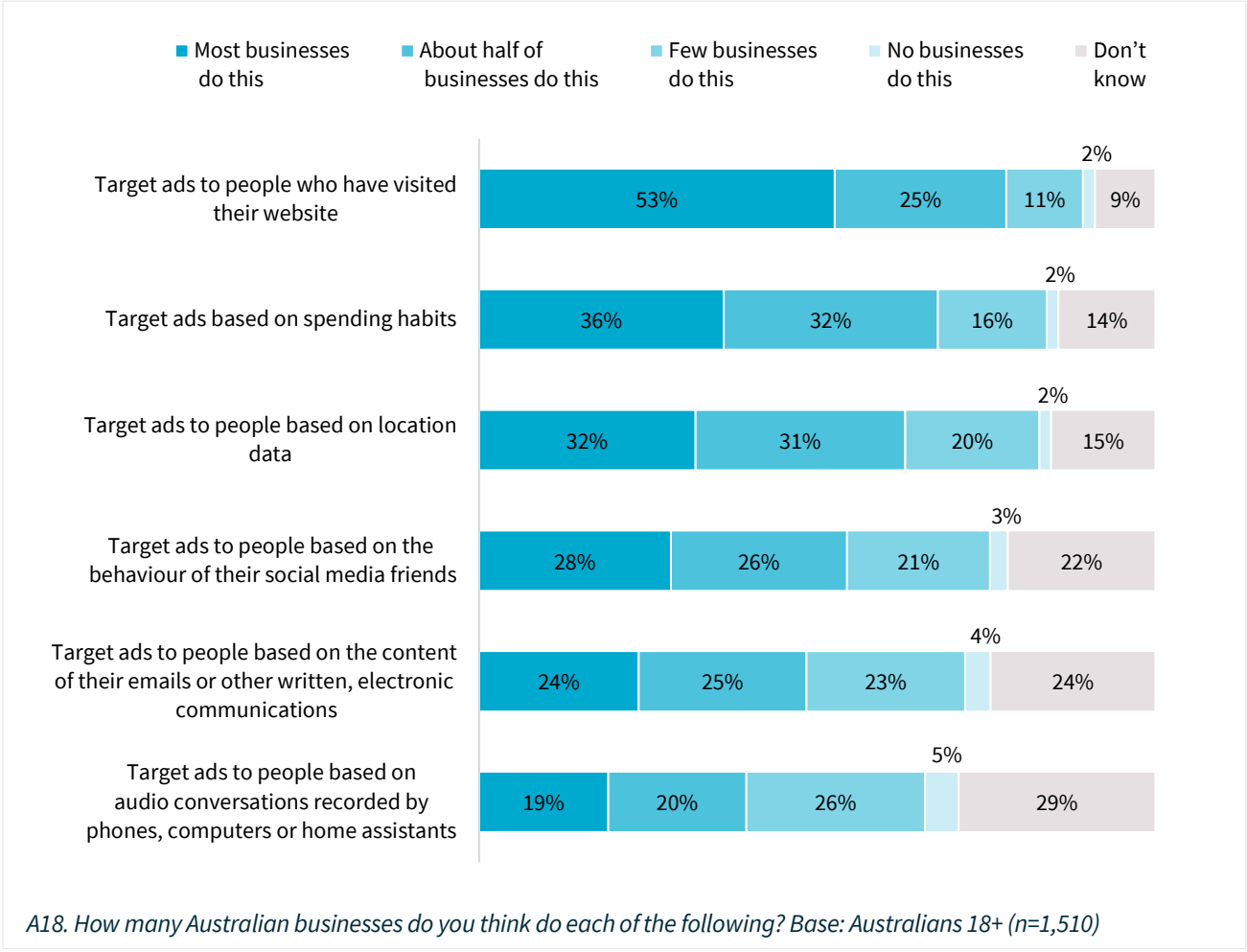
- targeting ads to people who visit their website (78% think more than half of businesses do so)
- targeting ads based on spending habits (68% think more than half of businesses do so), and
- targeting ads based on location data (63% think more than half of businesses do so).

Older Australians are more likely than their younger counterparts to believe that most businesses target ads to people who have visited their website. Fifty-seven percent of those aged 50 and over reported this, while 53% of those aged 35-49 and less than half (46%) of those aged 18-34 believe that most businesses target ads to people who have visited their website. Late adopters of new technology (42%) are also more likely to believe businesses target ads to people who have visited their website, compared with just 39% of early adopters.

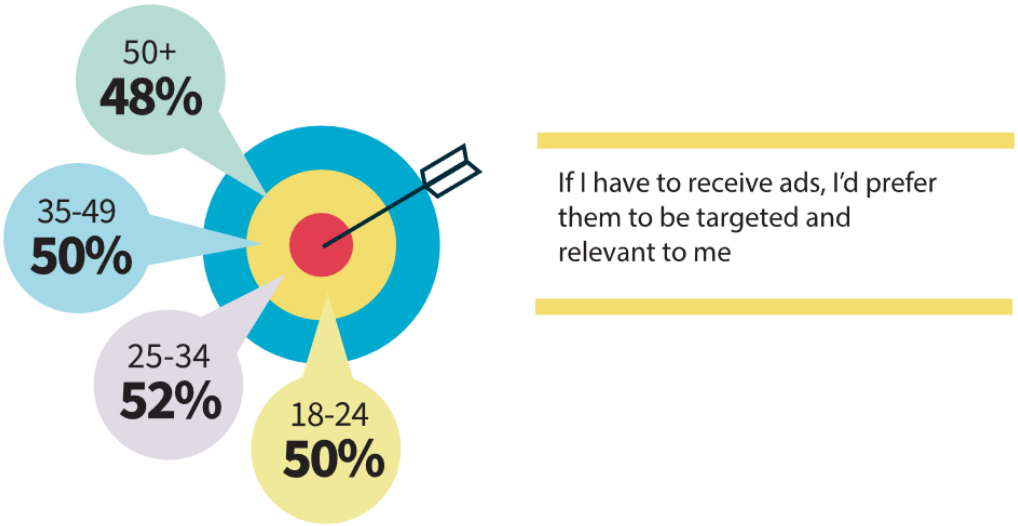


Targeted advertising based on audio conversations recorded by phones, computers or home assistants is believed to be occurring less often than any other practice. However, 40% believe half or more businesses do this. The proportion of people who believe no business targets ads using the listed data practices is very low, ranging from 2% to 5%.

Figure 8: Beliefs around the proportion of businesses that use targeted advertising techniques

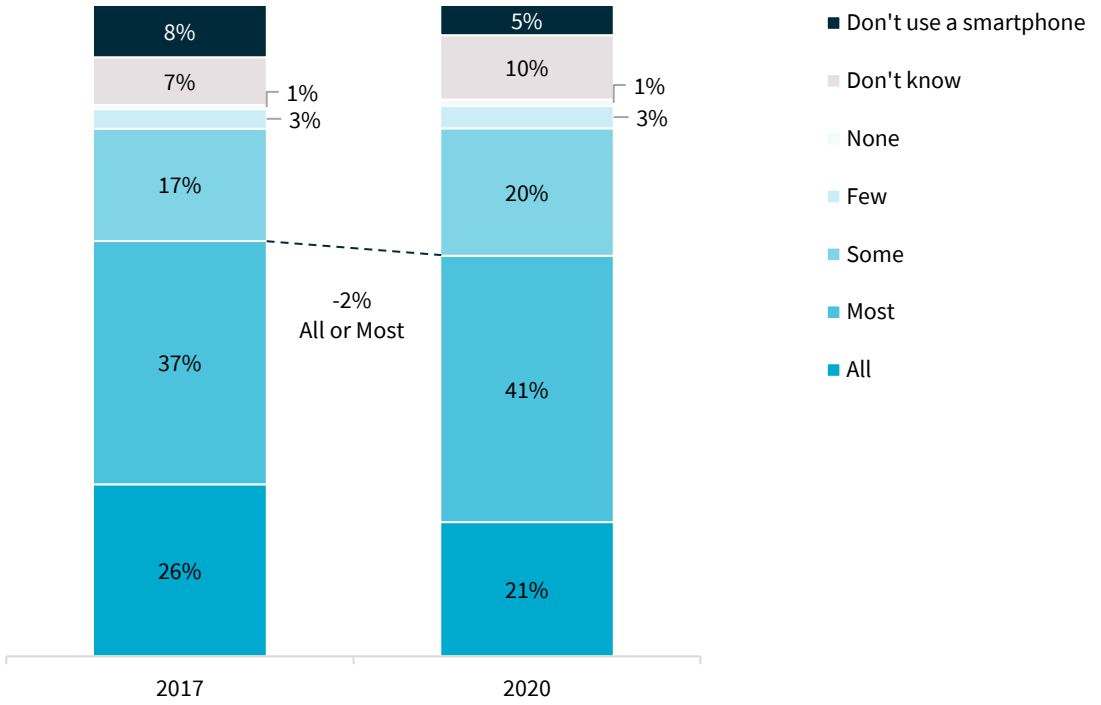


A18. How many Australian businesses do you think do each of the following? Base: Australians 18+ (n=1,510)



Compared with 2017 (63%), a similar proportion of Australians (62%) are likely to think that all or most smartphone apps collect information about the people who use them, a finding that is consistent across all demographics.

Figure 9: Beliefs around the proportion of smartphone apps that collect information about people who use them — by year



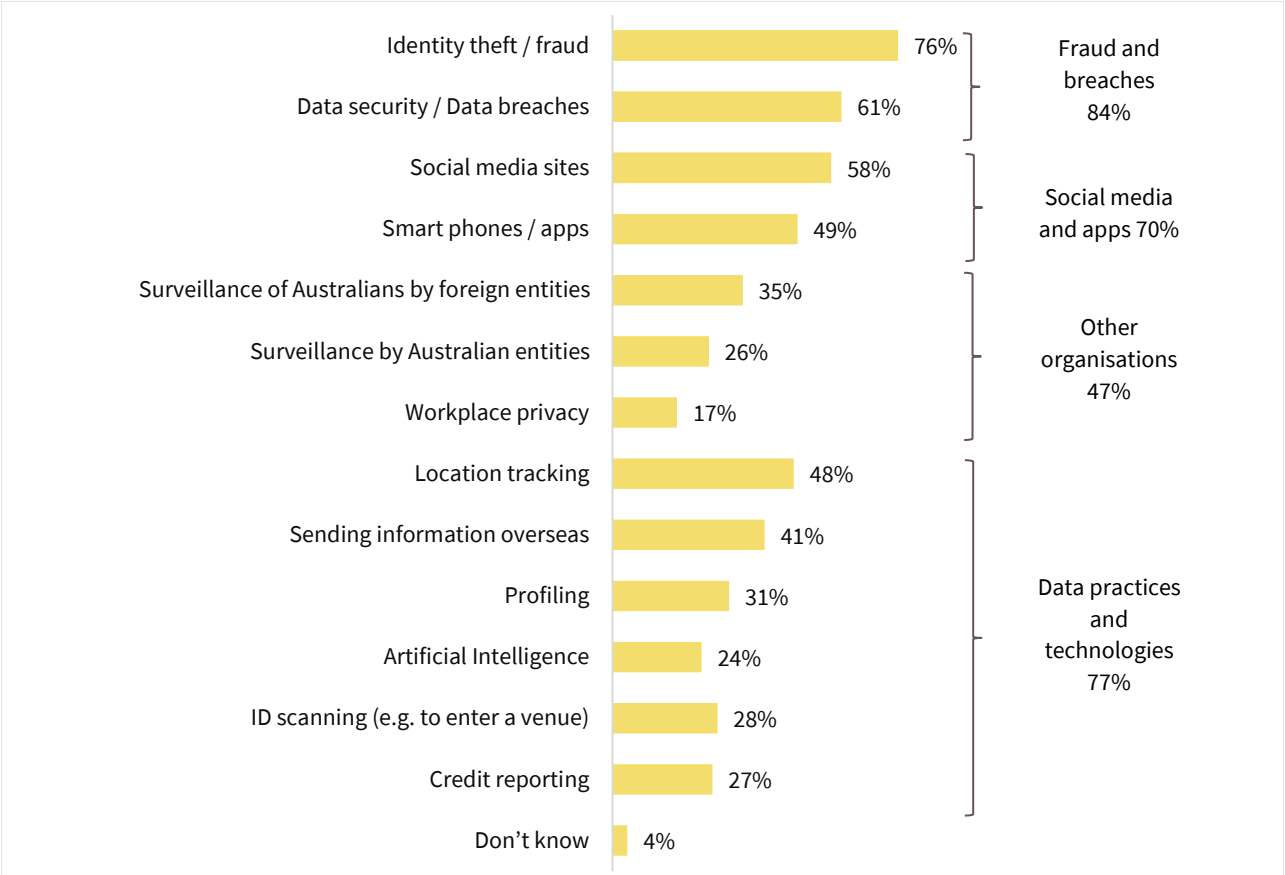
A19_2020 / Q24_2017. Proportion of smart phone apps that collect information about people who use them. Base: Australians 18+ (n=1510 in 2020, n=711 in 2017)

Perceived privacy risks

Australian views about privacy risks related to the use of personal data have shifted since 2017, as some digital data practices have become more widespread and evolved in scale and accuracy. The biggest risks identified in 2020 are 'identity theft/fraud' (76%) and 'data security/data breaches' (61%).

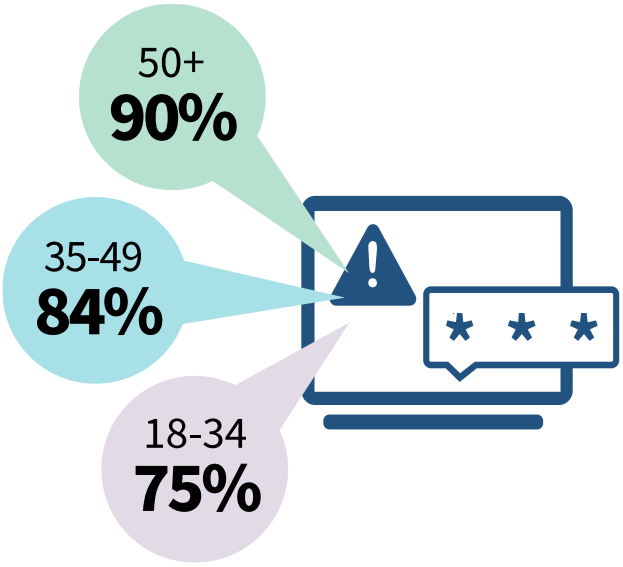
This question was unprompted in 2017 and therefore the percentages and data are not strictly comparable. However, in 2017, identity theft/fraud was less likely to be mentioned as a major risk than online services and social media sites (27% for social media in 2017 followed by 17% for identity theft/fraud).

Figure 10: Biggest privacy risks Australians are facing today



A8. What do you think are the biggest privacy risks that face people today? Base: Australians 18+ (n=1,510)

Ninety percent of those aged 50 and over consider 'fraud and breaches' as some of the biggest risks to their privacy. Fewer feel the same way among 35-49-year-olds (84%) and 18-34-year-olds (75%). Similarly, Australians aged 50 and over (49%) are more likely to consider 'sending information overseas' among the biggest privacy risks that Australians face today. This compares with 35% of those aged 35-49 and 34% of those aged 18-34 who feel that 'sending information overseas' is one of the biggest risks.



Most Australians think identity theft / fraud and data breaches / security are the biggest threat to privacy

A quarter (24%) of early adopters of new technologies feel that 'workplace privacy' is one of the biggest risks – this is only true among 17% of later adopters.

Levels of comfort with data practices

Australians are concerned about digital data practices such as information sharing (where personal information or user data is passed from one organisation to another for government, commercial or other purposes), location tracking and targeted advertising. Their level of discomfort with some of these practices is high, consistent with the belief that the practices are widespread and create considerable risks such as identity theft.

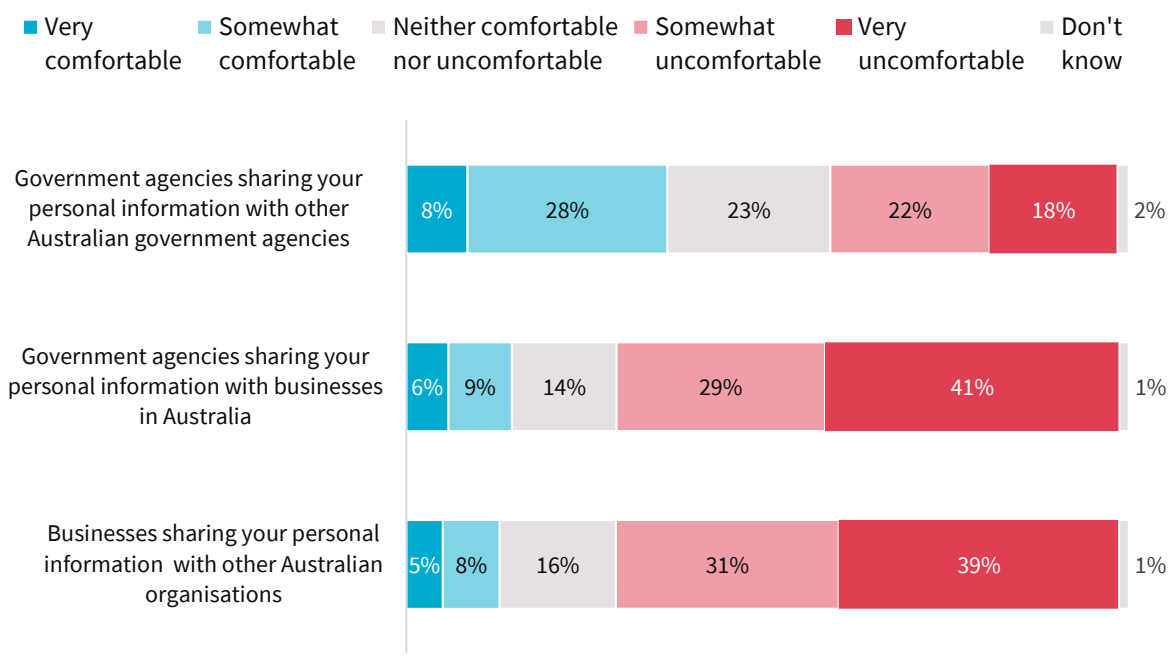
Comfort with information sharing by organisation type

Just over a third (36%) of Australians are comfortable with government agencies sharing their personal information with other Australian Government agencies, while 40% are uncomfortable with this. Australians are far less likely to be comfortable with government agencies sharing their personal information with businesses in Australia (15% comfortable, 70% uncomfortable) and businesses sharing their personal information with other Australian organisations (13% comfortable, 70% uncomfortable).

Note: Comfort is used when assessing how people feel about various actions. Trust is used when assessing how people feel about various organisations. There is some crossover with questions about organisations combining comfort and trust responses. Confidence is an alternative description for trust with respect to organisations.

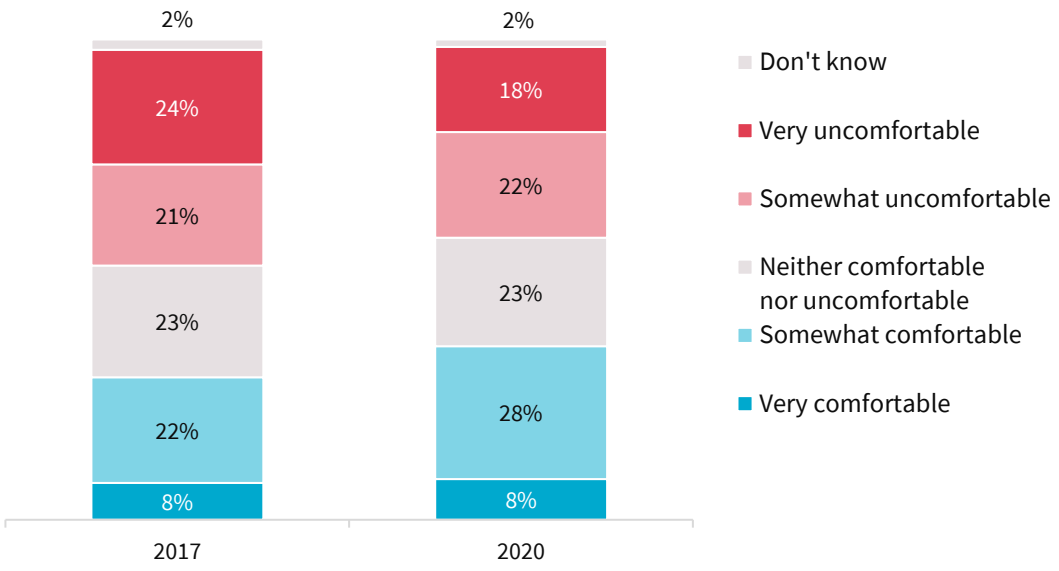
Australians are more likely to be comfortable (36%) with government agencies sharing information with other government agencies now, compared with 30% in 2017. Similarly, the proportion of people who are uncomfortable with this practice (40% in 2020) has decreased since 2017 (45%).

Figure 11: Comfort with information sharing by organisation type



B14. How comfortable or uncomfortable are you with… Base: Australians 18+ (n=1,506)

Figure 12: Comfort with government agencies sharing information with other Australian government agencies over time



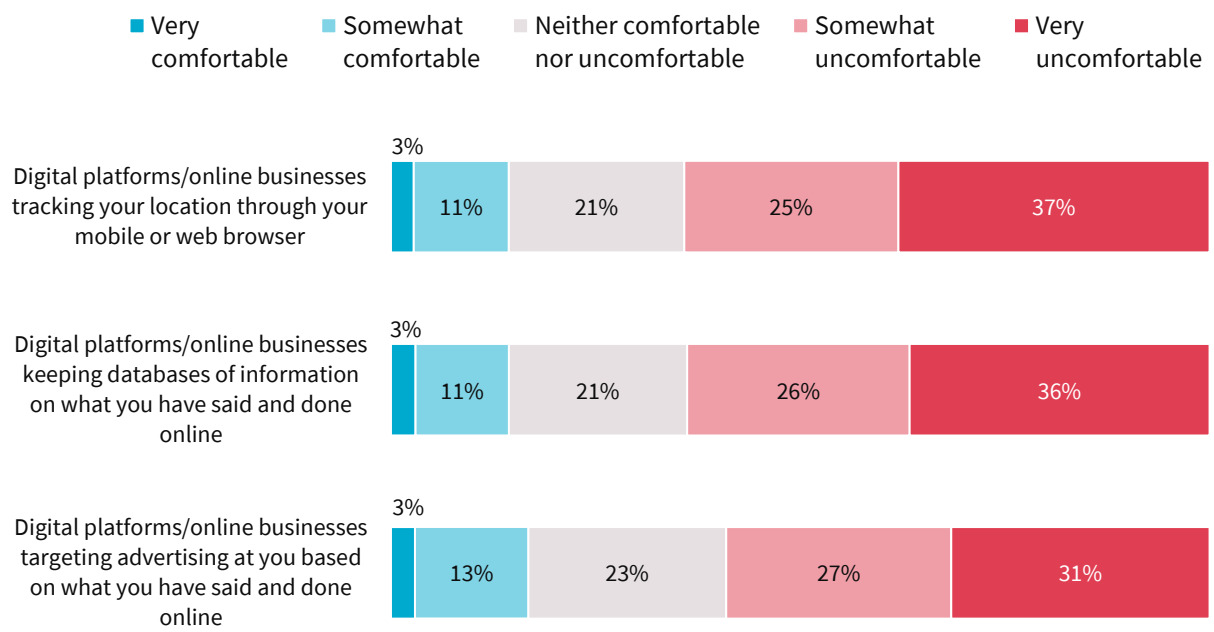
B14_2020 / Q14C_2017. And how comfortable or uncomfortable are you with government agencies sharing information with other government agencies? Base: Australians 18+ (n=1,506 in 2020, n=717 in 2017)

Comfort with digital platforms' data practices

At least half of Australians are uncomfortable (and 3 in 10 very uncomfortable) with digital platforms and other online businesses like social media sites:

- tracking their location through their mobile or web browser (62% uncomfortable, including 37% very uncomfortable)
- keeping databases of information on what they have said and done online (62% uncomfortable, including 36% very uncomfortable), and
- targeting advertising based on what they have said and done online (58% uncomfortable, including 31% very uncomfortable).

Figure 13: Comfort with digital platforms' data practices



A16. How comfortable are you with each of the following data practices? Base: Australians 18+ (n=1,510)

There are variations in levels of discomfort with digital practices across age demographics. In general, older Australians are less comfortable and younger Australians relatively more comfortable with each practice. Australians aged 65 years and older are equally uncomfortable with each of the identified data practices:

- 74% are uncomfortable with location tracking (including 47% very uncomfortable)
- 75% are uncomfortable with businesses keeping databases on what they have said online (including 46% very uncomfortable), and
- 73% are uncomfortable with targeted advertisements (including 45% very uncomfortable).

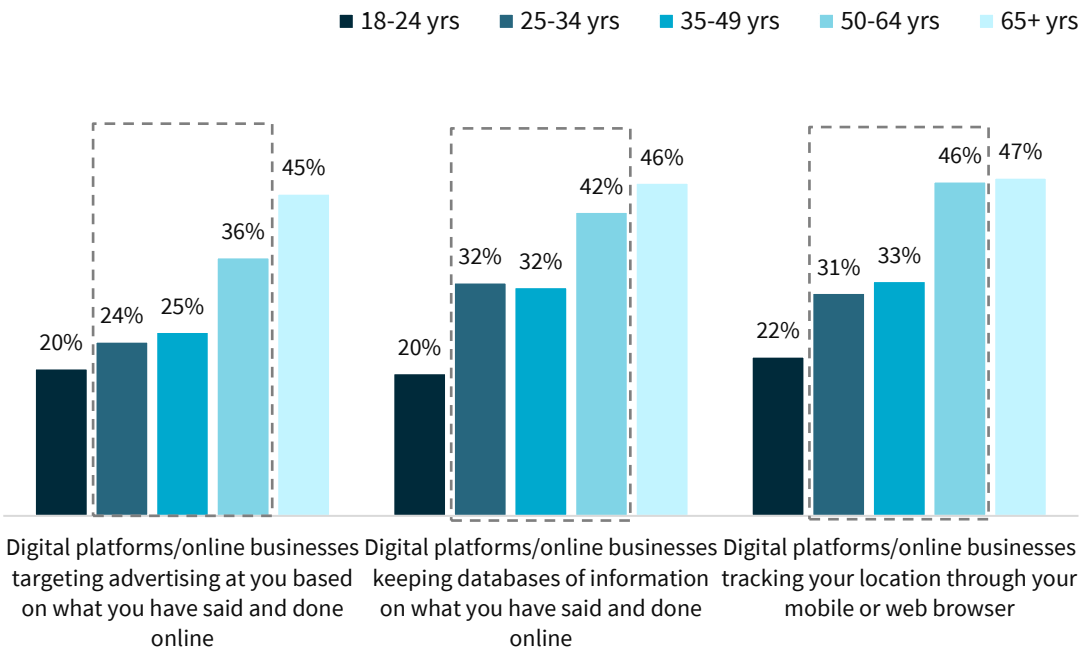
Those aged 65 and over are most likely to be very uncomfortable with each practice:

- 45% are very uncomfortable with digital platforms/online businesses targeting advertising based on what they have said and done online
- 46% are very uncomfortable with digital platforms/online businesses keeping databases of information on online behaviour, and
- 47% are very uncomfortable with digital platforms/online businesses tracking their location through their mobile or web browser.

In comparison:

- only 20% of Australians aged 18-24 are very uncomfortable with targeted advertising by digital platforms/online businesses
- 20% of 18-24-year-olds are very uncomfortable with digital platforms/online businesses keeping databases of online behaviour, and
- 22% are very uncomfortable with location tracking by digital platforms/online businesses.

Figure 14: High discomfort (% very uncomfortable) with digital platform/online business data practices by age



A16. How comfortable are you with each of the following data practices? Base: Australians 18-24 (n=108) / 25-34 (n=302) / 35-49 (n=391) / 50-64 (n=383) / 65+ (n=326)

Respondents were asked to provide other examples of data practices of digital platforms and online businesses they are uncomfortable with. Despite high levels of discomfort with the examples provided, the majority could not think of any other practices they were uncomfortable with (49% nominating nothing or don't know).

Of those who did nominate an additional practice, the sale, use or exchange of personal information without consent (11%) was most likely to create discomfort, followed by the practices of social media businesses (10%). Some felt discomfort with digital platforms and online businesses (7%) and advertising or spam (7%).

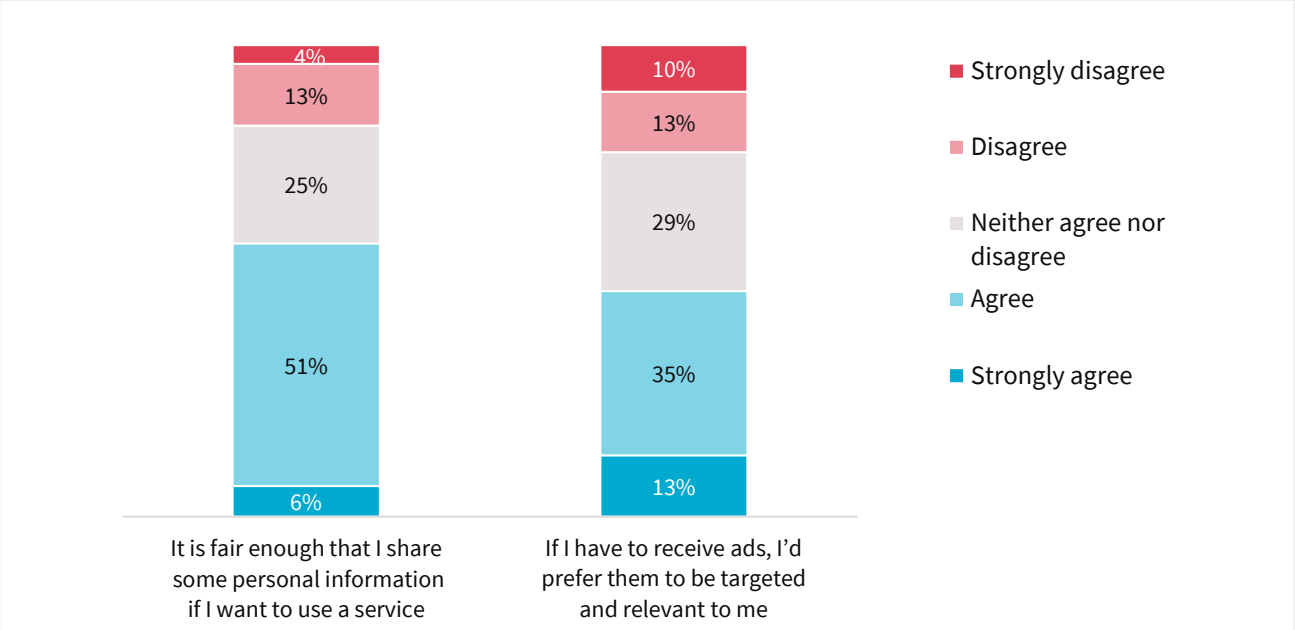
While no Australians aged 18-24, mentioned 'the sale or use of personal information without consent' as a concern, they were the most likely to mention 'social media' (21%). Other age groups were similarly likely to mention 'sale or use of personal information without consent' (12% of those aged 25-34, 9% of those aged 35-49 and 14% of those aged 50).

In contrast, likelihood of concerns about social media decreases with age: 14% of those aged 25-34; 9% of those aged 35-49 and 7% of those aged 50 over. (These are unprompted and may be impacted by higher levels of salience of social media as well as higher levels of concern.)

General acceptance of data practices

Most Australians (58%) agree it is fair enough they share some information if they want to use a digital service and, if they have to receive any ads, they'd prefer that they are targeted to them (48%). However, they are concerned if personal information is collected when it is not required to deliver the service (Figure 7). Eighty-one percent of Australians consider an organisation asking them for personal information that does not seem relevant to the purpose of the transaction to be misuse. (Figure 19).

Figure 15: How Australians feel about data privacy



B6_1 & B6_3. Thinking about data privacy, do you agree or disagree with the following? Base: Australians 18+ (n=1,506)

Levels of comfort by purpose and organisation

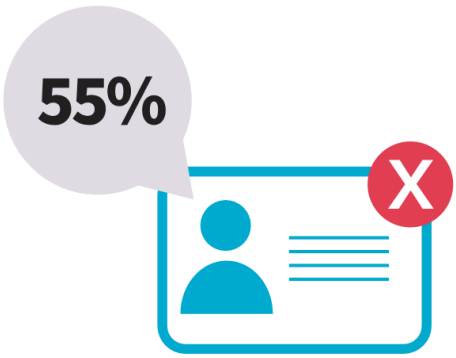
Business use of personal information

Overall levels of comfort with data practices vary according to the type of information collected, the organisation involved and the purpose behind it. Commercial profiling activities generally drive higher levels of discomfort among Australians than government data practices. For example:

- 56% are uncomfortable with a business collecting information from consumers' mobile devices to decide on location and content of billboards/outdoor advertising
- 55% are uncomfortable with a business creating profiles about consumers based on data collected about them, and
- 53% are uncomfortable with a business combining data about their customers (for example, loyalty card transaction history) with other data (for example, IP address, type of browser used) to better profile their customers.

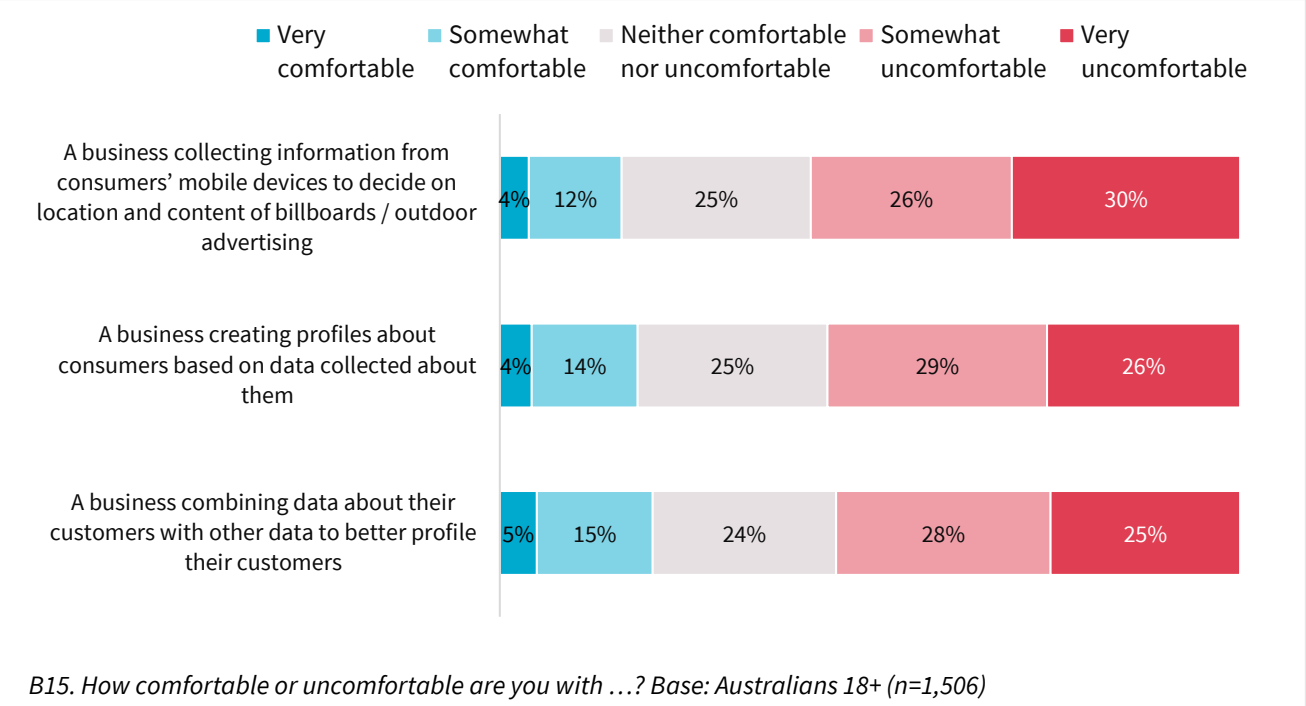
Older Australians are the most likely to be uncomfortable with each of the above practices; in particular, 66% of those aged 50 and over are very uncomfortable with businesses creating profiles about consumers based on data collected about them. This compares with 55% of Australians aged 35-49 and 40% of Australians aged 18-34 who feel the same way.

Early adopters of technology are the most likely to be comfortable with the creation of consumer profiles (32% somewhat comfortable or very comfortable), which compares with 17% of later adopters. Those who don't trust the social media industry are far more likely to be uncomfortable with the creation of consumer profiles (67%) than those who do (26%).



Half of Australians (55%) are uncomfortable with businesses creating a profile based on data collected about them

Figure 16: Levels of comfort of Australians with business use of data



B15. How comfortable or uncomfortable are you with …? Base: Australians 18+ (n=1,506)

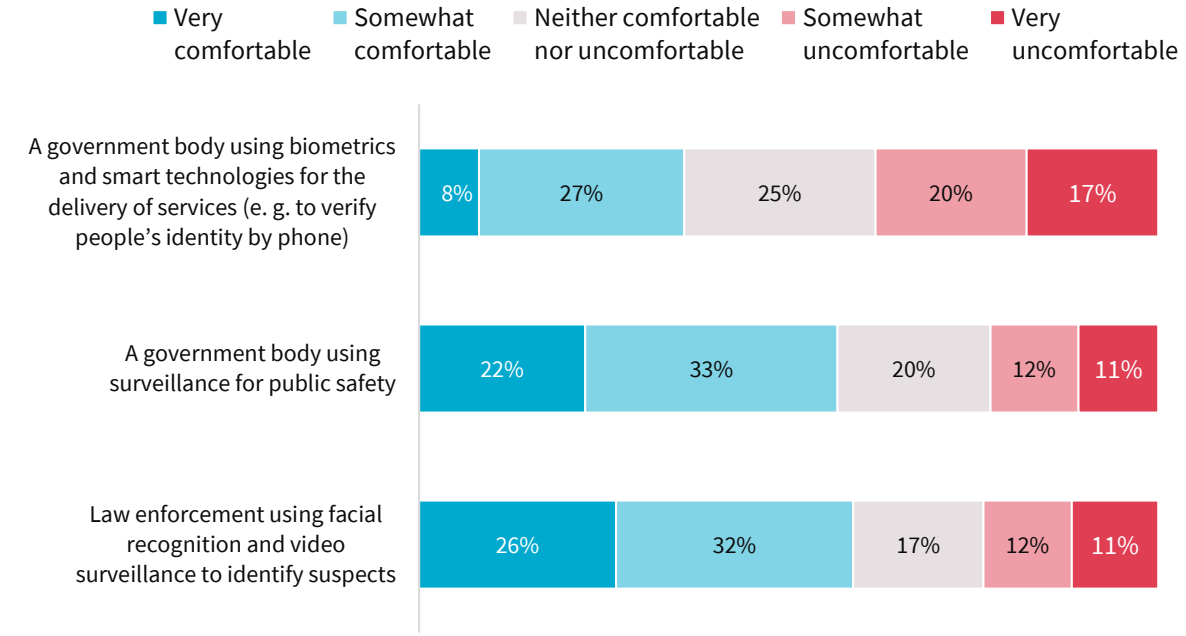
Government use of personal information

Government use of personal data is much less likely to make Australians uncomfortable. Of the data practices listed, Australians are just as likely to be comfortable (37%) as uncomfortable (34%) with a government body using biometrics and smart technologies for the delivery of services (for example, to verify people's identity by phone).

The majority of Australians are more likely to be generally comfortable with other practices, such as law enforcement using facial recognition and video surveillance to identify suspects (58% are comfortable, 23% uncomfortable) and a government body using surveillance for public safety (56% are comfortable, 22% uncomfortable).

Those most concerned about their privacy are more likely to be uncomfortable with these practices than average. Twenty-seven percent of those for whom protecting personal information is a major concern in life are uncomfortable with law enforcement using facial recognition, 26% with surveillance for public safety and 38% with the use of biometrics to deliver services.

Figure 17: Levels of comfort of Australians with government bodies/law enforcement using data

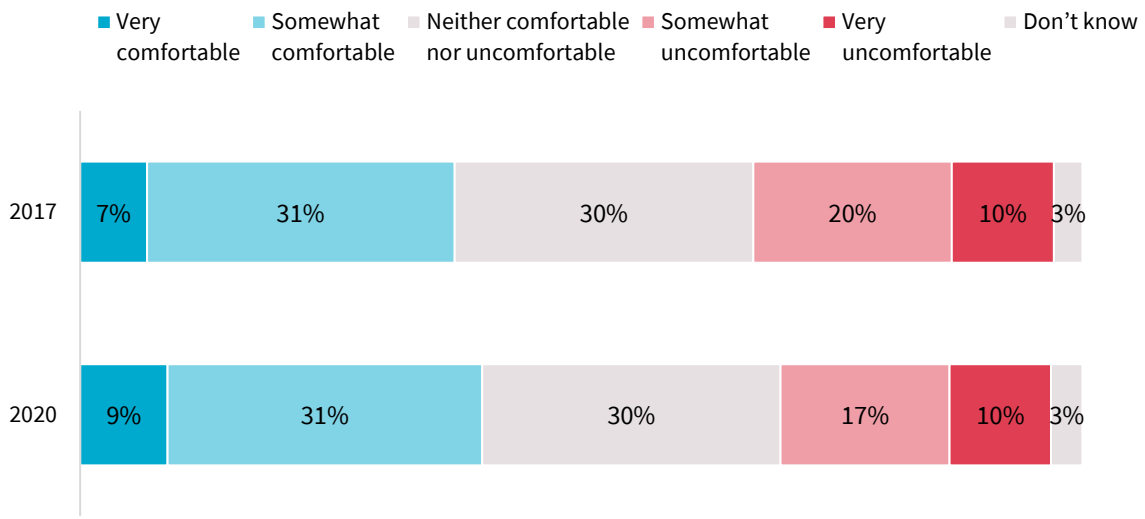


B15. How comfortable or uncomfortable are you with …? Base: Australians 18+ (n=1,506)

Government use of personal information for research purposes and policy development

When it comes to a government agency using the personal information that was provided to them for research or service and policy development, 40% of Australians are comfortable with this and 27% are not. This result is generally consistent with the 2017 survey (up 2% comfortable and down 3% uncomfortable).

Figure 18: Comfort with personal information provided to government agencies and departments being used for research, service development or policy development purposes



B16_2020 / Q11_2020. How comfortable or uncomfortable would you be with the personal information that you've provided to government agencies and departments being used for research, service development or policy development purposes? Base: 2020 (n=1,506)/ 2017 (n=704)

What Australians consider a misuse of personal information

The vast majority of Australians (between 72% and 84%) consider all of the data practices measured to be a misuse of their personal information. Among the most likely practices to be considered a misuse (84%) is an organisation using personal information in ways that cause harm, loss or distress.

More than 4 in 5 Australians (84%) consider supplying information to an organisation for a specific purpose and the organisation using it for another purpose to be misuse.

A similar percentage (81%) consider an organisation asking them for personal information that doesn't seem relevant to the purpose of the transaction and recording information on the websites they visit without their knowledge to be a misuse. This is particularly the case if the tracking of online activity leads to the price of a good or service being varied (79%).

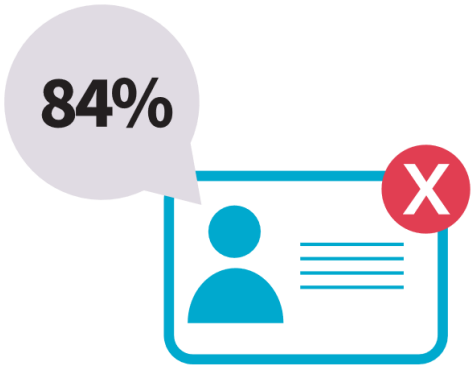
Seventy-nine percent of Australians consider an organisation inferring information about them (for example, sexual orientation, mental health, political views) based on what they do online to be misuse.

Eighty-three percent of Australians feel their personal devices listening to their conversations and sharing data with other organisations without their knowledge is misuse, as well as an organisation collecting information about them in ways that they would not expect (for example, an app scanning information about other apps used on a phone). Unexpected collection of information is most likely to be considered a misuse by those aged 50 and over (88%).

Australians are just as likely to feel an organisation revealing their information to other customers is a misuse (83%) as an organisation revealing their information to other organisations (82%). Older Australians, aged 50 and over, are the most likely to feel both practices are a misuse. Ninety-two percent consider revealing their information to other customers a misuse, while 90% consider an organisation revealing their information to other organisations a misuse.

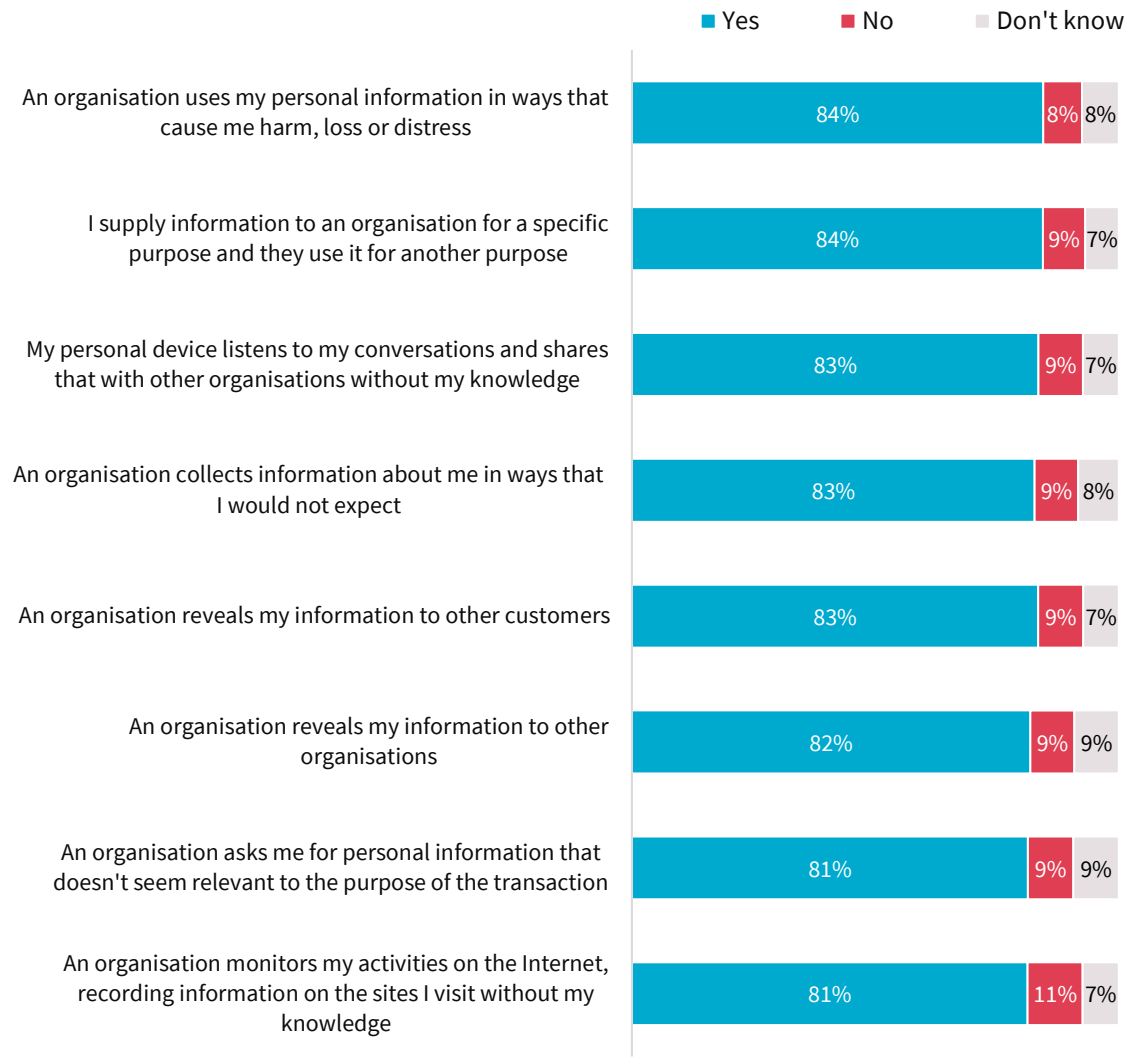
In contrast, only 73% of those aged 18-34 consider an organisation revealing their information to other customers a misuse and 74% aged 18-34 consider an organisation revealing their information to other organisations to be a misuse.

Early adopters of new technology are the least likely (74%) to consider sharing information with other organisations to be a misuse of personal information, compared with 84% of later adopters.



84% regard their personal information being used for other than the purpose or manner it was collected, or revealed to others is a misuse

Figure 19: Australians' beliefs that each data practice is a misuse

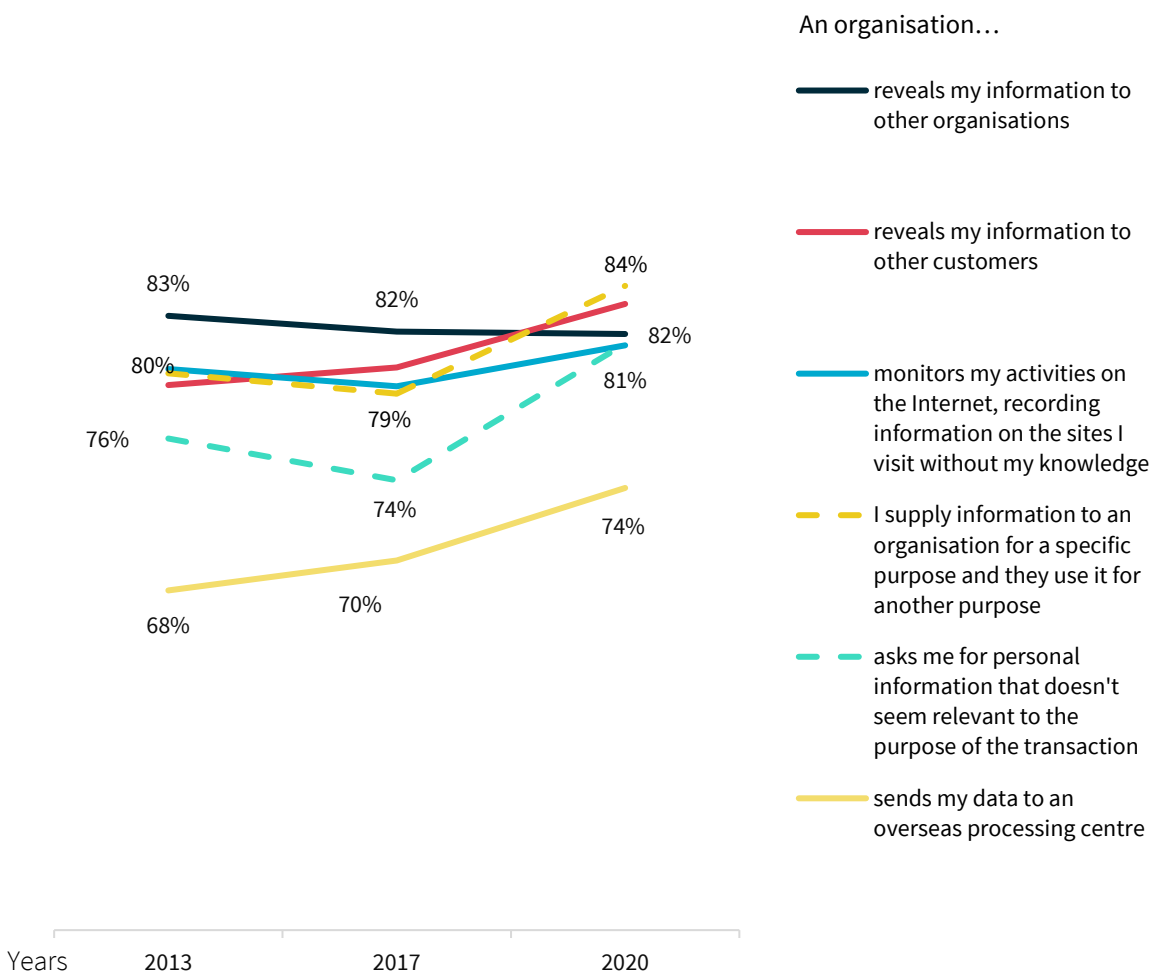


B9/B10/B11/B12. B9. Thinking now about the way that your personal information is handled by private or public sector organisations, which of the following instances would you regard to be a misuse of your personal information? Base: Australians 18+ (n=1,506)

Compared to 2017, for the elements measured in both years, Australians are now more likely to consider each data practice a misuse of their personal information. The biggest increase is for an organisation asking for information that doesn't seem relevant to the purpose of the transaction (up 7%), followed by supplying information to an organisation for a specific purpose that is used for another purpose (up 5%).

Although less likely to be seen as a misuse, there is a strong upward trend for 'sends my data to an overseas processing centre'.

Figure 20: Proportion of Australians who consider each data practice is a misuse 2013-2020



B9/B10/B11_2020. Thinking now about the way that your personal information is handled by private or public sector organisations, which of the following instances would you regard to be a misuse of your personal information? Base: Australians 18+ (n=950).
Q12_2017. Which of the following instances would you regard to be a misuse of your personal information? (n=632)

Note: "An organisation reveals my information to other organisations" label in the 2020 ACAPS was previously labelled "An organisation that you haven't dealt with gets hold of your personal information".

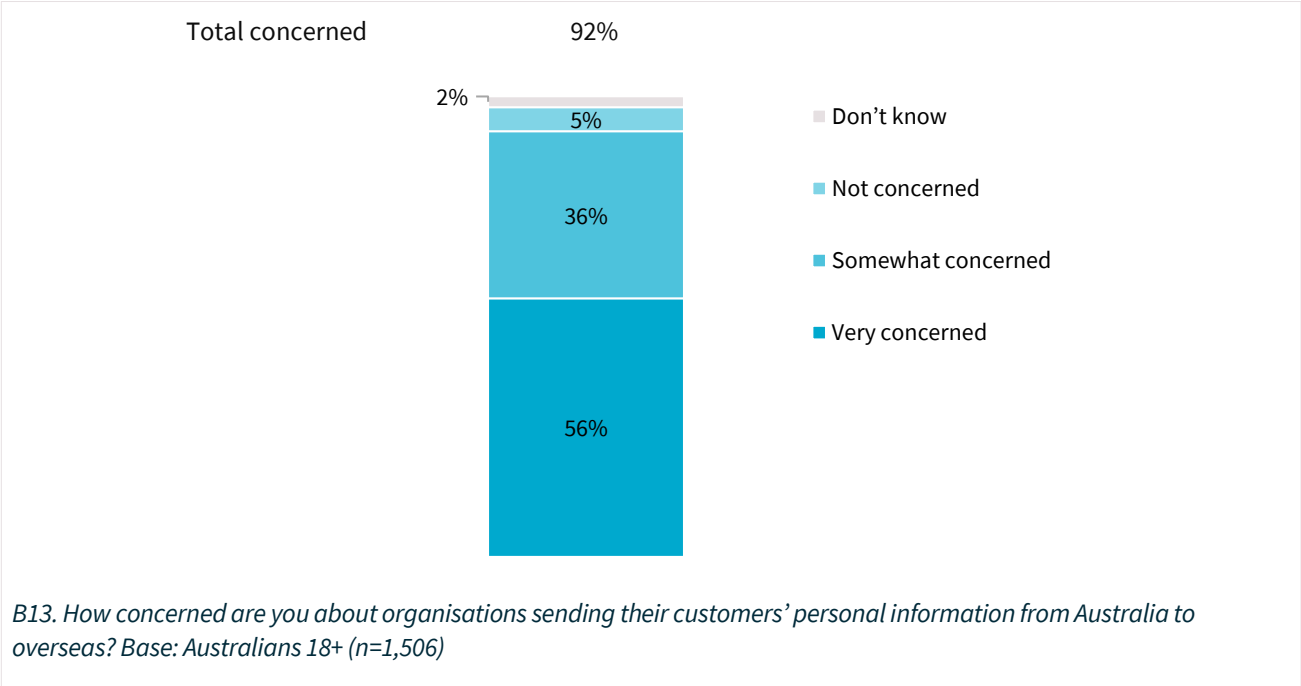
Sending data overseas

Three-quarters of Australians (74%) consider an organisation sending consumers' data to an overseas processing centre to be a misuse of personal information. This is a lower level of concern than for other data practices listed. Fewer Australians consider this practice a misuse than all other practices listed, with the exception of employers requesting access to social media accounts from their employees (72%).

Forty-one percent of Australians believe that sending information overseas is one of the biggest privacy risks people face today. Fifty-six percent of Australians are very concerned about organisations sending their customers' personal information from Australia to overseas. In total, 92% of Australians are somewhat to very concerned about this practice. Australians were just as concerned about this in 2017 (92% concerned) as they are in 2020.

Although older Australians are most likely to feel concerned about this (96%), 4 in 5 (79%) of those 18 to 24 years are concerned.

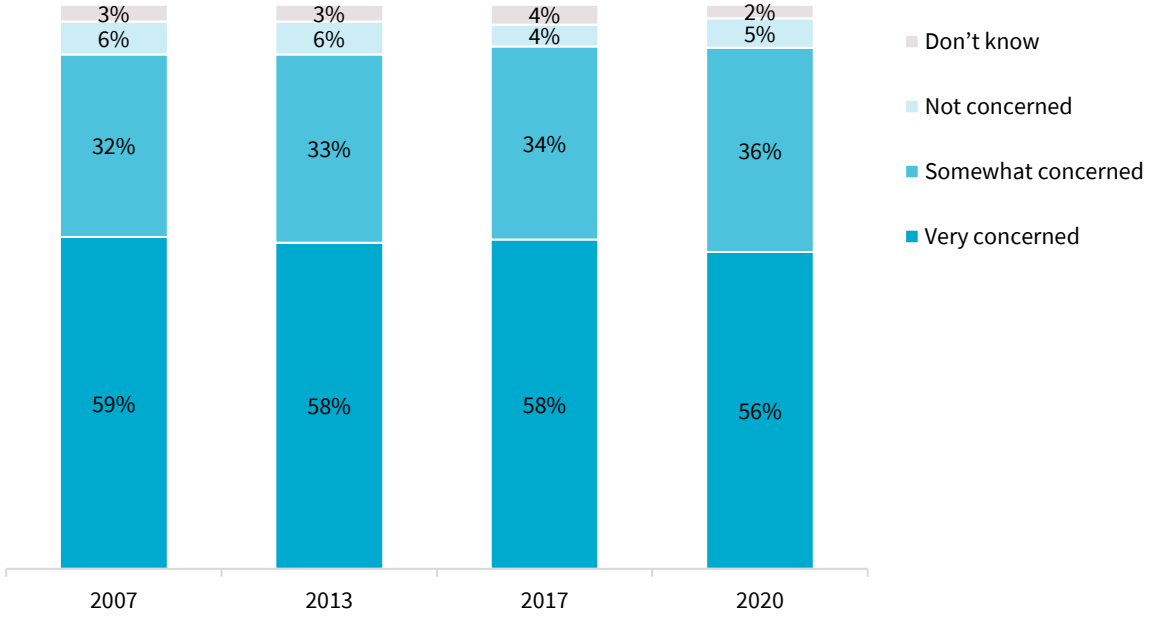
Figure 21: Concerns of Australians regarding their personal information being sent overseas



B13. How concerned are you about organisations sending their customers' personal information from Australia to overseas? Base: Australians 18+ (n=1,506)

Despite an increasing proportion of Australians considering their personal information being sent to an overseas processing centre to be a misuse, Australians are no more concerned about this now than they were in 2007.

Figure 22: Concerns of Australians regarding their personal information being sent overseas



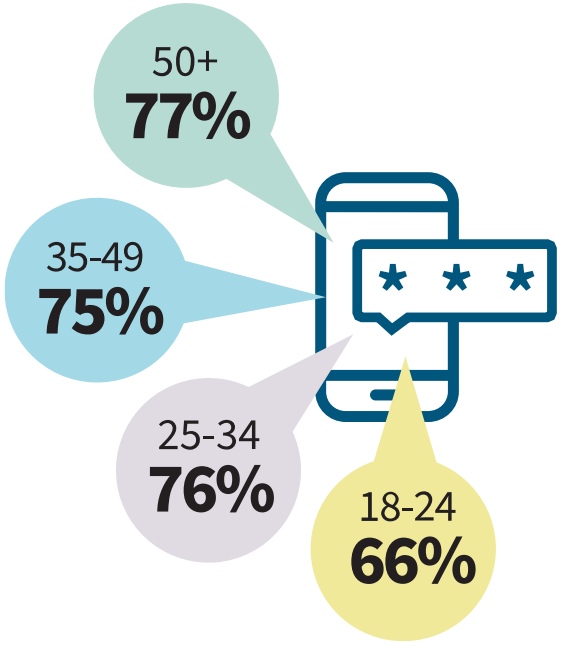
B13. How concerned are you about organisations sending their customers' personal information from Australia to overseas? Base: Australians 18+ (n=1,506)

Likelihood to take action to protect one's privacy

Three-quarters (75%) of Australians care enough about the protection of their personal information to 'actually do something about it' and only 30% believe it is too much effort to protect the privacy of their data (cf. 42% disagree). The belief that it's too much effort is highest among older Australians, aged 50 and over (77%).

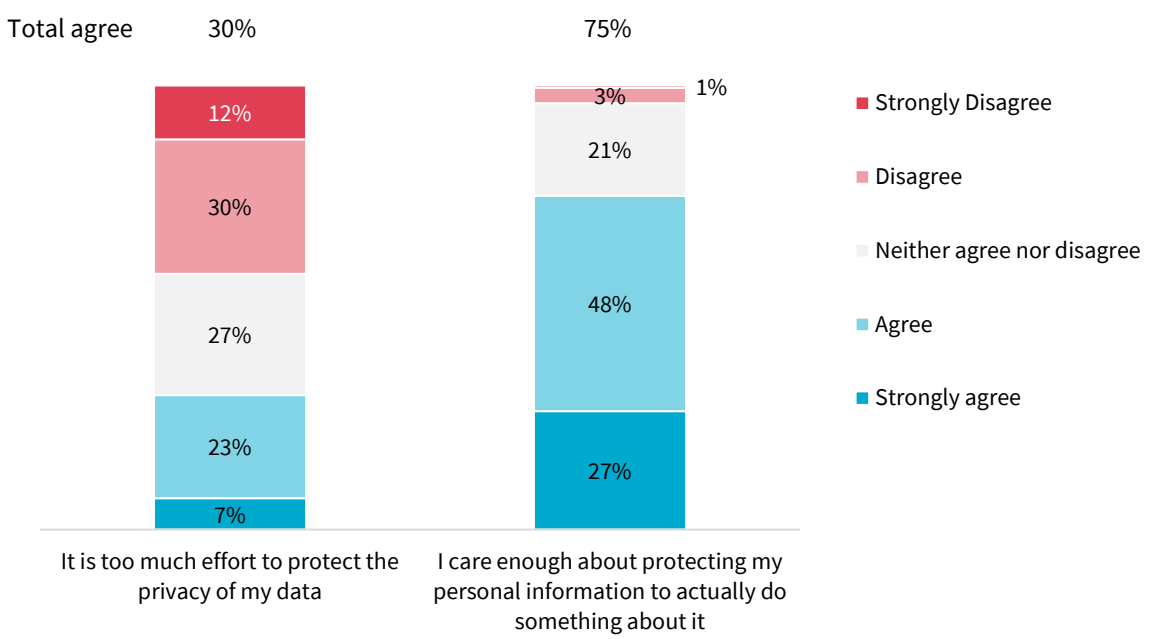
Younger Australians are less likely to care enough to take action to protect the privacy of their information and are more likely to agree it is too much effort to protect the privacy of their data.

Early adopters are more likely to strongly agree that they care enough about protecting their personal information to actually do something about it (38%; cf. average 27%).



Care enough to take action to protect their privacy

Figure 23: Australians' beliefs about protecting their data



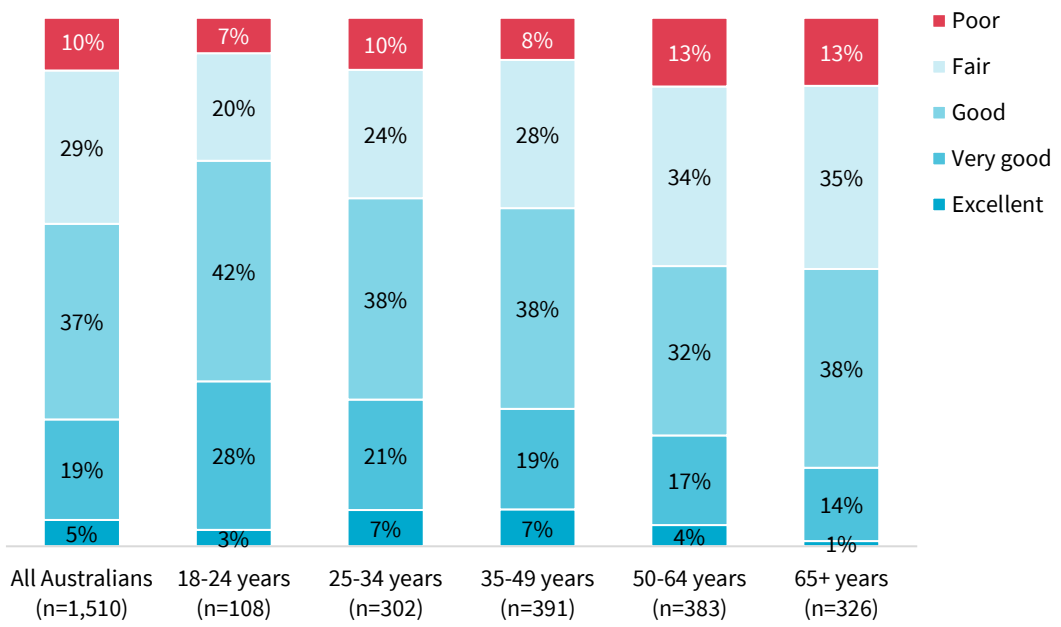
A7_3. Thinking about data privacy, to what extent do you agree or disagree with each of the following statements?
Base: Australians 18+ (n=1,506)

Australians' levels of knowledge about privacy

Almost a quarter (23%) of Australians rate their levels of knowledge about privacy as excellent or very good, whereas 40% rate their knowledge as fair to poor. There is a strong correlation by age, with younger Australians aged 18-34 more likely to rate their knowledge as excellent or very good (29%). Older Australians are less likely to rate their knowledge as excellent or good, with 25% of those aged 35-49, 21% of those aged 50-64 and 15% of those aged 65+ doing so.

Early adopters of technology are far more likely to rate their knowledge as excellent or very good (53%), compared with 23% of all Australians.

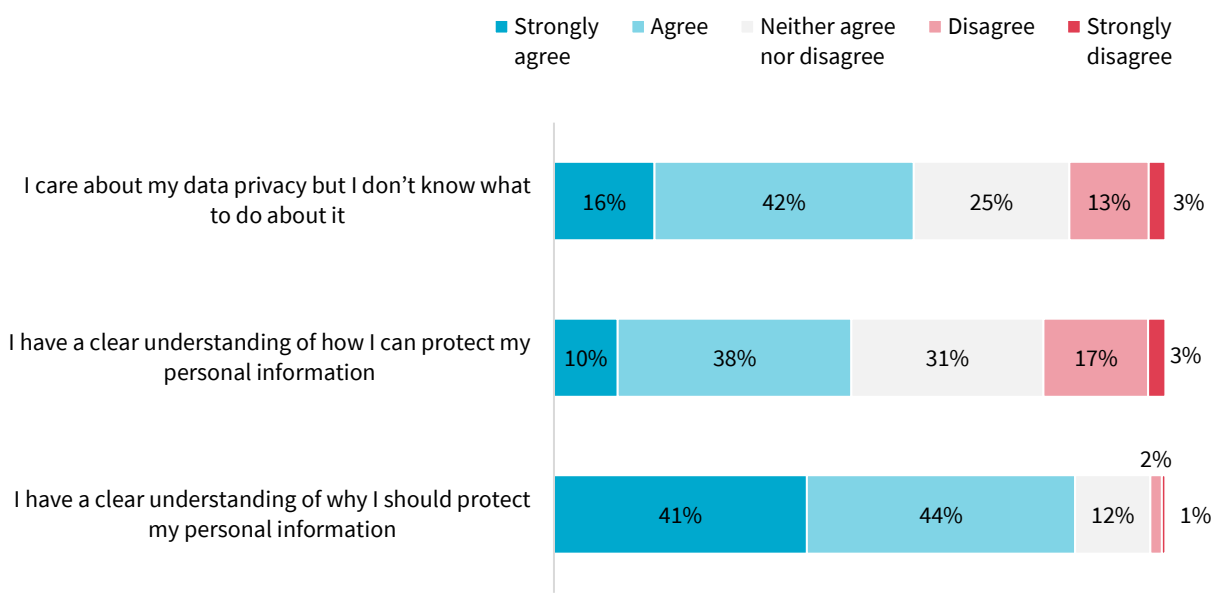
Figure 24: Australians' knowledge of data protection and privacy rights



A4. Before today, how would you rate your knowledge of data protection and privacy rights? Base: Australians 18+ (n=1,510)

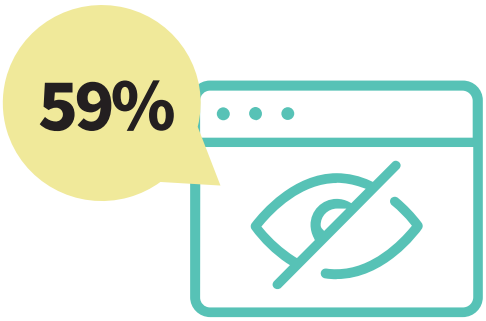
Australians have a very strong understanding of why they should protect their personal information (85% agree) but are less sure how they can do this (49% agree). Three in 5 (59%) care about data privacy, but don't know what to do about it.

Figure 25: Australians' beliefs on protecting their personal information



A7. Thinking about data privacy, to what extent do you agree or disagree with each of the following statements? Base: Australians 18+ (n=1,510)

Younger Australians (18-34) are more likely to know how to protect their personal information (54%), as are early adopters (72%). Less than half (47%) of later adopters know how to protect their personal information. Similarly, 51% of those aged 35-49 feel they know how to protect their personal information and only 2 in 5 (43%) of those aged 50 and over feel the same way.



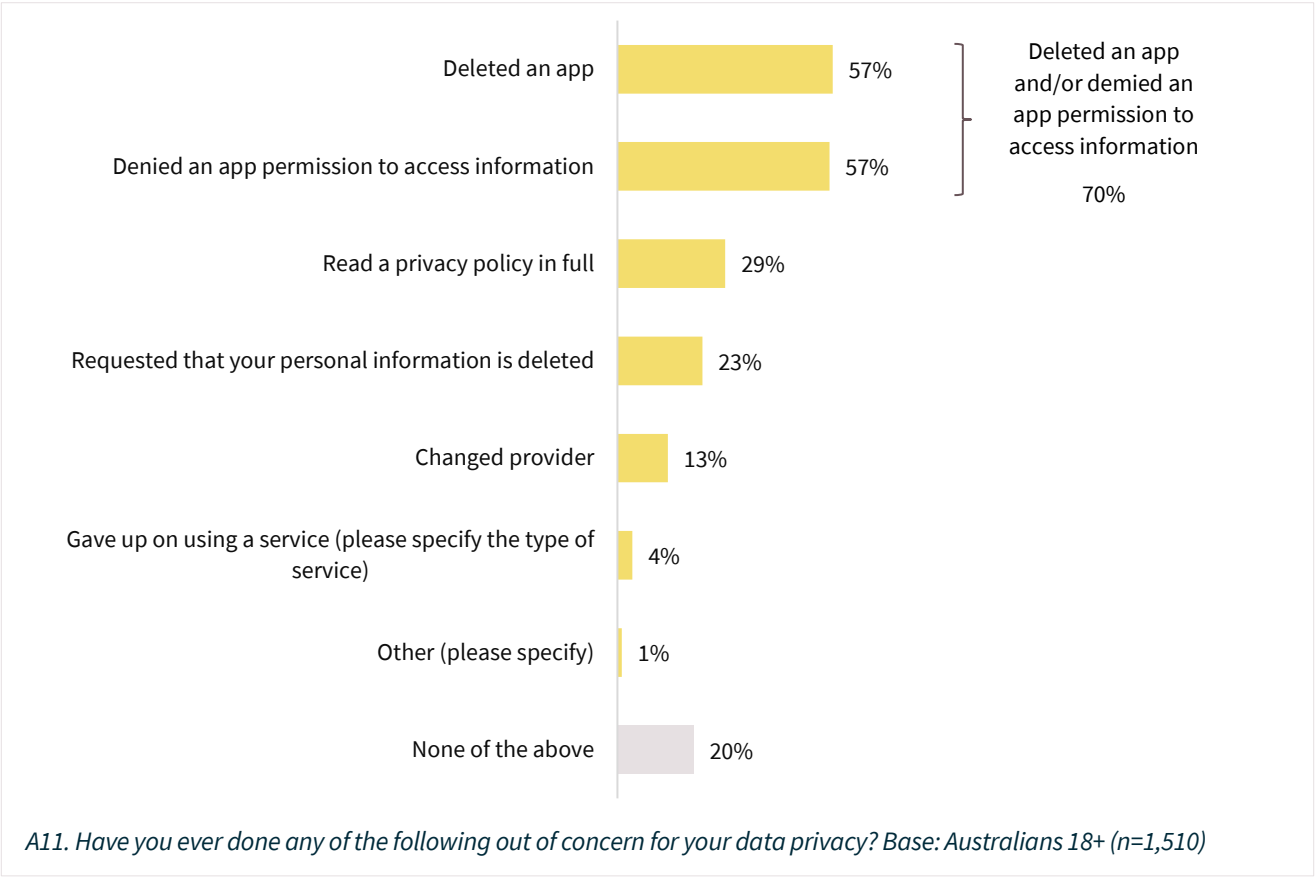
59% care about data privacy but don't know what to do about it

Actions Australians are taking to protect their privacy

Although 3 in 5 Australians say they are unsure about how to protect their privacy, many are already undertaking a range of data protection activities. At some point, 57% of Australians have deleted an app and another 57% have denied an app permission to access information. In total, 70% of Australians have done either or both. Other privacy protection measures Australians have taken include reading a privacy policy in full (29% of Australians have done this), requesting that their personal information is deleted (23% of Australians have done this) and changing provider (13% of Australians have done this).

Younger Australians are the most likely to have changed provider (17% of 18-34-year-olds have done so), as opposed to 12% among other Australians. Older Australians are the most likely to have given up on using a service out of concern for their privacy with 6% of those aged 50 or over, as opposed to 2% among other Australians.

Figure 26: Actions taken by Australians out of concern for their data privacy

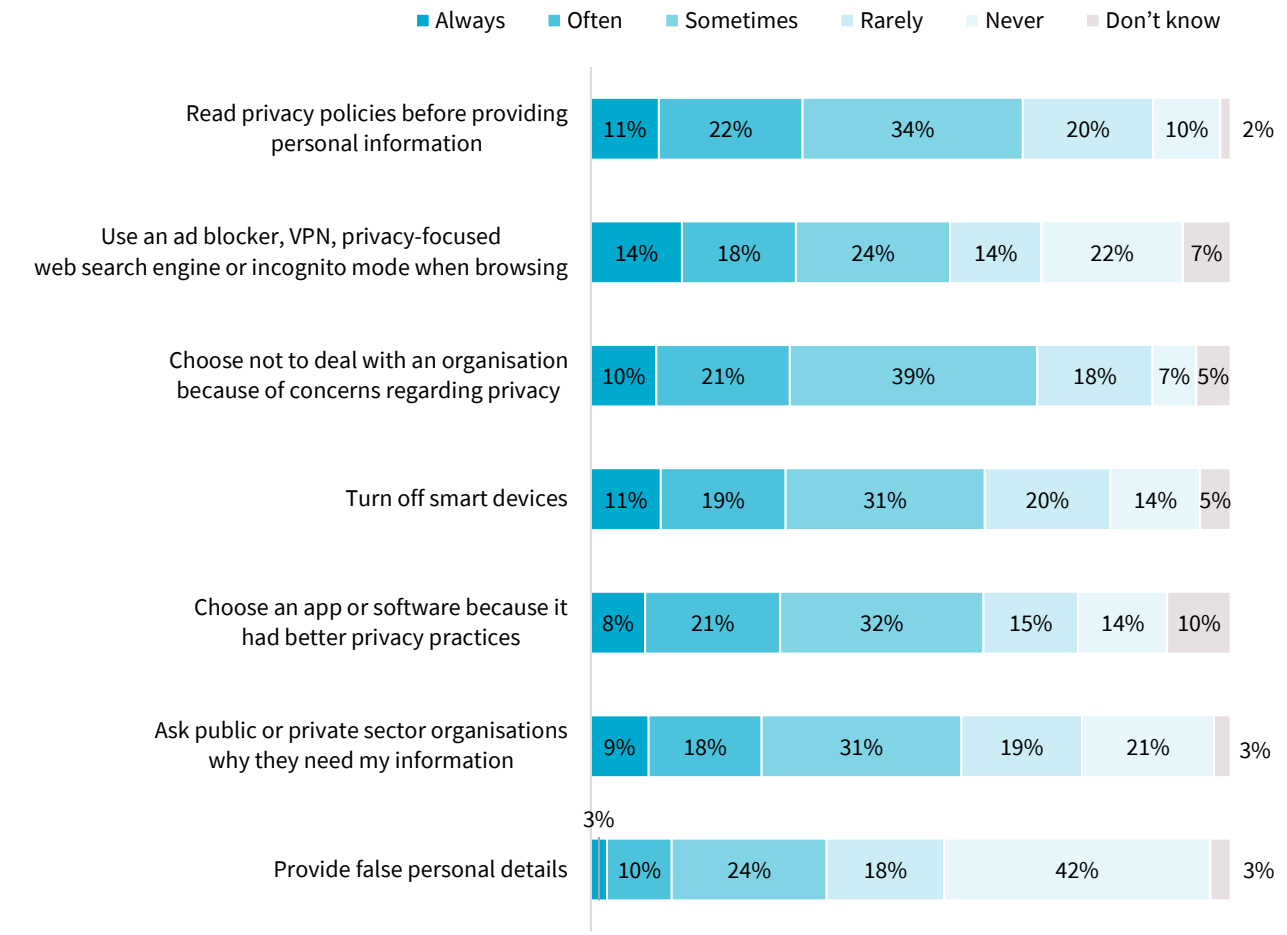


A11. Have you ever done any of the following out of concern for your data privacy? Base: Australians 18+ (n=1,510)

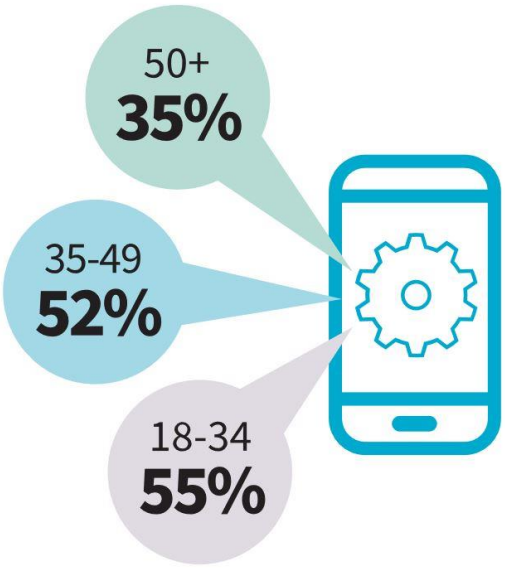
Over half of Australians often or always check that a website is secure before providing personal information (56%) and clear browsing and search history (51%). A significant minority often or always adjust privacy settings on a social networking website (46%), turn off GPS or location sharing on a mobile device (44%) and shred documents (41%).

Three in 10 or fewer often or always turn off smart devices (30%), choose an app or software because it had better privacy practices (30%), ask public or private sector organisations why they need their information (27%) or provide false personal details (13%).

Figure 27: Australians' participation in data protection activities



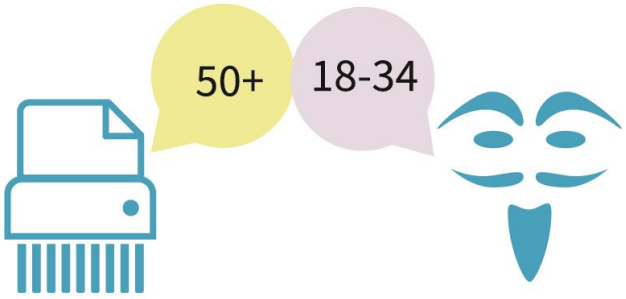
A12. How often do you participate in the following activities …? Base: Australians 18+ (n=1,510)



Younger Australians are more likely to adjust privacy settings on social networking websites

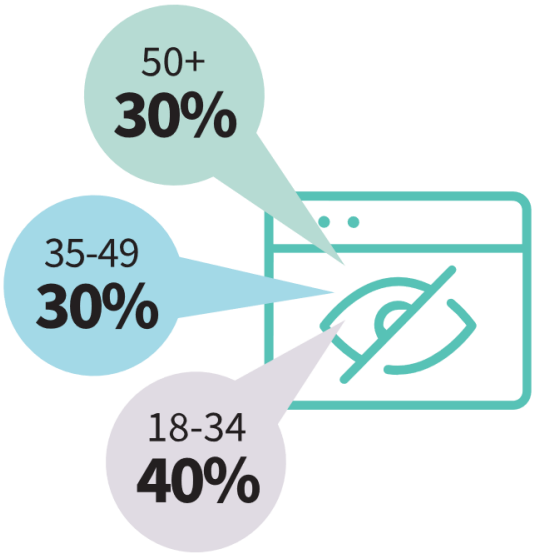
Older Australians aged 50 and over are significantly more likely than their younger counterparts to always or often shred documents (53%) and ask public or private sector organisations why they need their information (31%).

A third (32%) of Australians aged 35-49 reported that they often or always shred documents and a similar proportion of those aged 18-34 reported likewise (32%). Just under a quarter of those aged 35-49 (24%) and those aged 18-34 (24%) often or always ask public or private sector organisations why they need their information. Younger Australians aged 18-34 are the least likely to provide false personal details (25%).



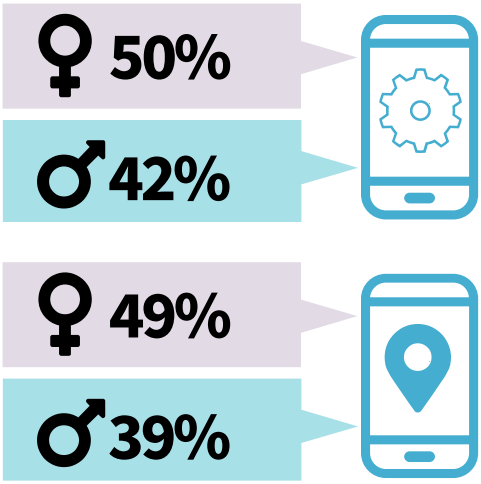
To protect their privacy, older Australians are more likely to shred documents and younger Australians are more likely to provide false information

Younger Australians are much more likely than their older counterparts to often or always use an ad blocker, VPN, privacy-focused web search engine or incognito mode when browsing (40%), or to adjust privacy settings on social networking websites (55%). Thirty percent of those aged 35-49 and 27% of those aged 50 and over always use an ad blocker, VPN or privacy-focused web search engine or incognito mode when browsing.



Younger Australians are more likely to often or always use an ad blocker, VPN, privacy-focused web search engine or incognito mode

Half of females (50%) often or always adjust privacy settings on social networking websites, while only 2 in 5 (42%) of males do likewise. Females are significantly more likely (49%) than males (39%) to 'often, or always turn off GPS or location sharing on mobile devices'. However, females are less likely (28%) than males (36%) to 'often, or always use an ad blocker, VPN, privacy-focused web search engine or incognito mode when browsing'. A quarter of females (25%) never use these tools.



Women are more likely than men to often or always adjust privacy settings on social media, turn off location sharing

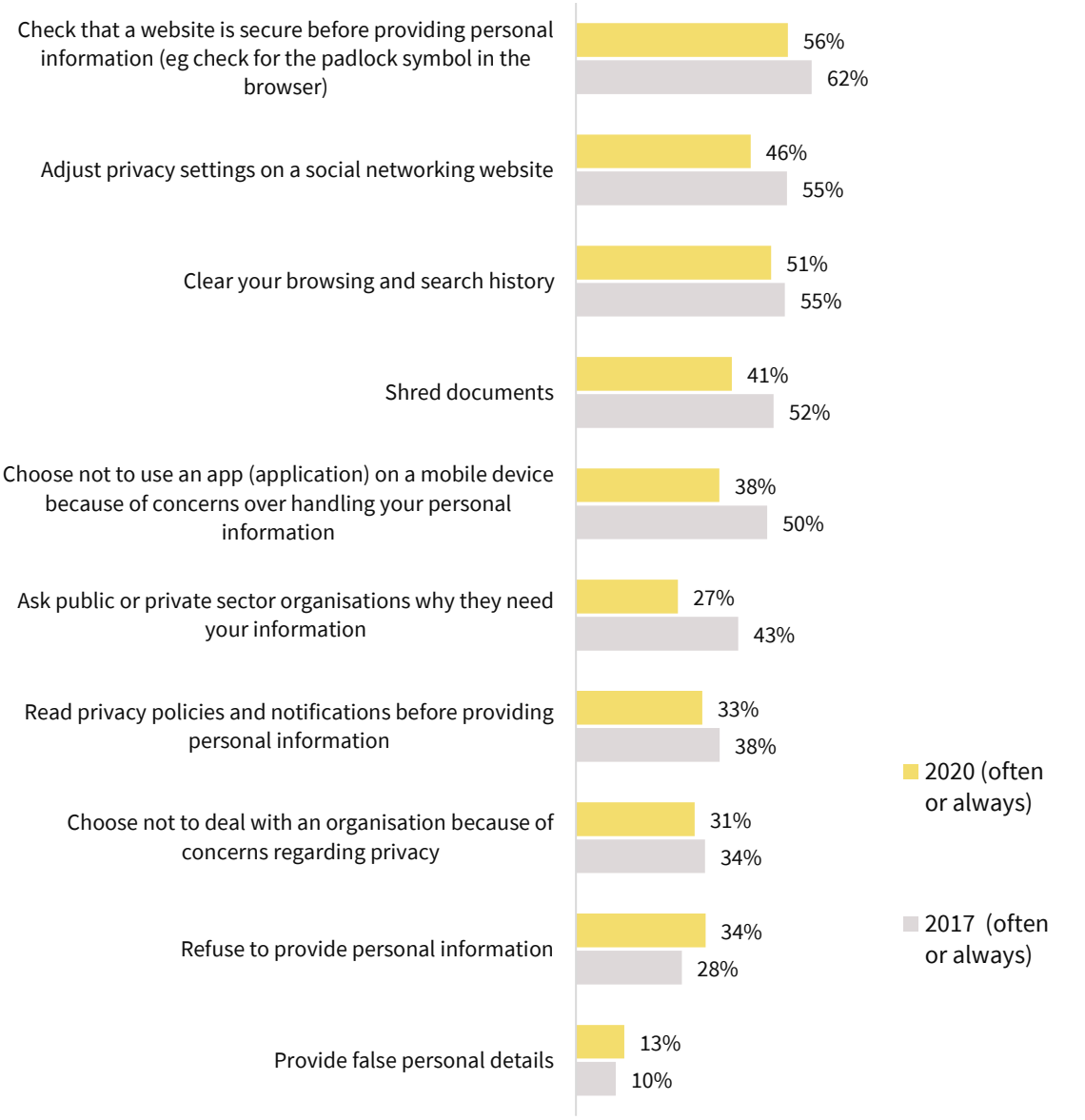
Early adopters of new technology are twice as likely (25%) compared to the national average (13%) to provide false personal information. Early adopters are also significantly more likely than the average Australian to always or often participate in the following activities to protect their privacy:

- turn off smart devices (53%), compared with a national average of 30%
- ask a public or private sector organisation why they need their information (42%), compared with a national average of 27%
- read privacy policies before providing personal information (49%), compared with a national average of 33%
- choose an app or software because it had better privacy practices (46%), compared with a national average of 30%
- adjust privacy settings on social networking websites (57%), compared with a national average of 46%, and
- choose not to deal with an organisation because of concerns regarding privacy (41%), compared with a national average of 31%.

Compared to 2017, Australians are less likely to take any of these measures often or always, with the exception of refusing to provide personal information (up 6%) and providing false personal details (up 3%).

The behaviours with the largest declines since 2017 are asking public or private sector organisations why they need your information (down 16%), choosing not to use an app on a mobile device because of concerns over handling your personal information (down 13%), shredding documents (down 11%) and adjusting privacy settings on a social networking website (down 10%).

Figure 28: Measures of protection of privacy always or often taken in 2017 and in 2020

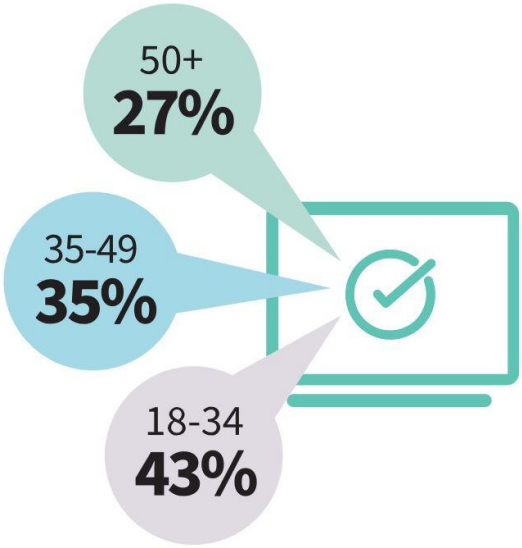


A12_2020. In order to protect your personal information how often do you ...? (n=1,150)
Q21_2017. The following questions are about things you might have done. To protect your personal information how often, if ever, do you? (n=717)

Levels of control over privacy

Almost 9 in 10 Australians (87%) want more control and choice over the collection and use of their personal information (2% do not). Currently, 1 in 3 Australians (34%) feel in control of their privacy, and 1 in 3 (34%) do not.

Older Australians are less likely to feel in control of their data privacy. A quarter (27%) of Australians aged 50 and over feel in control, as do 35% of those aged 35-49 and 43% of those aged 18-34. Early adopters (64%) are twice as likely as others (32%) to feel in control of their data privacy.



Younger people feel more in control of their data privacy than older people

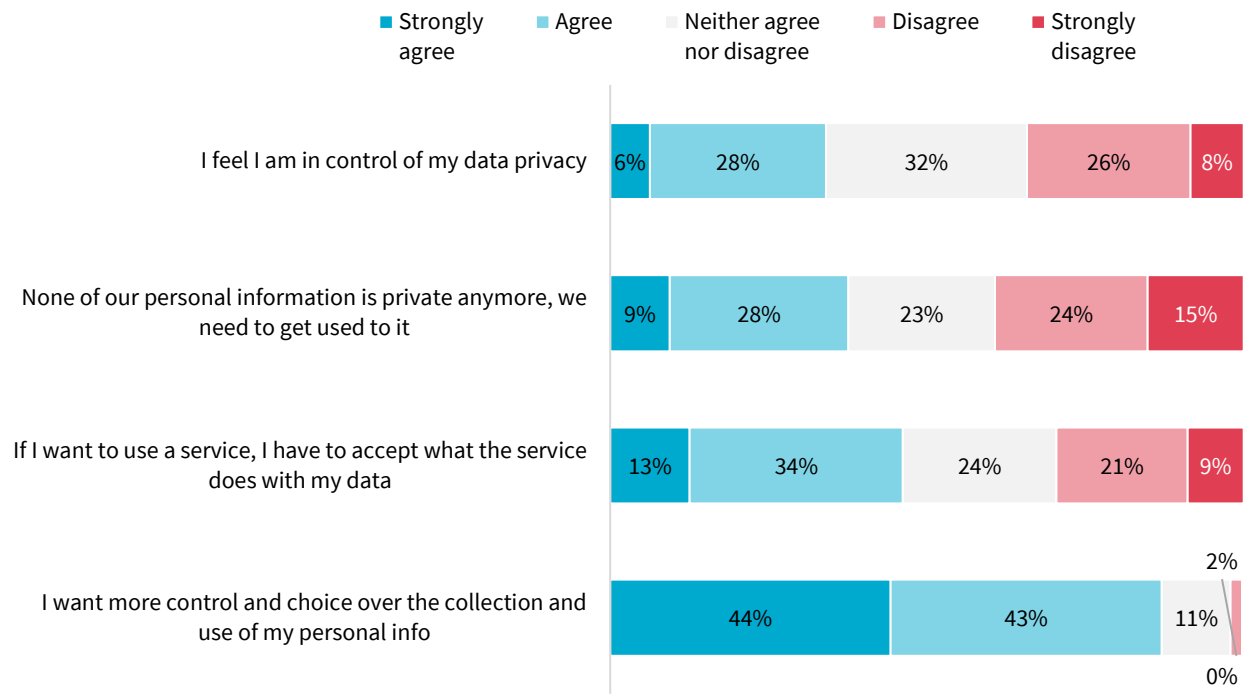
Almost half of Australians (46%) believe that if they want to use a service, they have to accept what the service does with their data (30% disagree).

Sentiment is divided on the statement 'none of our personal information is private anymore, we need to get used to it'. A similar proportion of Australians agree (38%) as disagree (39%). Younger Australians 18-34 are the most likely to agree with this statement (43%) and the least likely to disagree (27%).

However, younger Australians are also more likely to take control in the digital realm by adjusting settings on social media, using ad blockers, VPNs and privacy-focused web search engines or choosing an app or software because it has better privacy practices. However, they are less likely to shred documents or to ask public or private sector organisations why they need their information. This indicates that context is important, with younger Australians more likely to take control of their privacy in a digital environment, whereas older Australians are more likely to take control outside the digital realm.

A similar proportion of Australians agree (38%) as disagree (39%) with the statement that 'none of our personal information is private anymore, we need to get used to it'. Younger Australians 18-34 are the most likely to agree with this statement (43%) and the least likely to disagree (27%).

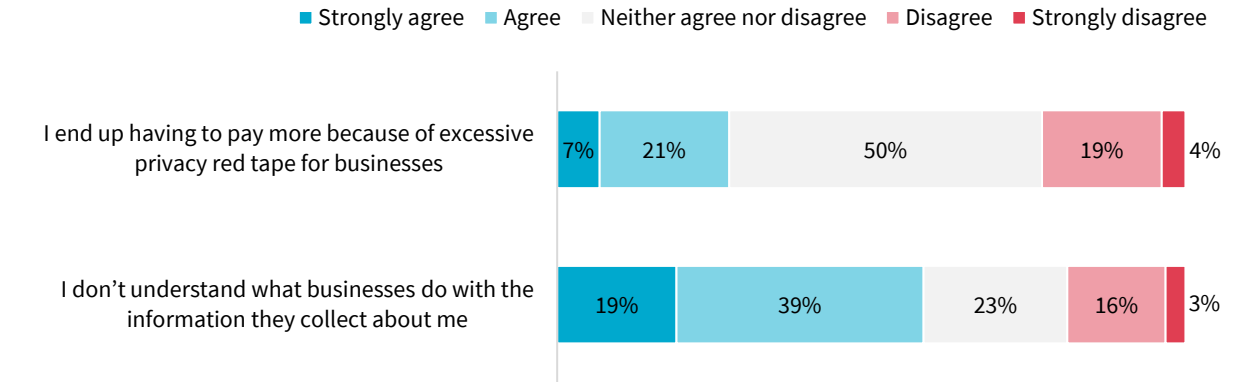
Figure 29: Australians' beliefs on data privacy



B2. Thinking about data privacy, to what extent do you agree or disagree with each of the following statements?
B6. Thinking about data privacy, do you agree or disagree with the following? Base: Australians 18+ (n=1,506)

Australians are also split as to whether or not privacy will end up costing them more due to excessive red tape for businesses: 27% agree with this sentiment, whereas 23% disagree. There is a strong gender split, with 33% of males believing they will end up paying more due to privacy, compared with 21% of females. The majority of Australians (58%) don't understand what businesses do with the information they collect about them.

Figure 30: Australians' beliefs about data privacy and businesses



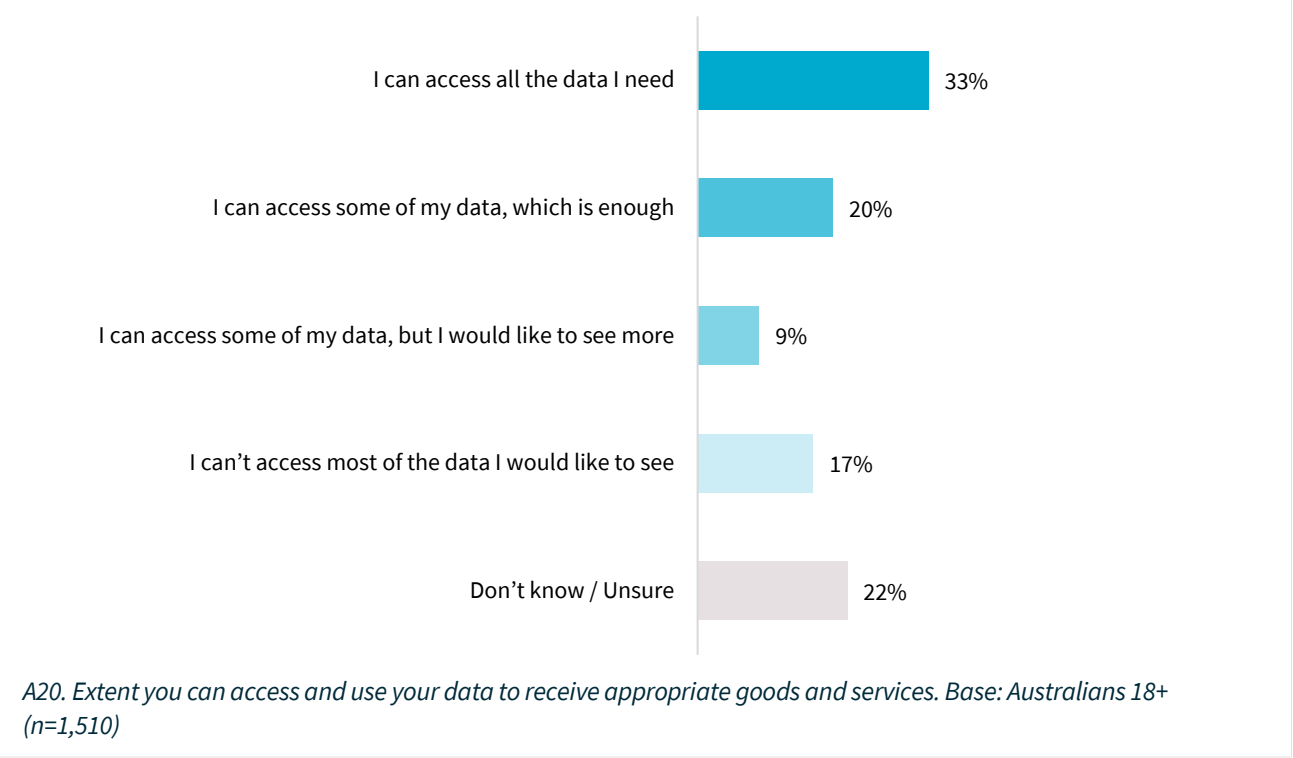
B6. Thinking about data privacy, do you agree or disagree with the following? Base: Australians 18+ (n=1,506)

Over half (53%) of Australians are satisfied with the amount of personal data they can access and use to receive appropriate goods and services, while a quarter (26%) are dissatisfied.

Younger Australians are more likely than their older counterparts to feel dissatisfied with the degree to which they can access personal data. A third (32%) of those aged 18-34 feel dissatisfied about this, while 31% of those aged 35-49 and only 17% of those aged 50 and over are dissatisfied with the degree to which they can access personal data.

Older Australians are the most likely to not know or be unsure about the extent to which they can access and use their personal data (26%). One in 5 (21%) of Australians aged 35-49 and 16% of Australians aged 18-34 do not know or are unsure about the extent to which they can access and use their personal data.

Figure 31: The extent to which Australians can access and use data



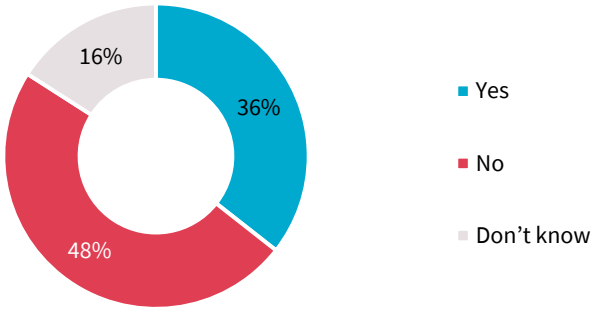
A20. Extent you can access and use your data to receive appropriate goods and services. Base: Australians 18+ (n=1,510)

Two-thirds (64%) of Australians are unaware that they can request access to their personal information from businesses and government agencies. Over half (53%) of Australians aged 18-34 years and late adopters of new technology (56%) are unaware that they can request to access their personal information from businesses and government agencies. This compares to 45% of those aged 35-49 years and 48% of those aged over 50. Early adopters (32%) are less likely to be unaware of this privacy right, as are those among the last (51%), middle (47%) and first (48%) to adopt technology.

Over half (53%) of Australians aged 18-34 years and late adopters of new technology (56%) are unaware that they can request to access their personal information from businesses and government agencies. This compares to 45% of those aged 35-49 years and 48% of those aged over 50. Early adopters (32%) are less likely to be unaware of this privacy right, as are those among the last (51%), middle (47%) and first (48%) to adopt technology.

Compared to 2017, the same proportion of Australians (36% in 2017) are aware that they can request access to their personal information held by businesses and government agencies.

Figure 32: Percentage of Australians who are aware they can request access to personal information



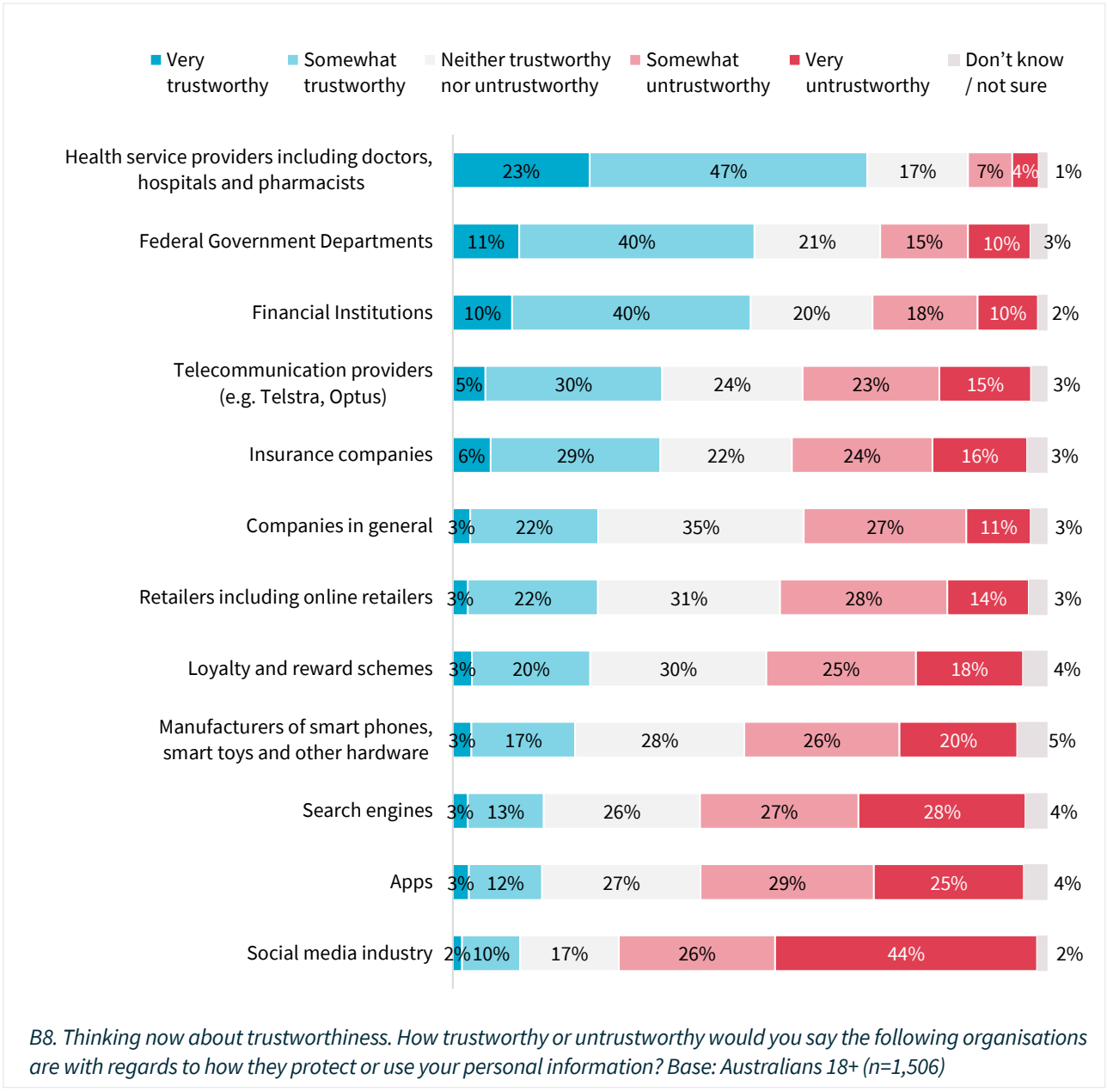
A23. Are you aware that you can request to access your personal information from businesses and government agencies? Base: Australians 18+ (n=1,510)

Trust in organisations

Half (49%) of Australians feel that most of the organisations they deal with are transparent about the way they use their personal information, while close to 1 in 5 (17%) do not.

Levels of trust in personal information handling vary substantially by organisation type. Australians consider the social media industry the most untrustworthy in how they protect or use their personal information (70% consider this industry untrustworthy), followed by search engines (55% untrustworthy) and apps (54% untrustworthy).

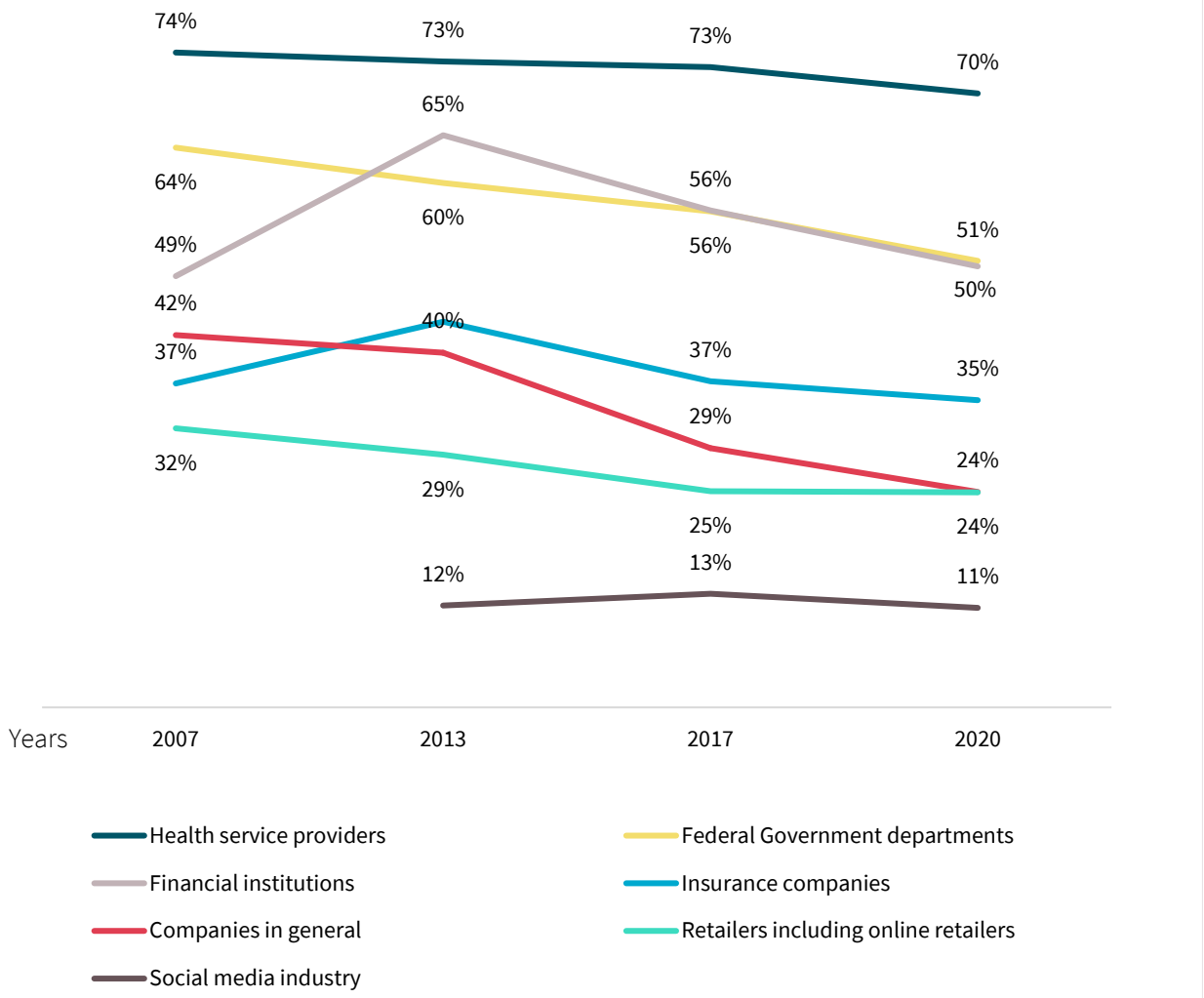
Figure 33: Australians' beliefs on how trustworthy organisations are with personal information



B8. Thinking now about trustworthiness. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information? Base: Australians 18+ (n=1,506)

Since 2007, there has been a general downward trend in trust in most of the categories presented. Trust in companies in general is down by 13%. Trust in Federal Government departments is down 14%, with a steady decline in trust over the past 13 years.

Figure 34: Proportion of Australians considering each organisation trustworthy from 2007 to 2020



B8_2020 / Q8_2017. Thinking now about trustworthiness. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information? Base: Australians 18+ (n=950)

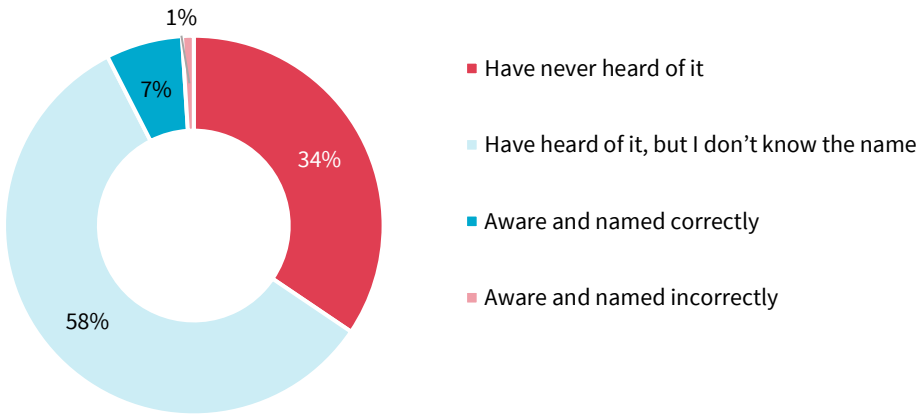
Part 2: Privacy legislation

Awareness of the Privacy Act

Only 7% of Australians could name the Privacy Act as the main law that promotes and protects the privacy of individuals in Australia on an unprompted basis. Fifty-eight percent of Australians have heard of it but didn't know its name and 1% named it incorrectly. A third (34%) cannot recall ever having heard the name of this law.

While the proportion of those who can name the Privacy Act is consistent across age groups, those who have never heard of it are more likely to be younger. Forty-three percent of those aged 18-34 have never heard of it, as have 34% of those aged 35-49 and 29% of those aged 50 and over. Conversely, those who have heard of it, but don't know the name, are likely to be older. Sixty-three percent of those aged 50 and over have heard of it but don't know the name, as have 59% of those aged 35-49 and 51% of those aged 18-34.

Figure 35: Percentage of Australians who are aware of the Privacy Act

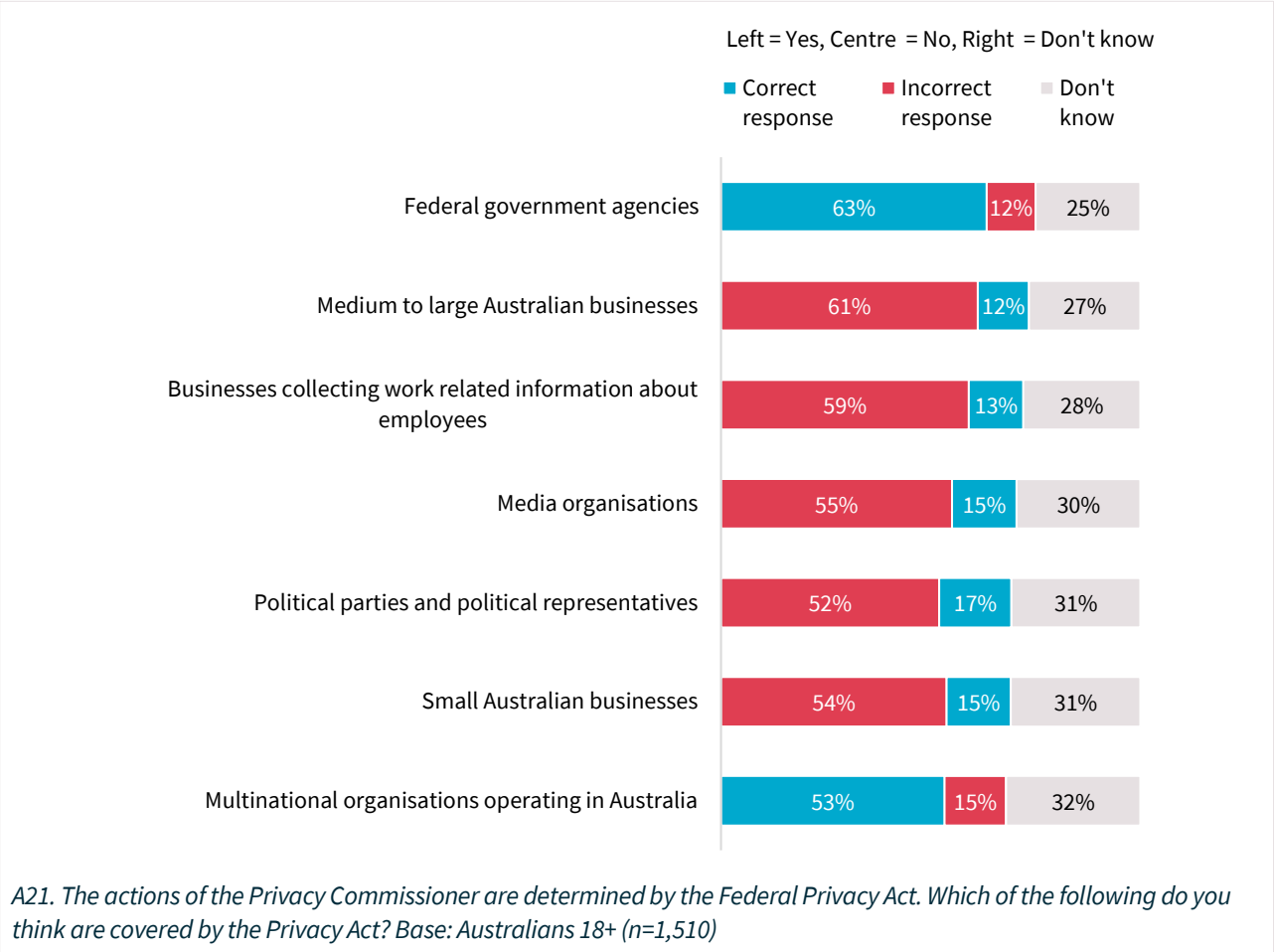


A5. Are you aware of the main law that promotes and protect the privacy of individuals in Australia? Base: Australians 18+ (n=1,510)

Awareness of organisation types covered by the Privacy Act

Australians have a limited understanding of which businesses are covered by the Privacy Act. Australian Government agencies, medium to large Australian businesses and multinational businesses operating in Australia are covered, whereas small businesses, political parties and representatives, media organisations and businesses recording work-related information about employees are not. The proportion correctly identifying organisation types that are covered ranged from 53% to 63%, whereas the proportion correctly identifying organisation types that are not covered ranged from 13% to 17%. The low proportion of people correctly identifying which business types are not covered is consistent with a population simply assuming that most businesses are covered.

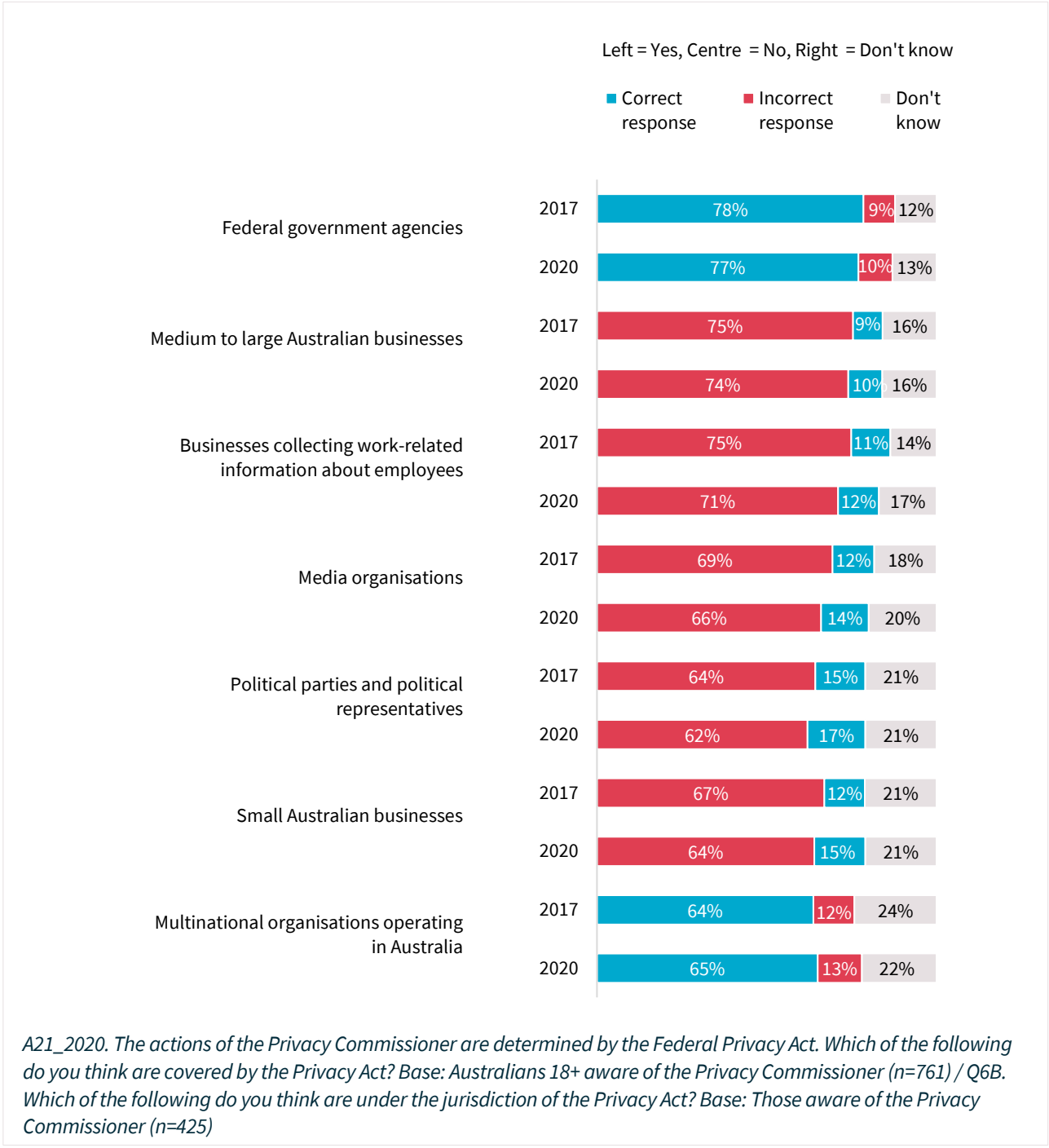
Figure 36: Awareness of sectors covered by the Privacy Act



A21. The actions of the Privacy Commissioner are determined by the Federal Privacy Act. Which of the following do you think are covered by the Privacy Act? Base: Australians 18+ (n=1,510)

In 2017, this question was only asked of Australians who were aware of the Privacy Commissioner. Among this cohort, a slightly higher proportion are aware in 2020 that political parties (17%) and small businesses (15%) are not covered by the Privacy Act – in 2017, 15% of those aware of the Privacy Commissioner knew that political parties were are not covered and 12% knew that small businesses are not covered.

Figure 37: Awareness of sectors covered by the Privacy Act in 2017 and 2020 – filtered to those aware of the Privacy Commissioner



A21_2020. The actions of the Privacy Commissioner are determined by the Federal Privacy Act. Which of the following do you think are covered by the Privacy Act? Base: Australians 18+ aware of the Privacy Commissioner (n=761) / Q6B. Which of the following do you think are under the jurisdiction of the Privacy Act? Base: Those aware of the Privacy Commissioner (n=425)

Organisations that should be covered by the Privacy Act

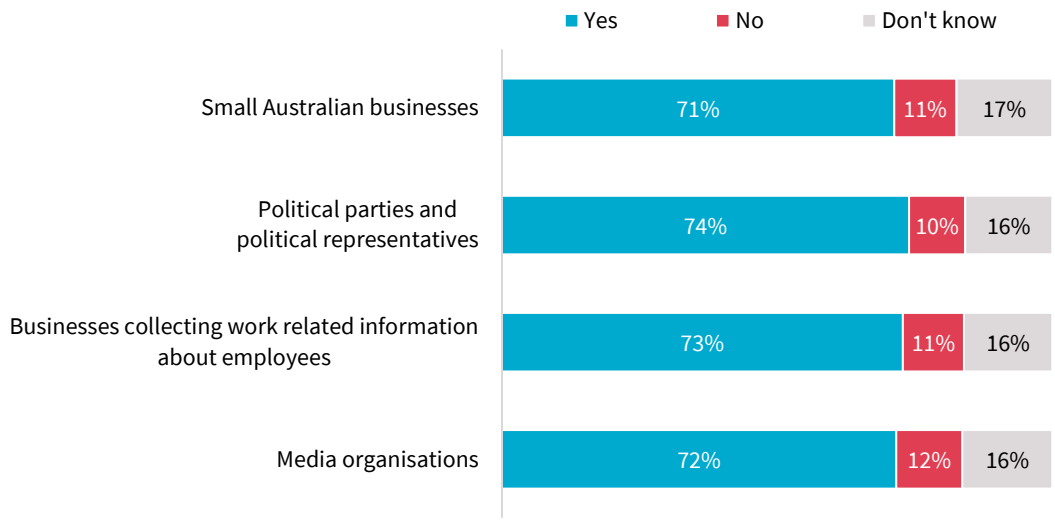
Almost three-quarters of Australians feel that each of the 4 exempt organisation types should be required to protect personal information in the same ways that government and larger businesses are required to. This desire for inclusion in the Privacy Act is equally high for each sector. Seventy-one percent think small Australian businesses should be included, 72% for media organisations, 73% for businesses collecting work-related information about employees and 74% for political parties and political representatives.

Australians who have a higher knowledge of data protection and privacy rights are more likely to think that some exempt sectors should remain exempt. This is especially true for small Australian businesses, with 28% of those with an excellent knowledge of data protection considering they should not be required to protect personal information in the same ways that government and larger businesses are required to (24% for media organisations, 23% for political parties and 13% for businesses collecting work-related information about employees).

Among those who knew that each of these sectors is not covered by the Privacy Act:

- 69% believe political parties and representatives should be covered
- 64% believe businesses collecting work-related information about employees should be covered
- 61% believe media organisations should be covered
- 58% believe small Australian businesses should be covered by the Privacy Act.

Figure 38: Belief that each sector should be covered by the Privacy Act



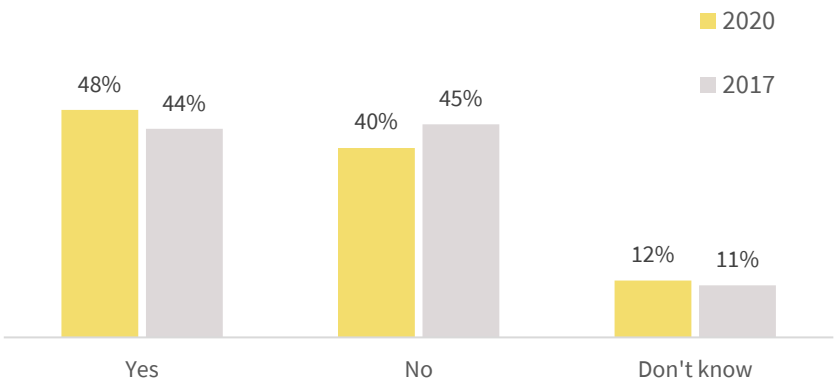
A22. The following sectors are currently exempt from the Privacy Act. Should they be required to protect your personal information in the same ways that government and larger businesses are required to? Base: Australians 18+ (n=1,510)

Awareness of the Privacy Commissioner

Awareness of the Privacy Commissioner was measured on a prompted basis. Half (48%) of Australians know about this role, which is an increase of 4% since 2017.

Australians aged 50 and over are much more likely to be aware of the Privacy Commissioner (55%) as well as Australians with a postgraduate or bachelor's degree (54%). Fewer than half (47%) of Australians aged 35-49 and just 2 in 5 (38%) of those aged 18-34 are aware of the Privacy Commissioner. Those with lower levels of education are less likely to be aware, with 52% of those with an undergraduate diploma, TAFE or trade certificate and 41% of those whose highest education level is up to Year 12 being aware of the Privacy Commissioner. Australians who are retired (54%) or working (51%) are also much more likely to be aware of the Privacy Commissioner than others. Just a third (34%) of students are aware of the Privacy Commissioner.

Figure 39: Awareness of the Privacy Commissioner over time



A6_2020. Are you aware that a Privacy Commissioner exists to uphold privacy laws and to investigate complaints concerning the misuse of personal information? Base: Australians 18+ (n=966)

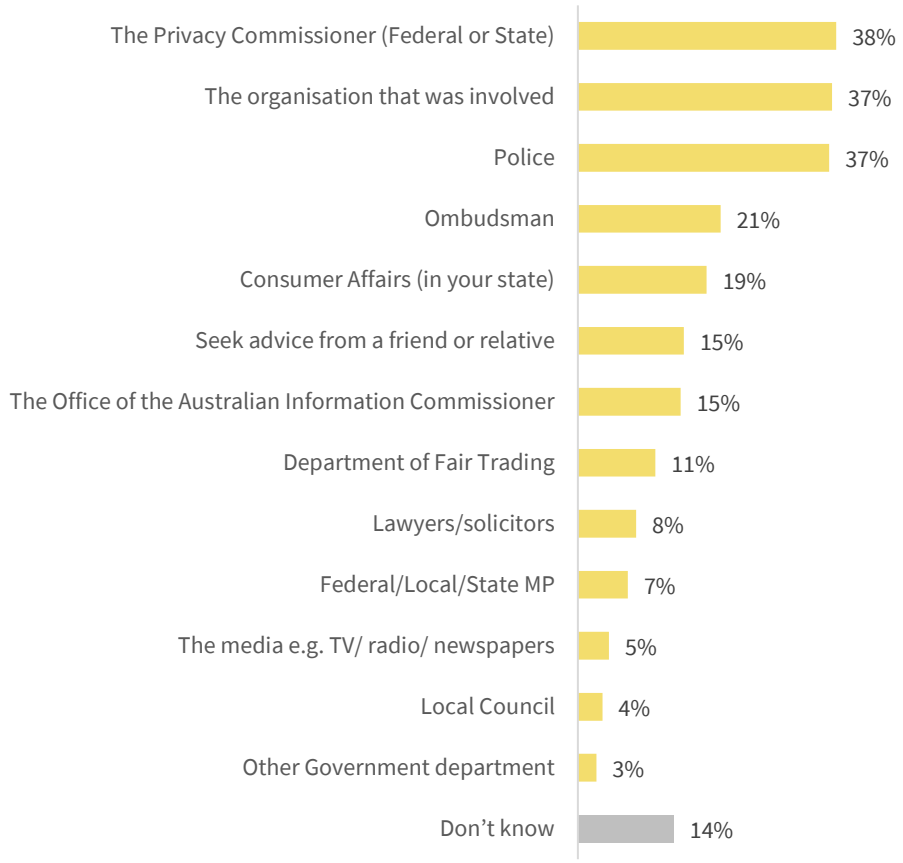
Q6_2017. Were you aware that an Australian Government Privacy Commissioner exists to uphold privacy laws and to investigate complaints concerning the misuse of personal information? Base: Australians 18+ (n=967)

Entity to whom Australians would report a misuse of privacy

Australians are just as likely to report a misuse of privacy to the police (37%) as the Privacy Commissioner (38%). Among those who are aware that the Privacy Commissioner exists to uphold privacy laws and to investigate complaints concerning the misuse of personal information, 54% would report a misuse to the Privacy Commissioner, well ahead of the police (36%). Conversely, among those previously not aware of the Privacy Commissioner, 22% would report a misuse to the Privacy Commissioner, 38% to the police.

Likelihood to report a misuse to the Privacy Commissioner also increases with knowledge of data protection. Forty-four percent of those with good or excellent knowledge would report a misuse to the Privacy Commissioner, while only 32% of those with fair to poor knowledge would do likewise. Older Australians, aged 50 and over, are more likely to have the Privacy Commissioner as a point of contact for information misuse (51%), whereas just 32% of those aged 35-49 and 25% of those aged 18-34 would report a misuse to the Privacy Commissioner.

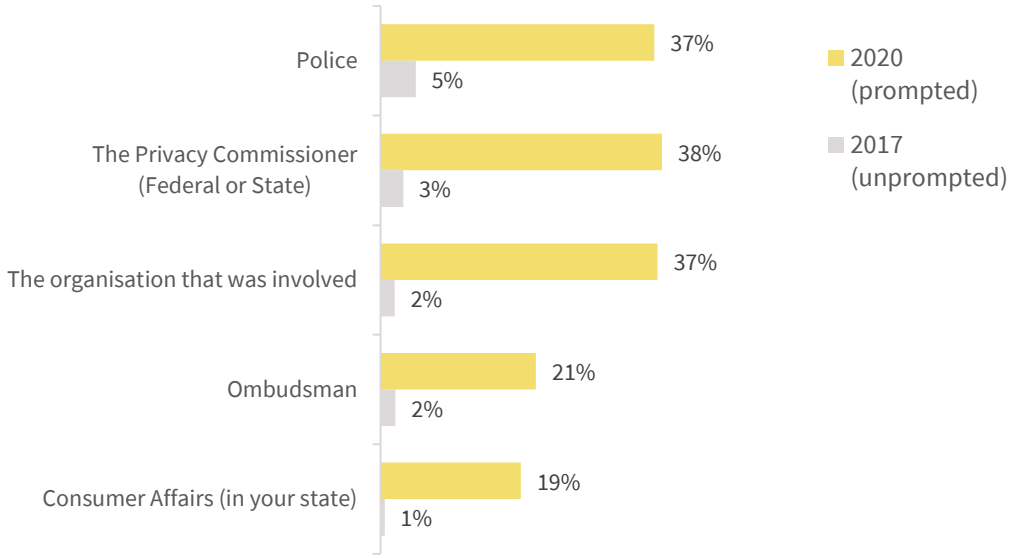
Figure 40: Australians' point of contact to report misuse of personal information



A10. If you wanted to report misuse of your personal information to someone, who would you be most likely to contact?
Base: Australians 18+ (n=1,510)

In 2017, this question was asked on an unprompted basis to ensure all relevant categories were uncovered. It changed to a prompted question in 2020. However, based on the relative numbers of people selecting each response, Australians are now more likely to report a misuse to a Privacy Commissioner than to the organisation that was involved or to the police.

Figure 41: Organisations people would report a misuse of personal information to in 2017 and 2020

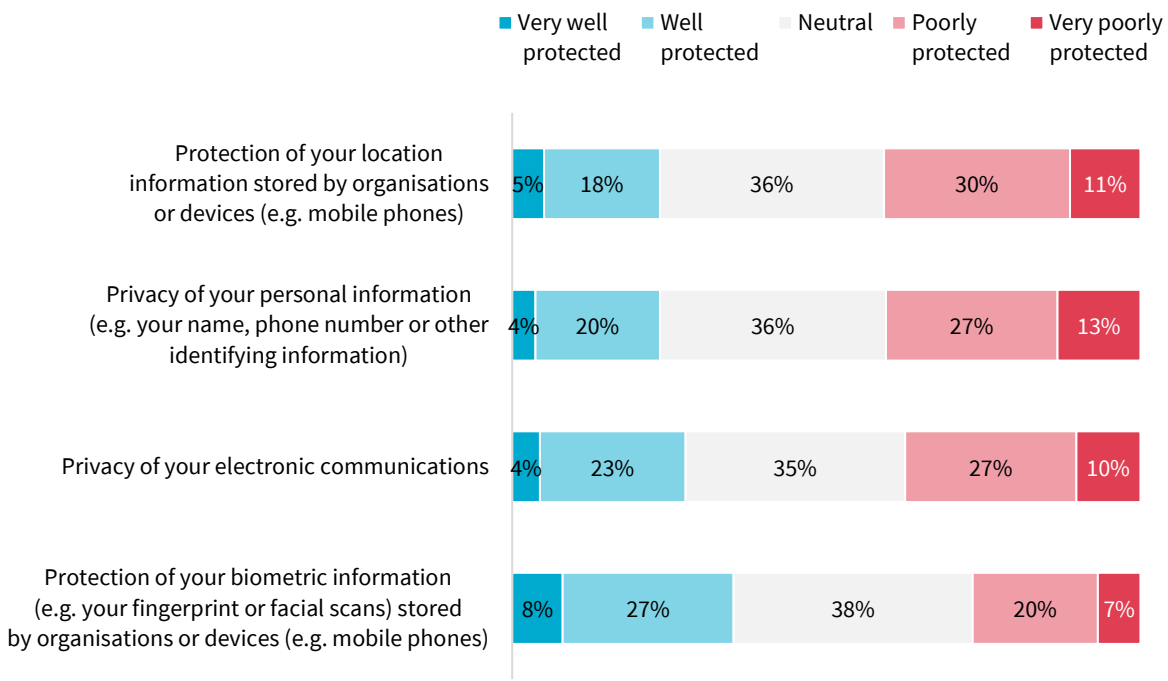


A10_2020 prompted. If you wanted to report misuse of your personal information to someone, who would you be most likely to contact? Base: Australians 18+ (n=964)
Q17_2017 unprompted. If you wanted to report misuse of your personal information to someone, who would you be most likely to contact? Australians 18+ (n=967)

Degree to which Australians feel their privacy is protected

Only a quarter (24%) of Australians feel the privacy of their personal information is well protected and 40% feel it is poorly protected. Similarly, a quarter (24%) feel their location information is well protected, whereas 41% feel it is poorly protected. Australians feel slightly more protected when it comes to electronic communications (28% well protected, 37% poorly protected). The protection of biometric information is the only area where more Australians feel well protected (35%) than poorly protected (27%).

Figure 42: Perception of levels of protection regarding specific privacy rights



B7. Thinking about legal and other protections. How protected do you feel in regard to the following privacy rights?
Base: Australians 18+ (n=1,506)

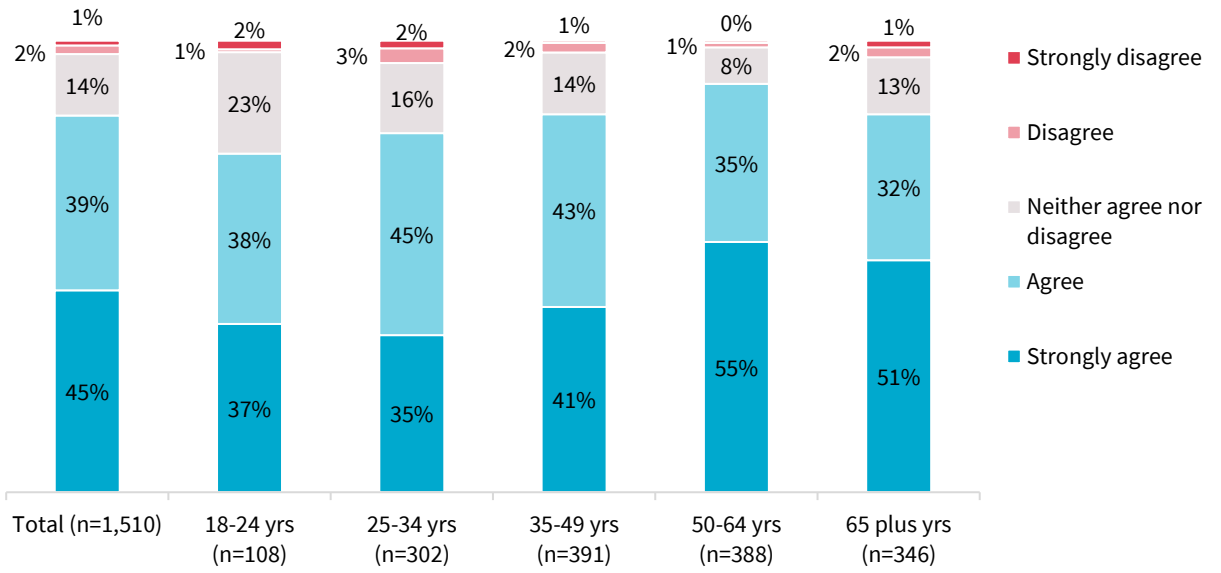
Older Australians, aged 50 and over, tend to be more likely than average to feel that information is poorly protected. A third (32%) feel that biometric information is poorly protected, 45% feel that electronic communications are poorly protected, 49% feel that personal information is poorly protected and half (50%) feel that location information is poorly protected.

The youngest cohort, on the other hand, are the least likely to feel these privacy rights are poorly protected. Eighteen percent of those age 18-34 feel this way about biometric information, 28% for electronic communications, 32% for personal information and 30% for location information.

Demand for greater government protection

The vast majority (83%) of Australians would like the government to do more to protect the privacy of their data. This finding is broadly consistent across most demographic groups, although older Australians are more likely to strongly agree. Fifty-four percent of those aged 50 and over strongly agree, compared with 41% of those aged 35-49 and 36% of those aged 18-34.

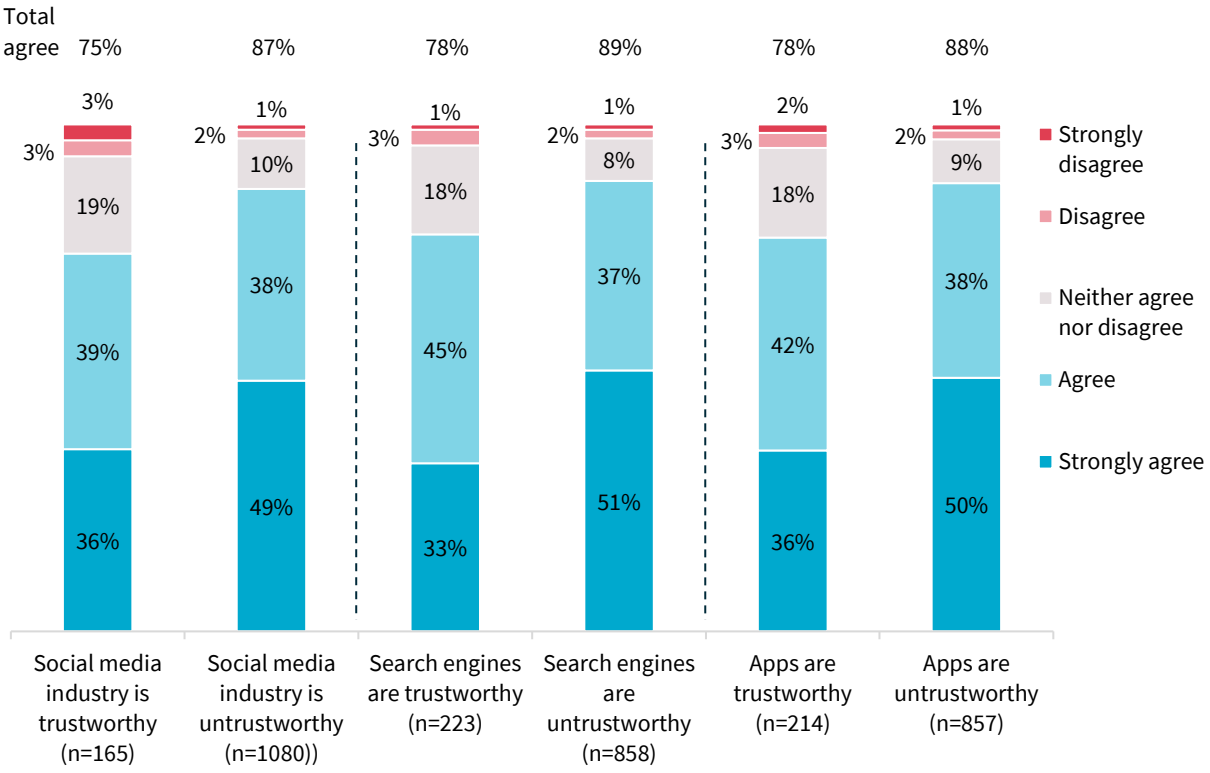
Figure 43: Australians' beliefs that the government should do more to protect the privacy of their data



B2_6. Thinking about data privacy, to what extent do you agree or disagree with each of the following statements? I would like the government to do more to protect the privacy of my data

While Australians feel poorly protected with regard to specific categories of personal information, they show appetite for higher levels of protection by the government. Those who consider digital services are untrustworthy are much more likely to want more protection from the government. For example, 87% of those who consider the social media industry untrustworthy would like the government to do more about privacy, compared to 75% of those who consider this industry trustworthy.

Figure 44: Australians' beliefs that the government should do more to protect the privacy of their data – organisation type breakdown



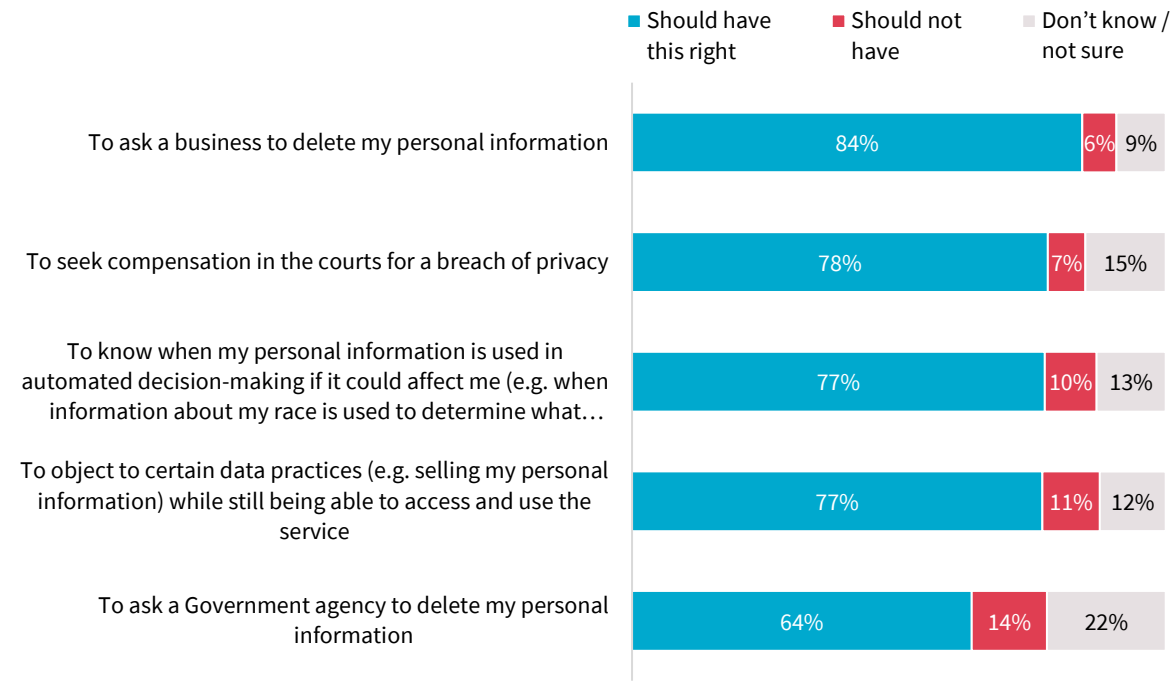
B2_6. Thinking about data privacy, to what extent do you agree or disagree with each of the following statements? I would like the government to do more to protect the privacy of my data

Additional rights under the Privacy Act

Australians are most likely to believe they should have the right to ask a business to delete their personal information (84%). This is followed by the right to seek compensation in the courts for a breach of privacy (78%), to know when their personal information is used in automated decision-making if it could affect them (77%) and the right to object to certain data practices while still being able to access and use the service (77%).

While fewer Australians believe they should have the right to ask a government agency to delete their personal information, this is still supported by two-thirds (64%) of people.

Figure 45: Australians' beliefs that they should or should not have specific privacy rights

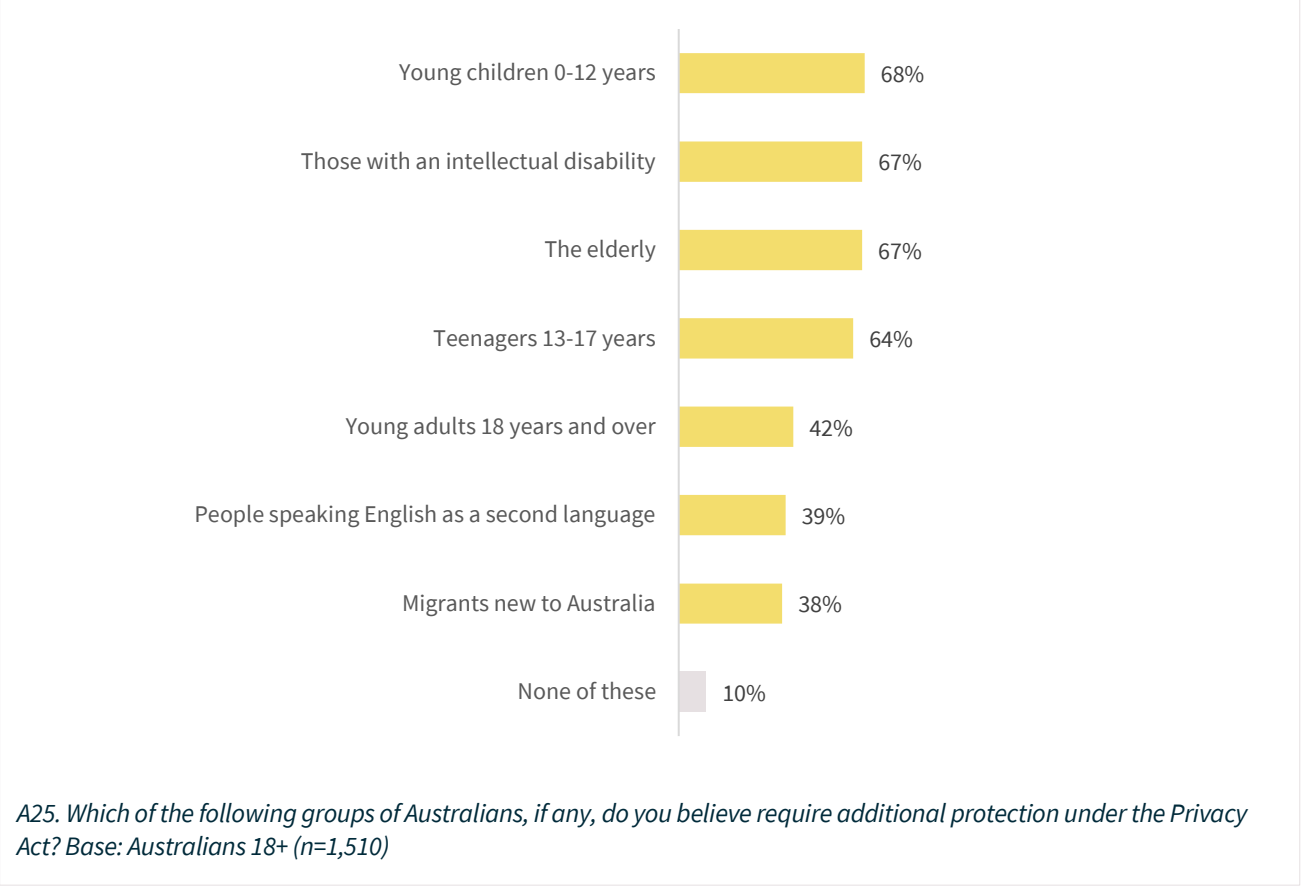


A24. Do you believe Australians should or should not have these rights? Base: Australians 18+ (n=1,510)

Vulnerable groups and the Privacy Act

Data protection and privacy rights are not only about regulating the activities of specific types of organisations but protecting groups of vulnerable Australians. Two-thirds of Australians believe that vulnerable groups, such as children under 12 years old (68%) and 13-17 years old (64%), elderly Australians (67%) and people with an intellectual disability (67%), require additional protection under the Privacy Act. A significant minority of Australians also support the additional protection of young adults (42%), people who speak English as a second language (39%) and new migrants to Australia (38%). Older Australians are more likely to think all the listed groups require additional protection.

Figure 46: Groups of Australians that should have additional protection under the Privacy Act



A25. Which of the following groups of Australians, if any, do you believe require additional protection under the Privacy Act? Base: Australians 18+ (n=1,510)

66% of Australians consider at least one vulnerable group of Australians should have additional protection under the Privacy Act

Privacy policies

Despite the majority (84%) of Australians believing the privacy of their information is important, only a third (31%) of Australians read privacy policies on internet sites and just 1 in 5 (20%) both read them and are confident they understand them.

The main reasons why Australians don't read privacy policies include their length and complexity. Australians are also using alternative measures to protect their privacy such as deleting apps or denying an app's permission to access information.

> A privacy policy is a statement that explains in simple language how an organisation or agency handles personal information

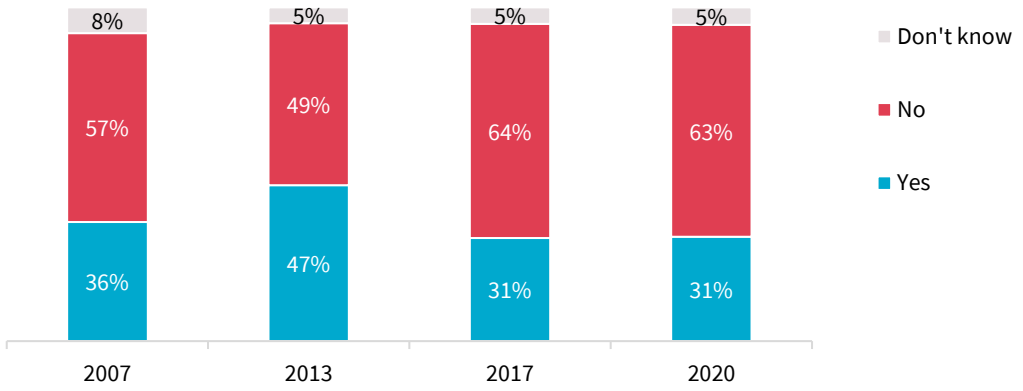
Australians strongly support measures to improve privacy policies by using simple, standard language and including a plain English summary.

Those who read privacy policies are much more likely to actively take steps to ensure the protection of their privacy and personal information. While we cannot establish that reading policies *causes* people to act, there is certainly a relationship. Privacy policies help Australians understand the privacy implications of using a service. It is therefore crucial that privacy policies are written to be easily understood.

Readership and comprehension of privacy policies online

The majority (84%) of Australians feel privacy of information and data is important when choosing a digital service. However, 69% do not normally read the privacy policy attached to any internet site. Australians are much less likely to have read a privacy policy in full (29%) than to have deleted an app or denied an app permission to access information (57% for both). The proportion who read privacy policies has not changed since 2017.

Figure 47: Proportion of Australians who normally read privacy policies on internet sites



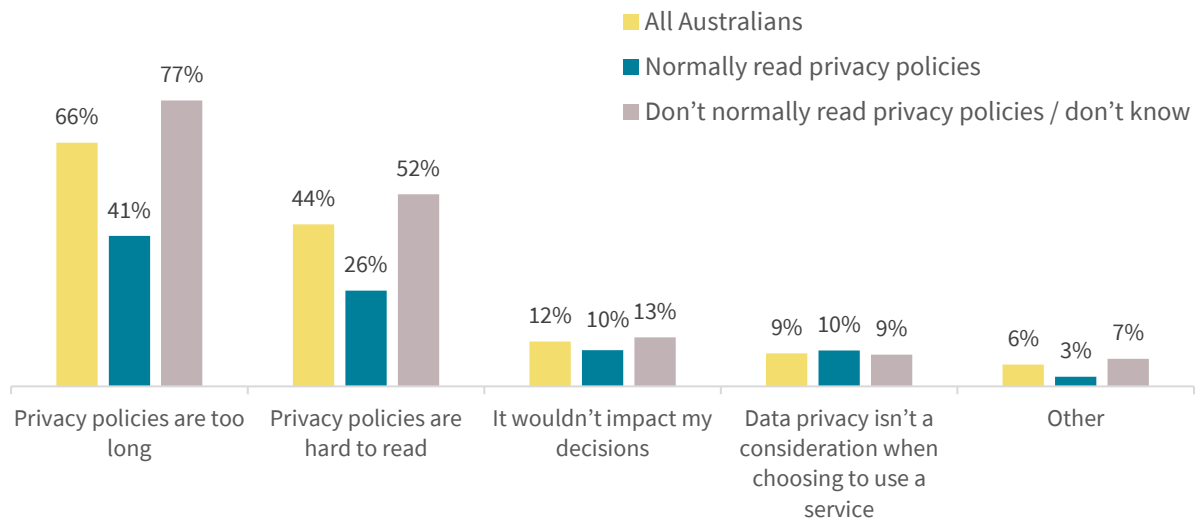
B20_2020. Do you normally read the privacy policy attached to any internet site? Base: Australians 18+ (n=1,506)

Reasons for not reading privacy policies

The key reasons Australians don't read privacy policies attached to internet sites is because of the length (77%) followed by their complexity (52%). Even among those who normally read the privacy policy attached to a site, 41% sometimes don't because it is too long and 26% sometimes don't because it is too hard to read.

Reasons for not reading a privacy policy vary across age groups. Younger Australians are the most likely to not read policies because they are too long with three-quarters (74%) listing this as a reason compared to 58% of the oldest Australians (65+). Half (49%) of older Australians do not read privacy policies because they are too hard to read, they are followed by their younger counterparts with 45% of aged 35-64, 38% of those aged 35-34 and 39% of 18-24-year-olds.

Figure 48: Reasons Australians don't read privacy policies

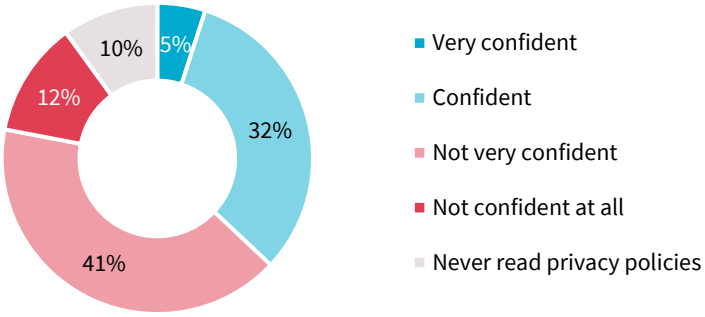


B21. Which of the following describes why you don't read privacy policies? by B20. Do you normally read the privacy

Comprehension of privacy policies

When Australians do read privacy policies, comprehension difficulties are widespread. Fewer than 2 in 5 Australians (37%) are confident they have understood them when they read them, and 53% are not confident. The remaining 10% never read privacy policies.

Figure 49: Confidence in comprehension of privacy policies after reading



B22. How confident are you that you have understood a privacy policy after reading it? Base: Australians (n=1506)

When analysing readership and comprehension together, 1 in 5 Australians (20%) normally read privacy policies *and* feel confident they have understood them.

Figure 50: Confidence in comprehension of privacy policies after reading – reading habit breakdown

B20. Do you normally read the privacy policy attached to any internet site? B22. How confident are you that you have understood a privacy policy after reading it? Base: Australians who know whether they normally read privacy policies (n=1,442)

The impact of privacy policies on behavioural change

Privacy policies impact behaviour. Seventy percent of Australians have taken action after reading a privacy policy. This includes:

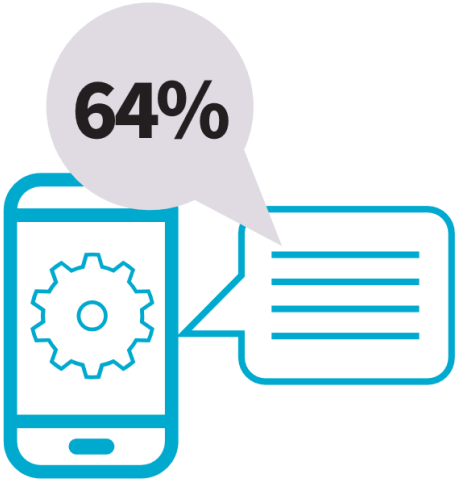
- 44% who chose not to use a service
- 28% who deleted an app, and
- 23% who changed the default privacy settings.

Those who normally read privacy policies (84%) are more likely to take action to protect their privacy than those who don't normally read them (56%). Those who are confident they understand privacy policies are also more likely to take action (74% cf. 67% of those who don't).

A third (32%) of Australians are more likely to change their default privacy settings after reading a privacy policy. Interestingly, those less confident they understand privacy policies are more likely to change their default privacy settings as a result of reading them (37%; cf. 29% of those who are confident they understand).

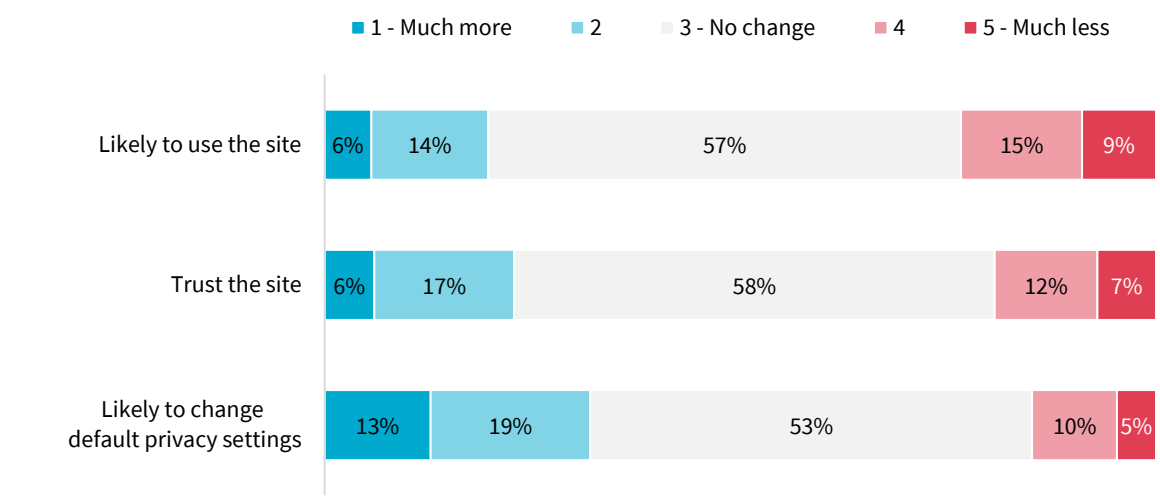
Overall, 23% of Australians are likely to trust a site more if they have read the privacy policy, compared to 19% who trust it less.

Twenty percent of Australians are more likely to use a site after reading a privacy policy, compared with 23% who are less likely to use it. Younger Australians (18-34 years) are less likely to use a site (26% compared to 17% more likely). This is more balanced for Australians aged 35-49 with 1 in 5 being both more likely (18%) and less likely (21%) to use the site as a result of reading the policy, and those aged 50+ with 23% being more likely to use and the same proportion (23%) being less likely to use the site after reading the privacy policy.



64% of Australians have taken action after reading a privacy policy, such as not using a service, deleting an app or changing default privacy settings

Figure 51: Impacts of reading a privacy policy

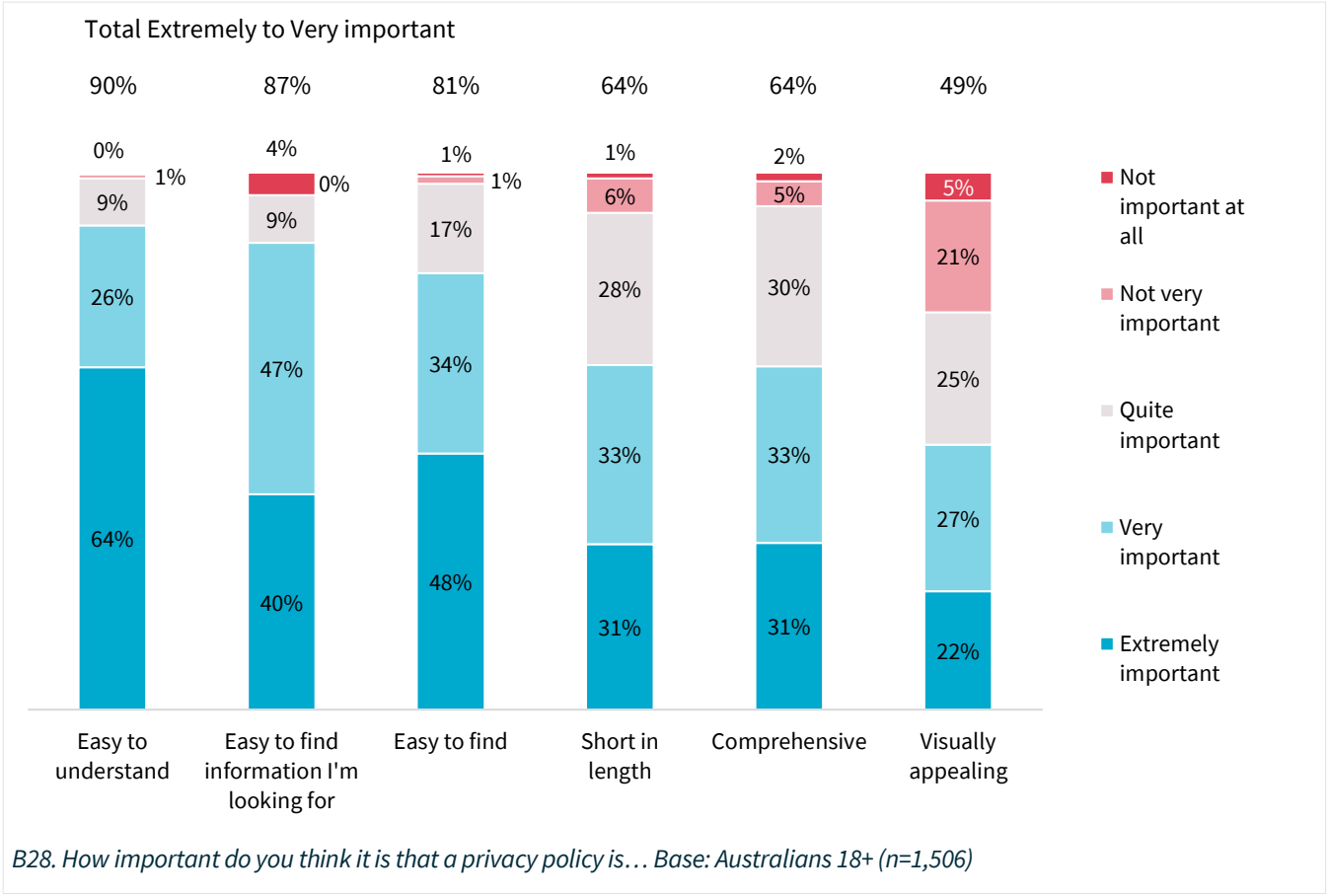


B24. What impact, if any, does reading a privacy policy have upon your attitude towards a site? Does it make you…
Base: Australians 18+ (n=1506)

Key features in privacy policies

Australians are most likely to rate ease of comprehension (90%) and ease of navigation (87%) as very important in a privacy policy. Being easily able to find the policy is the third most important point to Australians – 48% find this very important. Being short in length is important to 64%, while just as many (64%) find it important that privacy policies are comprehensive.

Figure 52: Importance of specific attributes of privacy policies to Australians



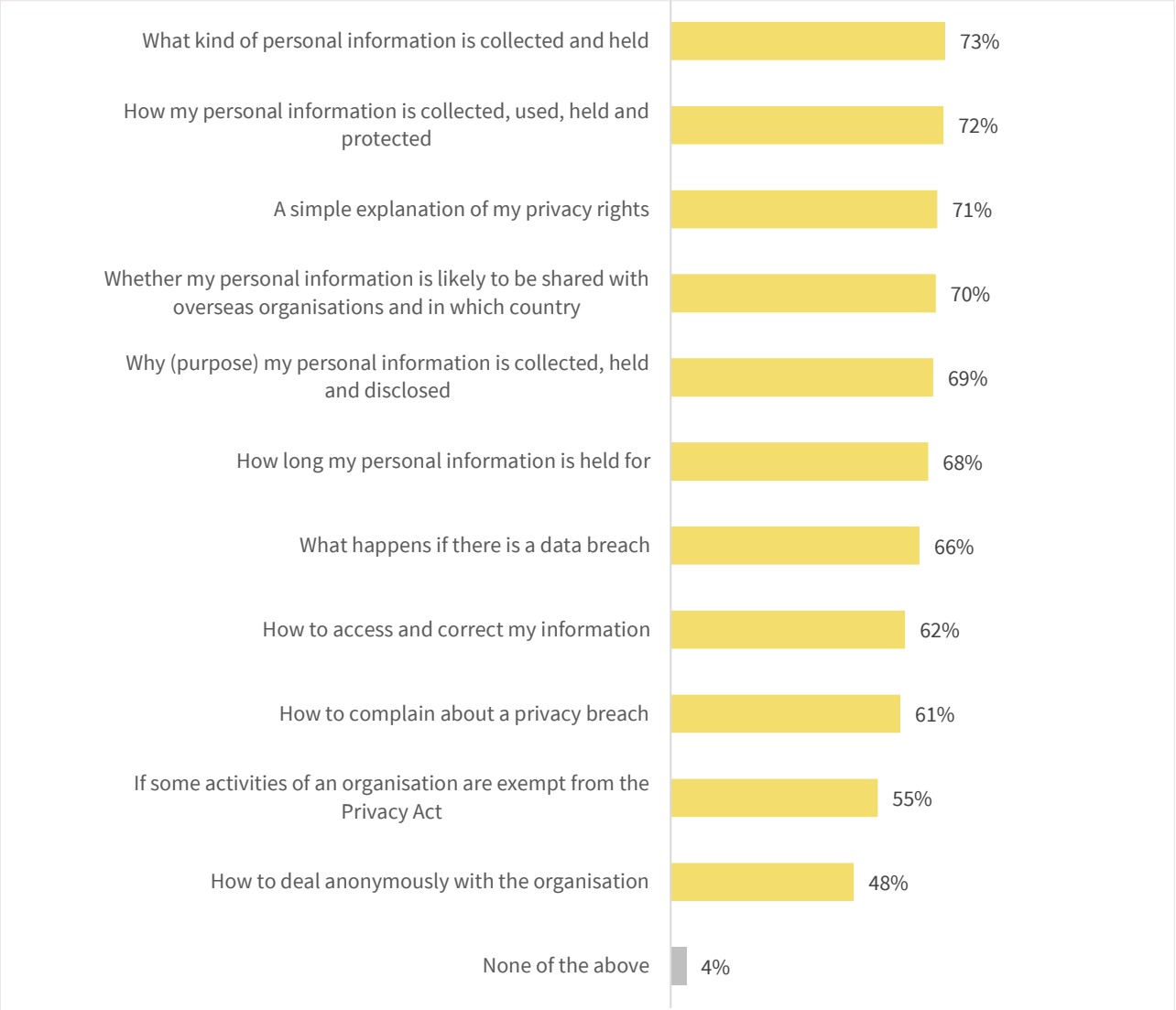
B28. How important do you think it is that a privacy policy is… Base: Australians 18+ (n=1,506)

A policy that is easy to understand is equally important to those who normally read policies (89%) and those who don't (91%), as well as to those who are confident they understand a policy when they read it (89%) and those who are not (92%).

Desired content in privacy policies

In terms of the information Australians consider should be covered by privacy policies, they are most likely to want to know *what* personal information is being collected and held and *how* it is collected, held and protected. However, the majority of Australians believe all elements should be included, with the exception of how to deal anonymously with the organisation, which just under half (48%) would like to see included.

Figure 53: What Australians think a privacy policy should include



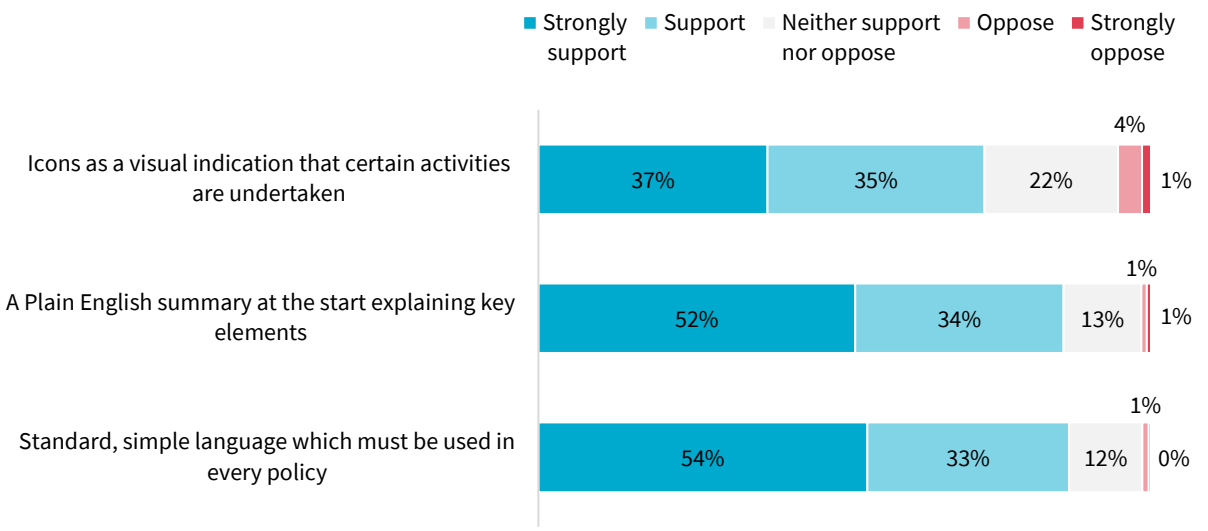
B27. Some people think that privacy policies should be as short as possible, others think they should be comprehensive. With this in mind, which of the following do you think should be in all privacy policies? Base: Australians 18+ (n=1,506)

Improvements to privacy policies

Echoing the desire for privacy policies that are easy to understand, levels of support are very high for 3 improvements tested in the survey: simple language, a plain English summary and use of icons.

The preferred way to improve the current format of privacy policies is the introduction of standard, simple language (87% support), followed by the introduction of a plain English summary at the start of every privacy policy explaining key elements (86% support). The introduction of icons as a visual indication that certain activities are undertaken (for example, if personal information is passed on to third parties or if data is stored overseas) receives comparatively less support (73% agree).

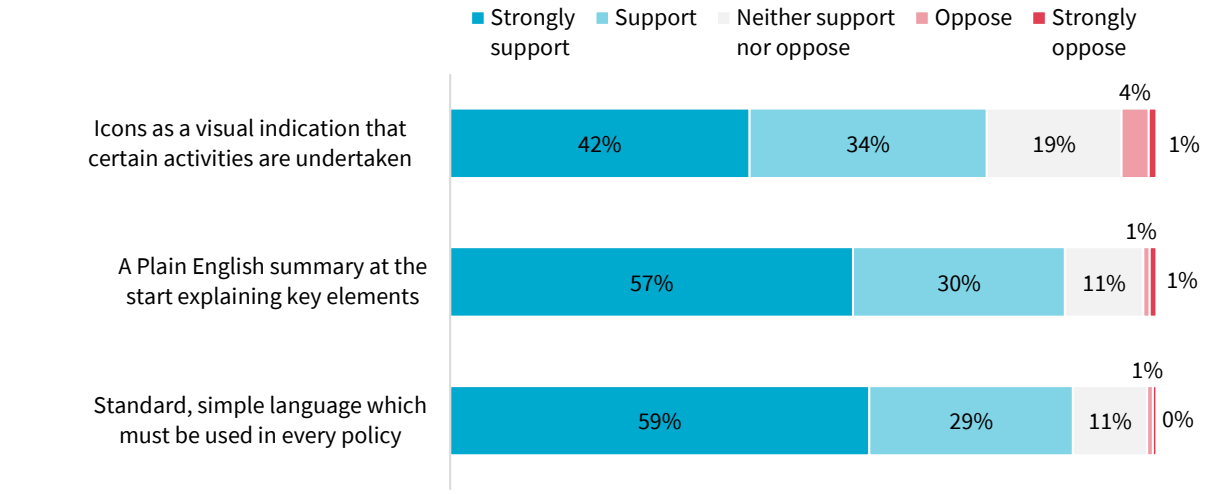
Figure 54: Suggestions to improve privacy policies



B25. There have been a number of suggestions to improve the privacy policies of Australian organisations. To what extent do you support or oppose each of the following ideas? Base: Australians 18+ (n=1506)

Those who are not confident they understand privacy policies are marginally more likely to strongly support each measure, implying these improvements appeal to the cohort of Australians most likely to benefit from them.

Figure 55: Suggestions to improve privacy policies among those who don't understand them

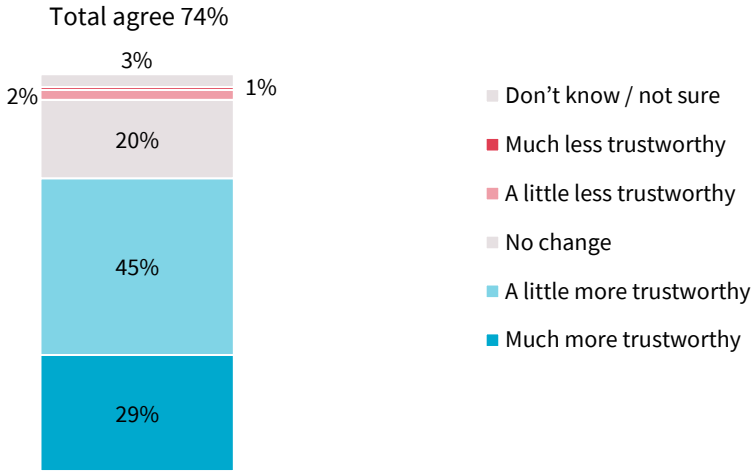


B25. There have been a number of suggestions to improve the privacy policies of Australian organisations. To what extent do you support or oppose each of the following ideas? Base: Australians 18+ who are not confident they understand privacy policies (n=825)

Privacy certification

A privacy certification would make certified organisations more trustworthy to three-quarters (74%) of Australians. Privacy certifications would most likely influence the perception of older Australians compared to their younger counterparts. Older Australians consider a certified organisation to be more trustworthy. This is driven by the oldest Australians, with 4 in 5 Australians over 65 years of age (84%) and those aged 50-64 (79%) as well as three-quarters (74%) of those aged 35-49 believing a privacy certification would make certified organisations more trustworthy. This is significantly less likely among Australians aged 18-34, with only 3 in 5 (62%) agreeing.

Figure 56: Impact of privacy certification on trust in organisations



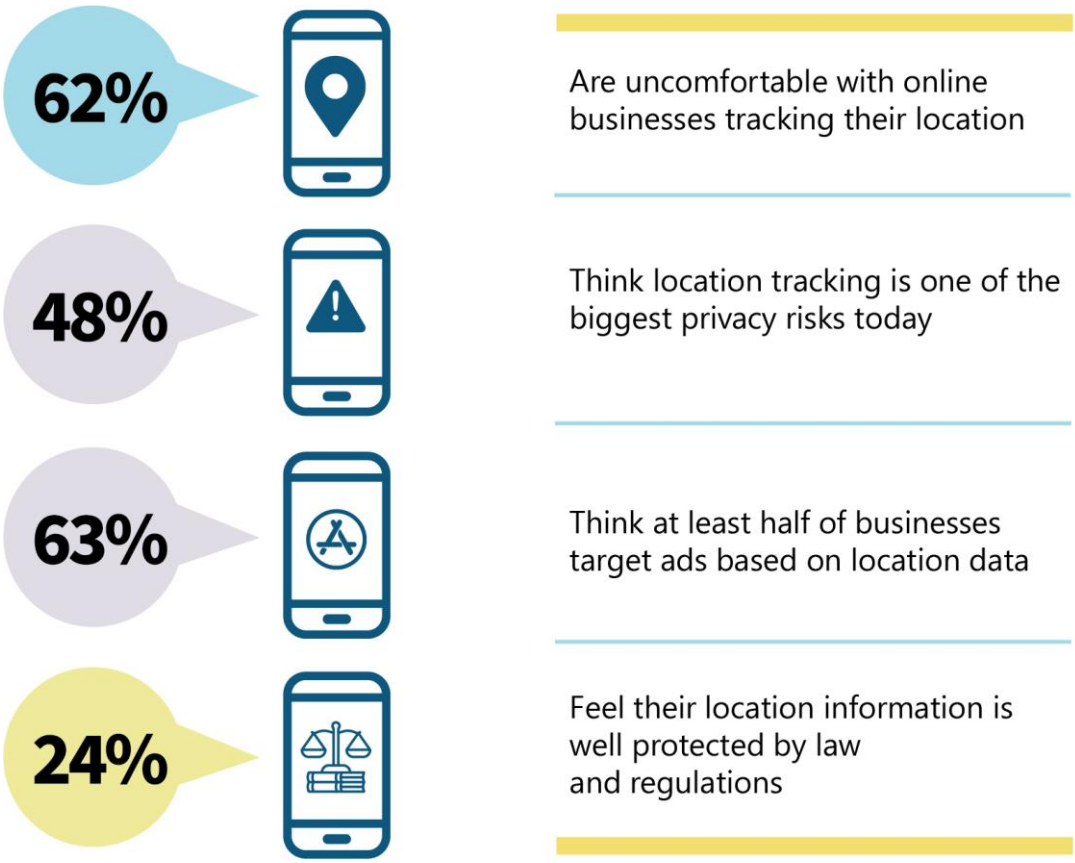
B26. To what extent would privacy certification make certified organisations more or less trustworthy? Base: Australians 18+ (n=1506)

Part 3: Location data

Australians are uncomfortable with the use of location tracking and the handling and use of that information. Half (48%) of Australians consider it is one of the biggest privacy risks today, ahead of sending data overseas (41%), surveillance by foreign entities (35%) or Australian entities (26%), profiling (31%) and ID scanning (28%).

Australians are more reluctant to provide their location data (56%) than their address (52%), phone number (50%), date of birth (38%), email address (30%), household composition (27%) or sexual orientation (25%). Similar to other types of personal information, the main reasons for not wanting to provide location data are safety and security, keeping the information private and not wanting to be profiled. Those who are reluctant to provide location information say it is because they do not want people knowing where they live or how to contact them (52%; cf. average 33%).

Nearly two-thirds of Australians (63%) think that at least half of businesses target ads based on location data. Over 2 in 5 Australians (44%) always or often turn off the GPS on their phone.

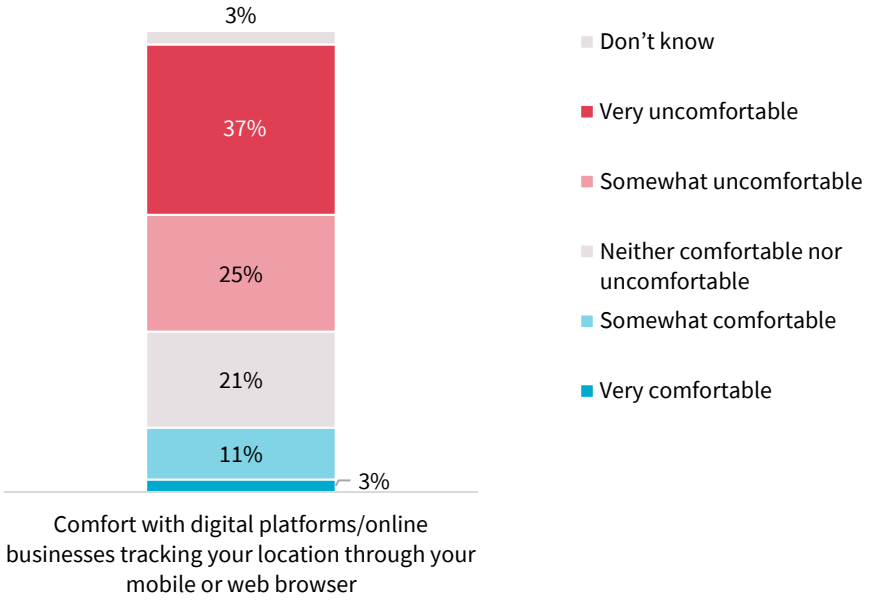


A8/A16_3/A18_2/B7_4. Attitudes of Australians towards Location tracking topics. Base: Australians 18+ (n=1,506 to 1,510)

Comfort with the use of location data

Two-thirds (62%) of Australians are uncomfortable with digital platforms/online businesses tracking their location through their mobile or web browser. This is higher among females, with two-thirds (65%) feeling uncomfortable compared to males (59%), and highest among older Australians, with three-quarters (72%) feeling uncomfortable compared to only 55% of those aged 18-49 years.

Figure 57: Australians' comfort with businesses tracking location

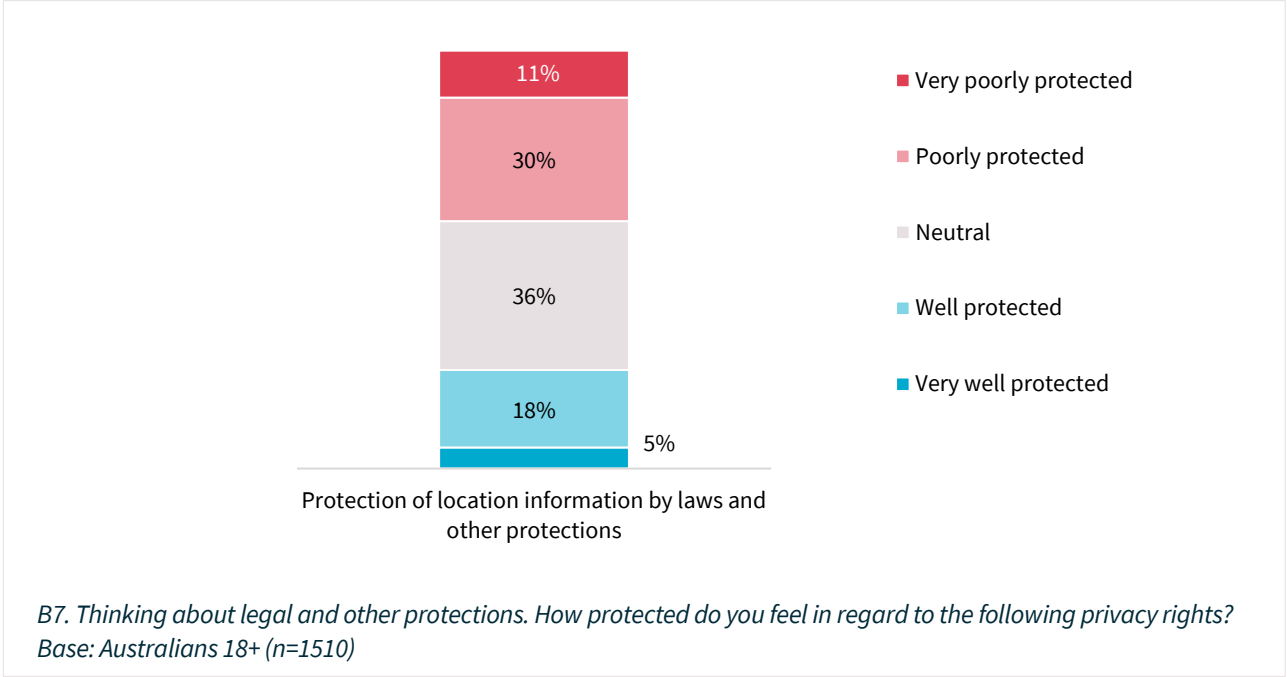


A16. How comfortable are you with each of the following data practices? Base: Australians 18+ (n=1510)

Protection of location data

Two in 5 Australians (41%) feel their location information stored by organisations or devices (such as their mobile phones) is poorly or very poorly protected by law. Conversely, 24% feel their location information is well or very well protected. Australians are more likely to feel their location information is poorly protected the older they are, with 54% of those aged 65+ and half (48%) of those aged 50-64 years feeling poorly or very poorly protected. This drops to close to 2 in 5 (38%) among those aged 35-49 and down to 30% among 18-34-year-olds.

Figure 58: Protection of location data

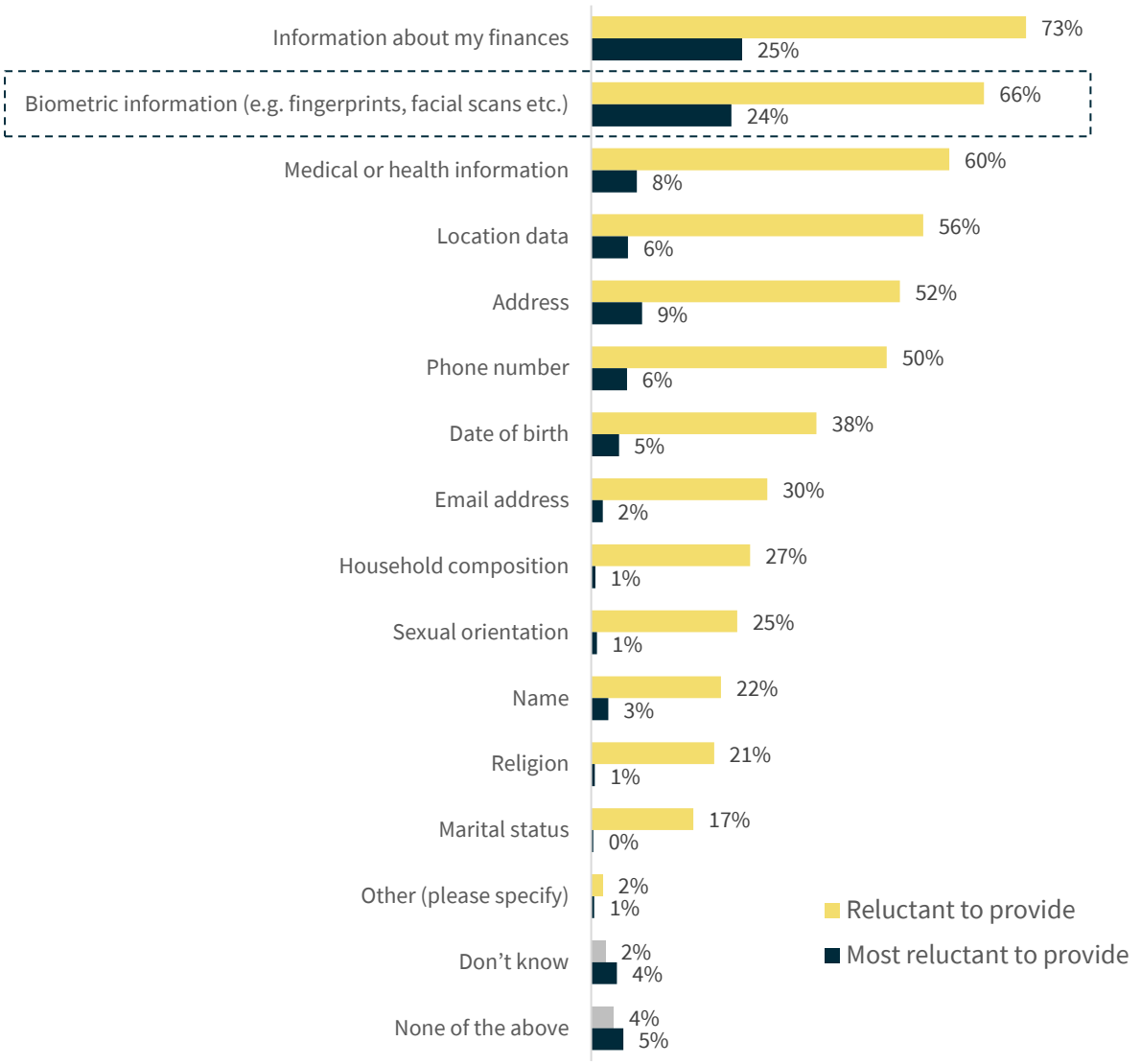


B7. Thinking about legal and other protections. How protected do you feel in regard to the following privacy rights? Base: Australians 18+ (n=1510)

Part 4: Biometric information

Two-thirds (66%) of Australians are reluctant to provide biometric information to a business, organisation or government agency and a quarter (24%) are more reluctant to provide biometric information than any other type of information. This is higher than unwillingness to provide medical or health information (60% reluctant and 8% most reluctant) and location data (56% reluctant and 6% most reluctant).

Figure 59: Type of information Australians are reluctant to provide to any organisation



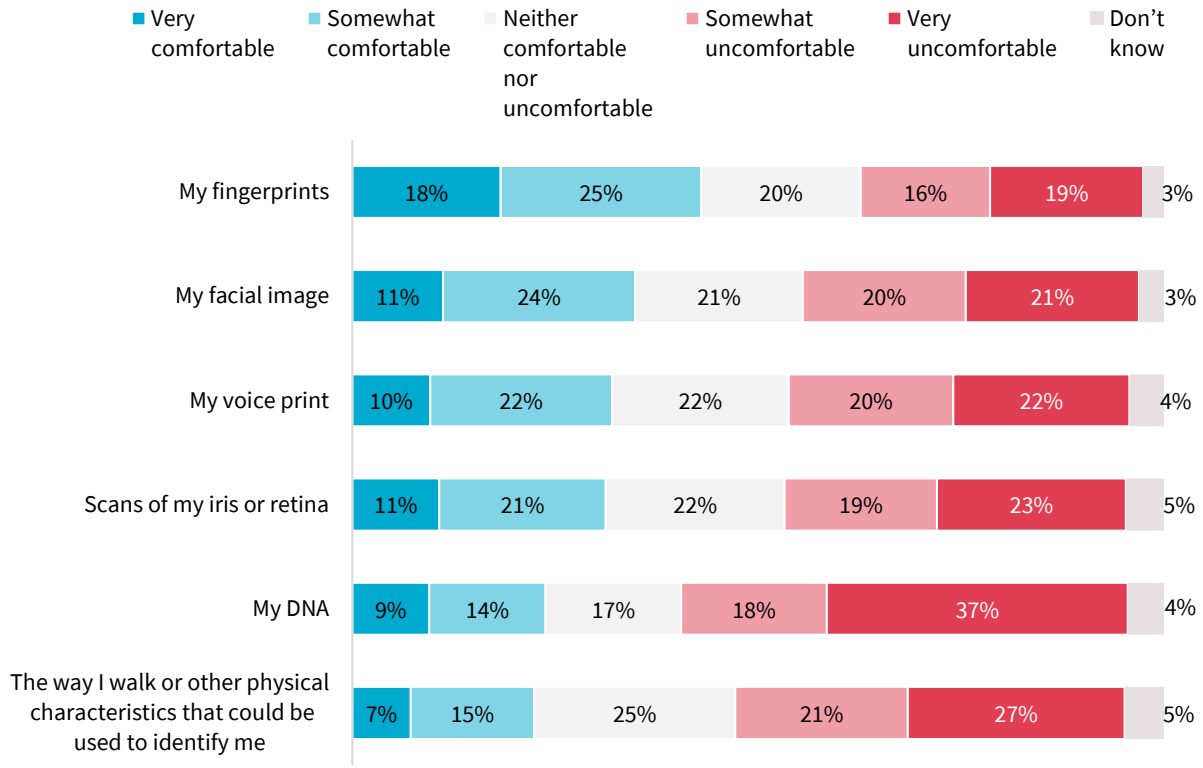
B3. Thinking now about providing your personal information to any business, organisation or government agency, in general, what types of information are you reluctant to provide? B4. And which one of these do you feel most reluctant to provide? Base: Australians 18+ (n=1,506)

Levels of reluctance vary depending on the organisation and the purpose of collection, with Australians generally being more comfortable providing biometric information to more trusted organisations in exchange for more personalised services.

Comfort with providing different types of biometric information

Collection of DNA is the type of biometric information most likely to make Australians feel uncomfortable (55% are uncomfortable, including 37% very uncomfortable). Levels of discomfort are higher than levels of comfort when it comes to the collection of all listed biometrics except for fingerprints. Australians tend to be more comfortable with the collection of biometric information that is widely used through smart devices and for government purposes, such as fingerprints (43% comfortable), facial images (35% comfortable) and voice prints (30% comfortable).

Figure 60: How comfortable Australians feel with collection of biometric information



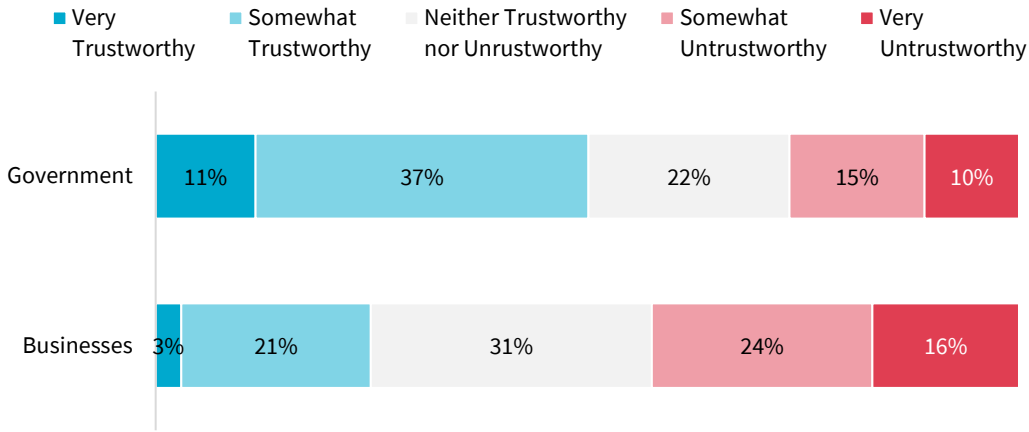
A13. How comfortable are you with the following types of biometric information being collected? Base: Australians 18+ (n=1,510)

Trust in private and public sector organisations to collect biometric information

Australians are much more likely to trust government than businesses to collect and use biometric information. Half (48%) consider government trustworthy (compared with 25% untrustworthy), however just 23% consider businesses trustworthy (compared with 40% untrustworthy).

Older Australians aged 65 and over (56%) are more likely than their younger counterparts to find government trustworthy with 2 in 5 (43%) of those aged 50-64 years, half (49%) of those aged 35-64 and only 45% of 18-34 year-olds viewing them as trustworthy. There are no strong differences by age with regard to trust in businesses.

Figure 61: Trustworthiness of organisations using biometric information



A15. In your opinion, how trustworthy are the following to collect and use biometric information? Base: Australians 18+ (n=1,510)

When it comes to government use of biometrics, over half are comfortable with law enforcement using facial recognition and video surveillance to identify suspects (58% comfortable, 23% uncomfortable) or a government body using surveillance for public safety (56% comfortable, 22% uncomfortable).

Comfort with providing biometric information for different purposes

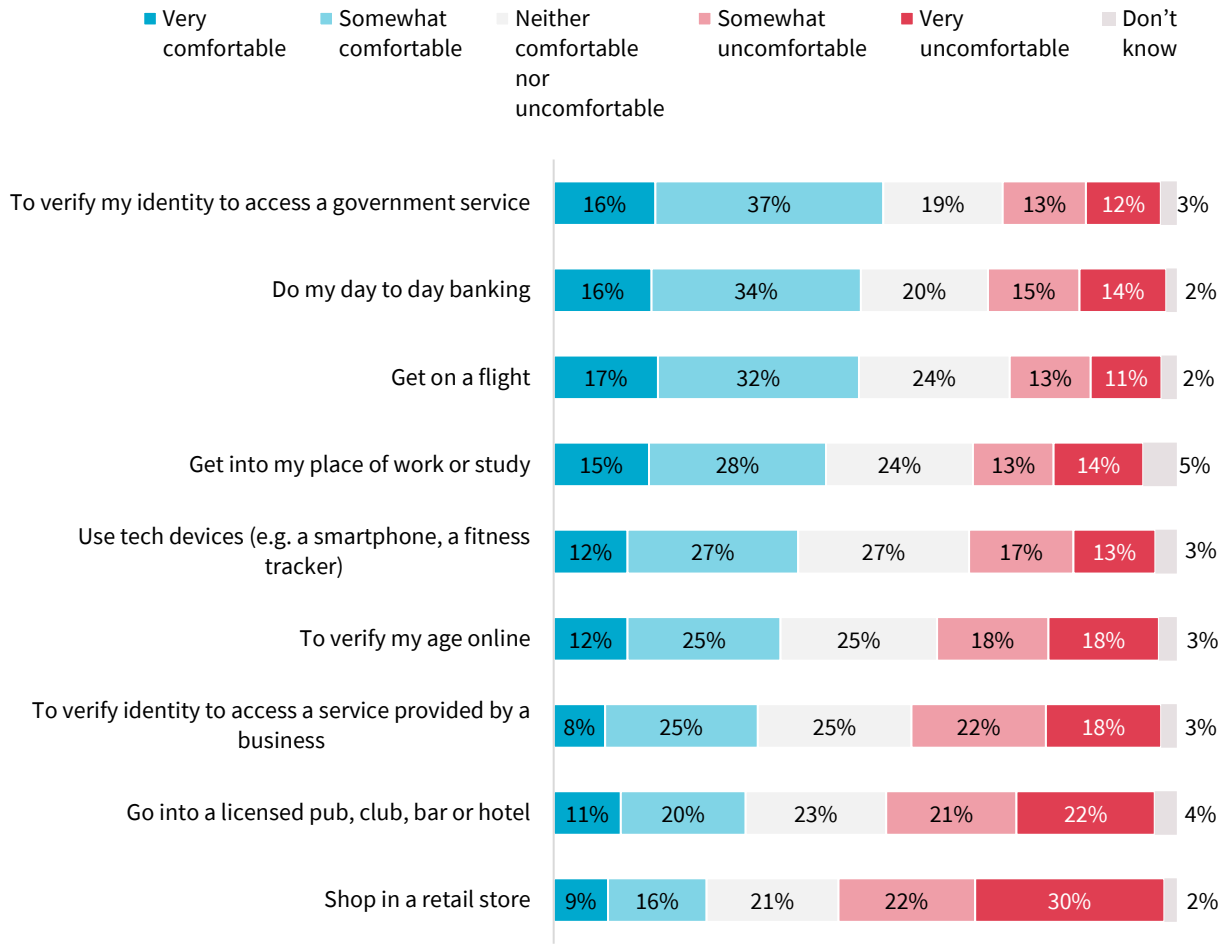
Half of Australians are comfortable providing their biometric information to verify their identity to access government services (53% are comfortable, 25% uncomfortable), to do their day to day banking (49% are comfortable, 29% are uncomfortable) or to get on a flight (49% are comfortable, 24% are uncomfortable). It should be noted that the Federal Government and financial institutions are the most trusted organisations with regard to the way they protect or use Australians' personal information (considered trustworthy by 51% and 50% of Australians respectively).

On the other hand, the majority of Australians are uncomfortable with the collection of their biometric information to shop in a retail store (52% uncomfortable, 25% comfortable), to get into a licensed pub, club, bar/hotel (43% uncomfortable, 31% comfortable) or to verify their identity to access services provided by a business or private organisation (40% uncomfortable, 33% comfortable). This correlates with a lower level of trust in retail, with 42% considering retail stores to be untrustworthy in the way they protect or use personal information.

Between 8% and 17% of Australians are very comfortable with each of the specified uses of biometric information.

At least a quarter of Australians are uncomfortable with each of the data practices listed, including the use of biometrics to access a government service.

Figure 62: How comfortable Australians feel with uses of biometric information



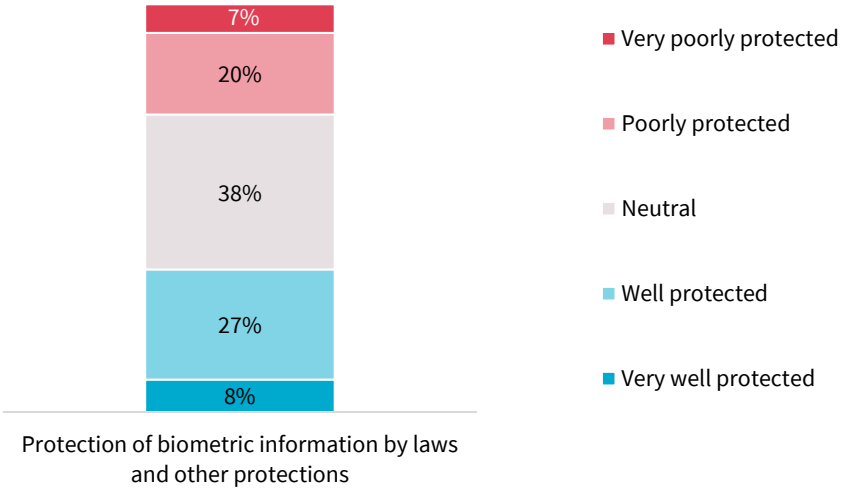
A14. How comfortable are you with the use of biometric information for the following purposes? Base: Australians 18+ (n=1,510)

Protection of biometric data

A third of Australians (35%) feel their biometric information stored by organisations or devices (such as their mobile phones) is well protected by laws and other protections, however 27% feel they are poorly protected. Thirty-eight percent of Australians are more likely to feel neither well protected nor poorly protected (38% neutral).

Younger Australians are more likely to feel their biometric information is well protected, with 45% of those aged 18-34 feeling well protected, this drops to a third (33%) among those aged 35-49 and down again to 3 in 10 among those aged 50-64 (31%) and of those over 65 (28%).

Figure 63: Protection of biometric information



B7_3. Thinking about legal and other protections. How protected do you feel in regard to the following privacy rights? Base: Australians 18+ (n=1,506)

Part 5: Artificial intelligence

Government agencies and private companies are increasingly using technologies such as artificial intelligence (AI) to make decisions that may impact individuals. This has the potential to generate significant opportunities and efficiencies for business, government, and the community. However, the use of these technologies also creates privacy risks particularly where there is a lack of transparency about how personal information is used to make decisions, accountability and human oversight.

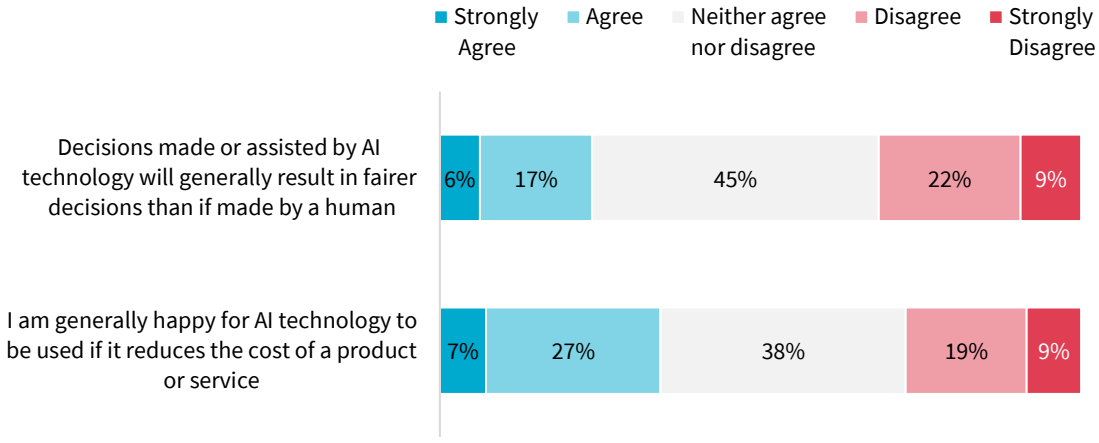
Over three-quarters of Australians (77%) consider the use of AI without their knowledge (for example, hiding ads or articles from their social media feed based on race or gender) to be a misuse of their personal information. In fact, a quarter (24%) feel AI is one of the biggest privacy risks facing Australians today. Although this rate is lower than many other potential privacy risks, it is more likely to be of concern among older Australians, with close to 3 in 10 (28%) of those aged 50+ agreeing it is a potential risk. This drops to about a quarter (23%) among those aged 35-49 and to 1 in 5 among 18-34-year-olds.

General attitudes towards AI

Thirty-two percent of Australians disagree that decisions made by AI will be fairer than decisions made by humans. A quarter of Australians (24%) believe decisions made by AI will be fairer than when there is a human involved and a third (34%) believe AI can lead to cost savings.

These beliefs are more widely held by younger Australians. Two in 5 (43%) of younger Australians, aged 18-34, are generally happy for AI to be used if it reduces the costs of products, this drops to 37% among 35-49-year-olds and down to 27% among Australians who are 50 and over. Three in 10 (31%) of those aged 18-34 believe decisions made or assisted by AI will be fairer than decisions made by humans, compared to a quarter (25%) of those aged 35-49 and 17% of those over 50 years. Males are more likely (27%) than females (21%) to believe decisions made or assisted by AI will be fairer than decisions made by a human.

Figure 64: General beliefs about AI technology



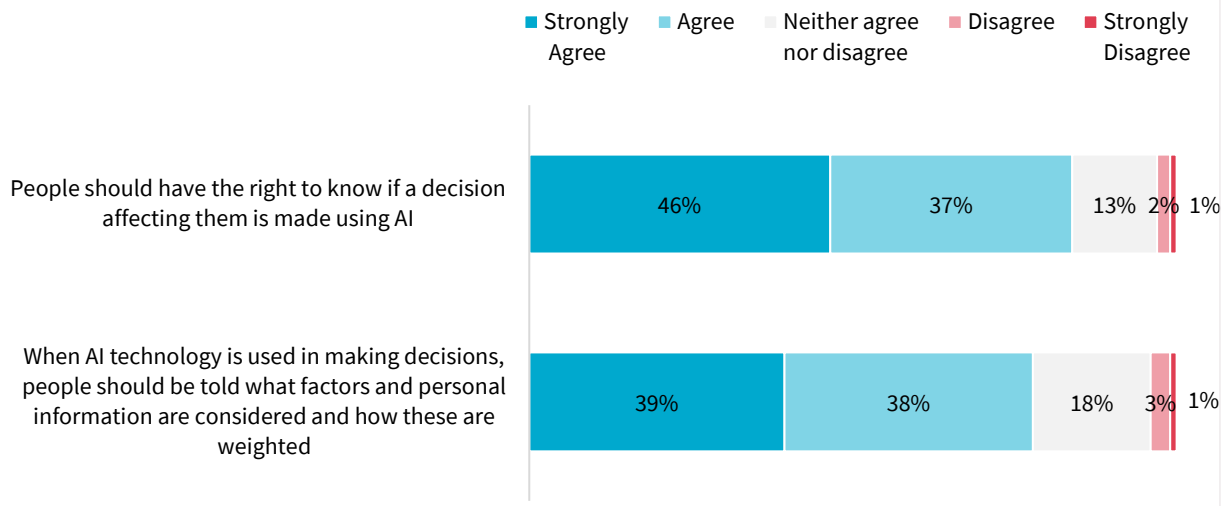
B19. To what extent do you agree or disagree with each of the following statements? Base: Australians 18+ (n=1,506)

Right to know if AI is being used

There is a strong belief (84% agree) that Australians have a right to know if a decision affecting them is made using AI technology. It is most widespread among older Australians with 9 in 10 (91%) of those aged 50 or more agreeing. This drops down to 83% among those aged 35-49 and to three-quarters (75%) for 18-34-year-olds.

Similarly, 78% believe that when AI technology is used to make or assist in making decisions, people should be told what factors and personal information are considered by the algorithm and how these factors are weighted. This attitude is also most widespread among older Australians, with 85% of those aged 50+ years agreeing, compared to three-quarters (76%) of those aged 35-49 and 69% of 18-34-year-olds.

Figure 65: Attitudes towards being informed when AI technology is used

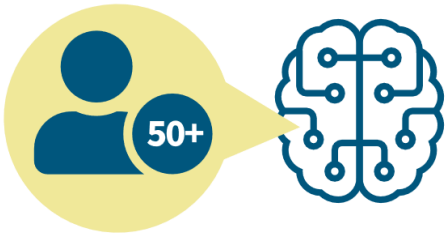


B19. To what extent do you agree or disagree with each of the following statements? Base: Australians 18+ (n=1,506)

Right to human oversight

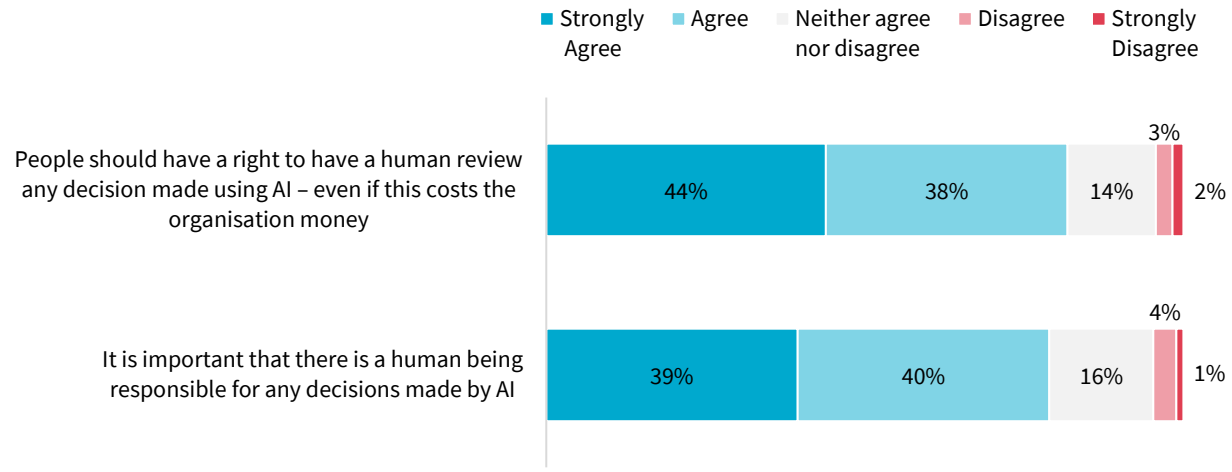
Over 4 in 5 (82%) Australians believe people should have a right to have a human review any decision made using AI, even if this costs the organisation money. A similar proportion (79%) believe it is important that there is a human responsible for any decisions made by AI.

Australians 50 years and older are more likely to hold both of these beliefs, with close to 9 in 10 agreeing people should have a right to have a human review (89%) and it is important that there is a human responsible for any decisions made by AI (87%). This drops down to close to 4 in 5 among those 35-49 years old (80% and 78% respectively). Australians aged 18-34 are the least likely to agree with both statements with three-quarters (74%) agreeing people should have the right to have a human review decisions made by AI and 69% agreeing it is important that there is a human being responsible for any decisions made by AI.



Australians 50+ are much more likely to think that people have the right to know if a decision affecting them is made using AI

Figure 66: Attitudes towards human oversight of decisions made by AI



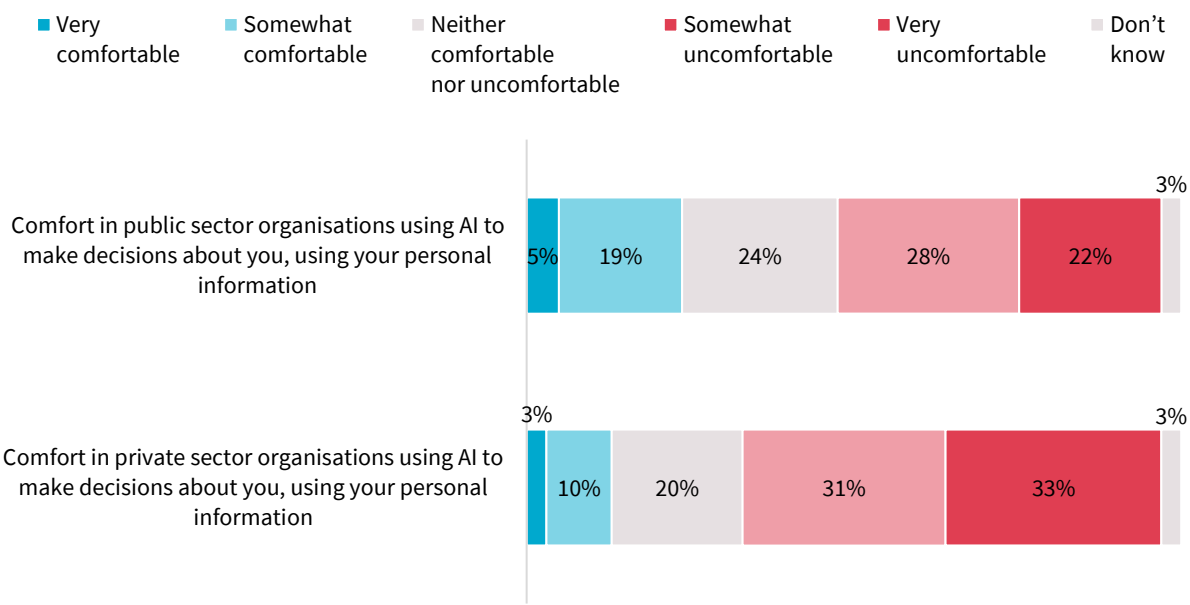
B19. To what extent do you agree or disagree with each of the following statements? Base: Australians 18+ (n=1,506)

Impact of organisation types on trust in AI

Levels of comfort with data practices involving AI vary depending on the level of trust in the organisation involved. Half (49%) of Australians are uncomfortable with public sector organisations using AI to make decisions using their personal information (24% comfortable). This increases to almost 2 in 3 (64% uncomfortable) when private sector organisations are involved (13% comfortable).

However, levels of comfort with data practices involving AI are lower for both sectors compared to other uses of personal information. For example, 40% of Australians are comfortable with government using personal information for research, service development or policy development purposes.

Figure 67: Comfort with organisations using AI to make decisions



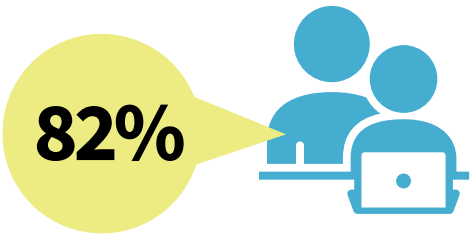
B17. How comfortable do you feel about public sector organisations using AI to make decisions about you, using your personal information? / B18. How comfortable do you feel about private sector organisations using AI to make decisions about you, using your personal information? Base: Australians 18+ (n=1,506)

Part 6: Children's privacy

Australian parents are more likely to be concerned about their children's privacy than their own and are very supportive of measures to increase the protection of their children's privacy and educate children on these issues.

Parents provide their children access to connected devices and digital services early in life and many are uncomfortable with businesses' handling of their children's personal information.

The majority of parents consider that children should have the right to grow up without being profiled and targeted (84% agree, 59% strongly agree), which is likely to influence the levels of discomfort with data practices that affect children. The increasing opportunities for profiling and targeting children also play a role, with 72% of parents concerned about the increasing privacy risk of internet-connected children's toys.

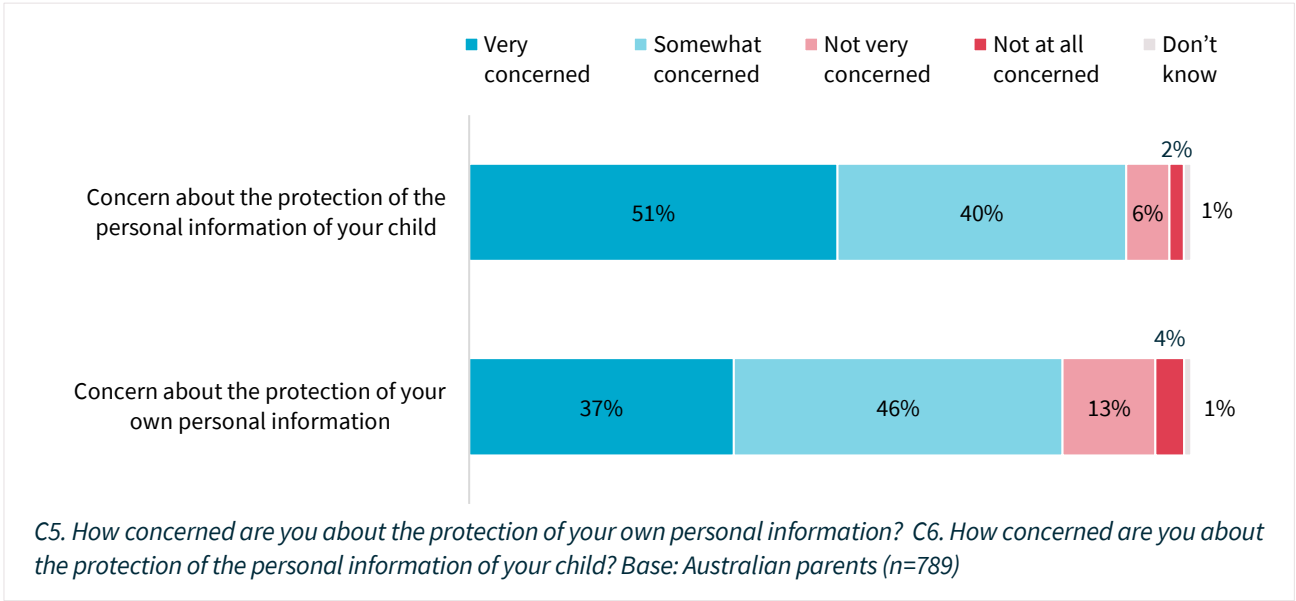


Most parents (82%) believe children must be empowered to use the internet and online services, but their data privacy must also be protected

Concerns for children's privacy

Parents are more concerned about their children's privacy (91% concerned, including 51% very concerned) than for their own (82% concerned, including 37% very concerned).

Figure 68: Parents' concerns about the protection of personal information



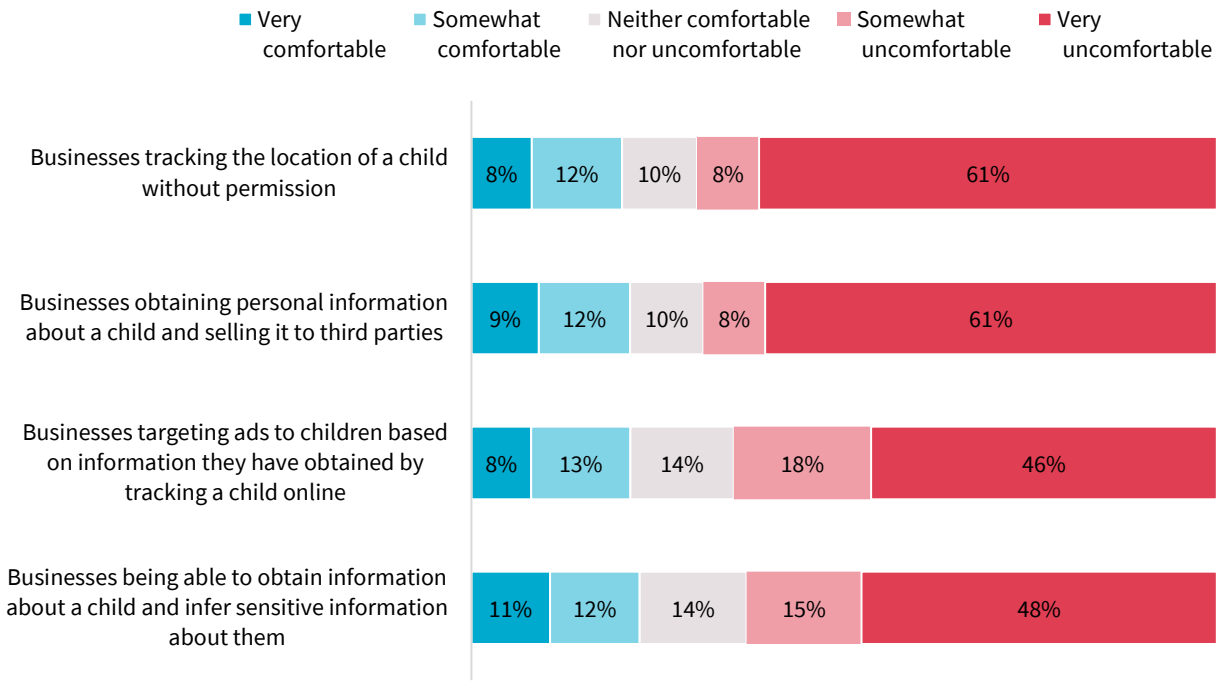
C5. How concerned are you about the protection of your own personal information? C6. How concerned are you about the protection of the personal information of your child? Base: Australian parents (n=789)

Parents are particularly uncomfortable with businesses tracking the location of a child (70% uncomfortable) and businesses obtaining personal information about a child and selling it to third parties (69% uncomfortable). Discomfort with both practices is consistent across children of different ages.

Sixty-five percent of parents are uncomfortable with businesses targeting ads to children based on information they have obtained by tracking a child online. This is highest among parents of children aged 10-13 (68%) and 14-17 (69%), compared with 60% of parents of children aged 2-5 and 63% of parents of children aged 6-9.

Almost two-thirds (63%) of parents are uncomfortable with businesses being able to obtain information about a child (such as age, location and interests) and infer sensitive information about them (such as a health condition).

Figure 69: Parents' levels of comfort with businesses using their child's personal information

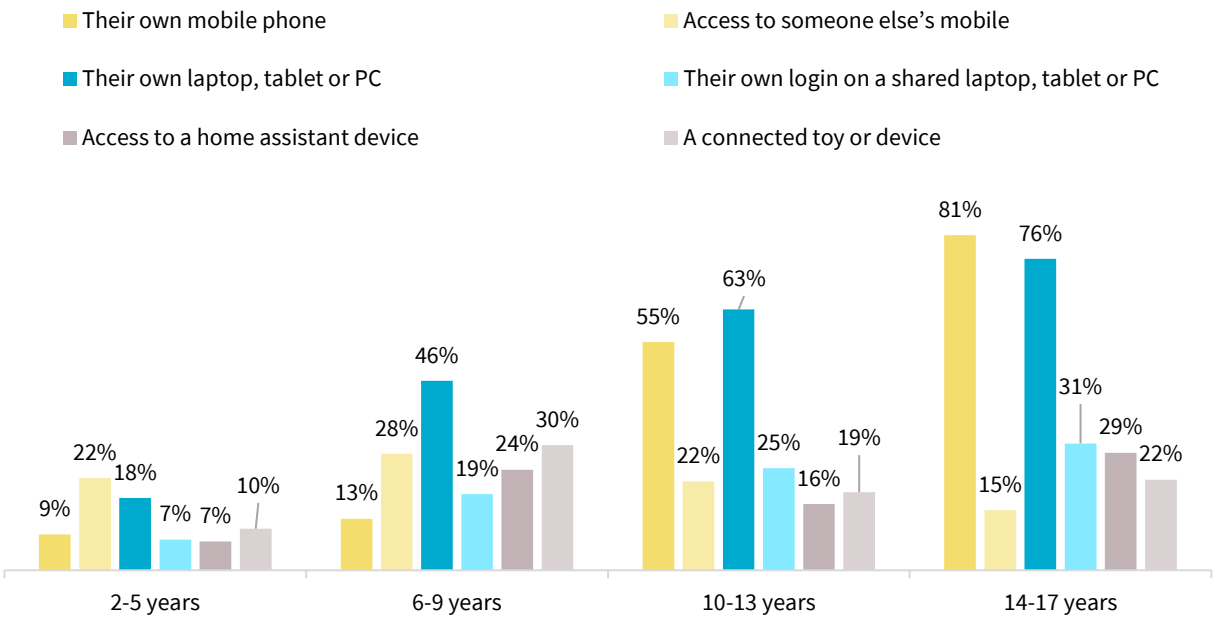


C14. Still thinking of children's data privacy. How comfortable are you with each of the following? Base: Australian parents (n=789)

Children’s access to and ownership of devices

Children tend to first own a laptop, tablet or PC, with almost half (46%) of children aged 6-9 owning their own device. Mobile phone ownership follows, with over half (55%) of those aged 10-13 owning a mobile. Access to home assistant devices and the use of connected toys or devices (for example, fitness trackers or robot toys) are less common.

Figure 70: Children's ownership of devices and social media accounts

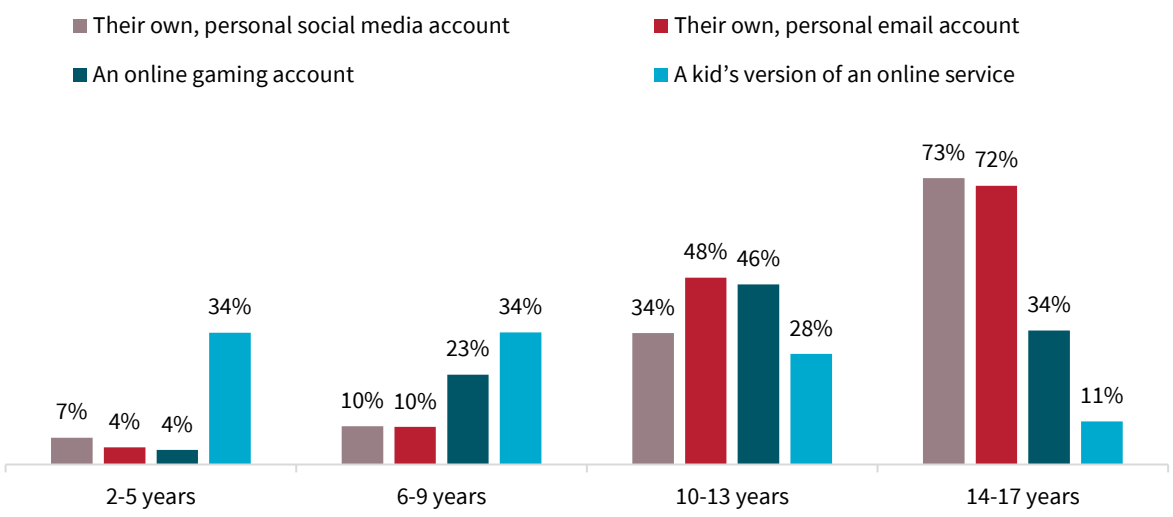


C3. To your knowledge, which of the following do they currently have? Base: Australian parents of children 2-5 years (n=223), 6-9 years (n=173), 10-13 years (n=173), 14-17 years (n=220)

Use of online accounts and services by children

Around a third (34%) of children aged 10-13 have their own social media account, rising to 73% of those aged 14-17. Half (48%) of children aged 10-13 have their own personal email account, rising to 72% of those aged 14-17. Online gaming accounts, such as Fortnite or Minecraft, peak at ages 10-13, the same age that the use of children's versions or restricted versions of online services, such as YouTube Kids or Facebook Messenger Kids, starts to diminish.

Figure 71: Children's online accounts



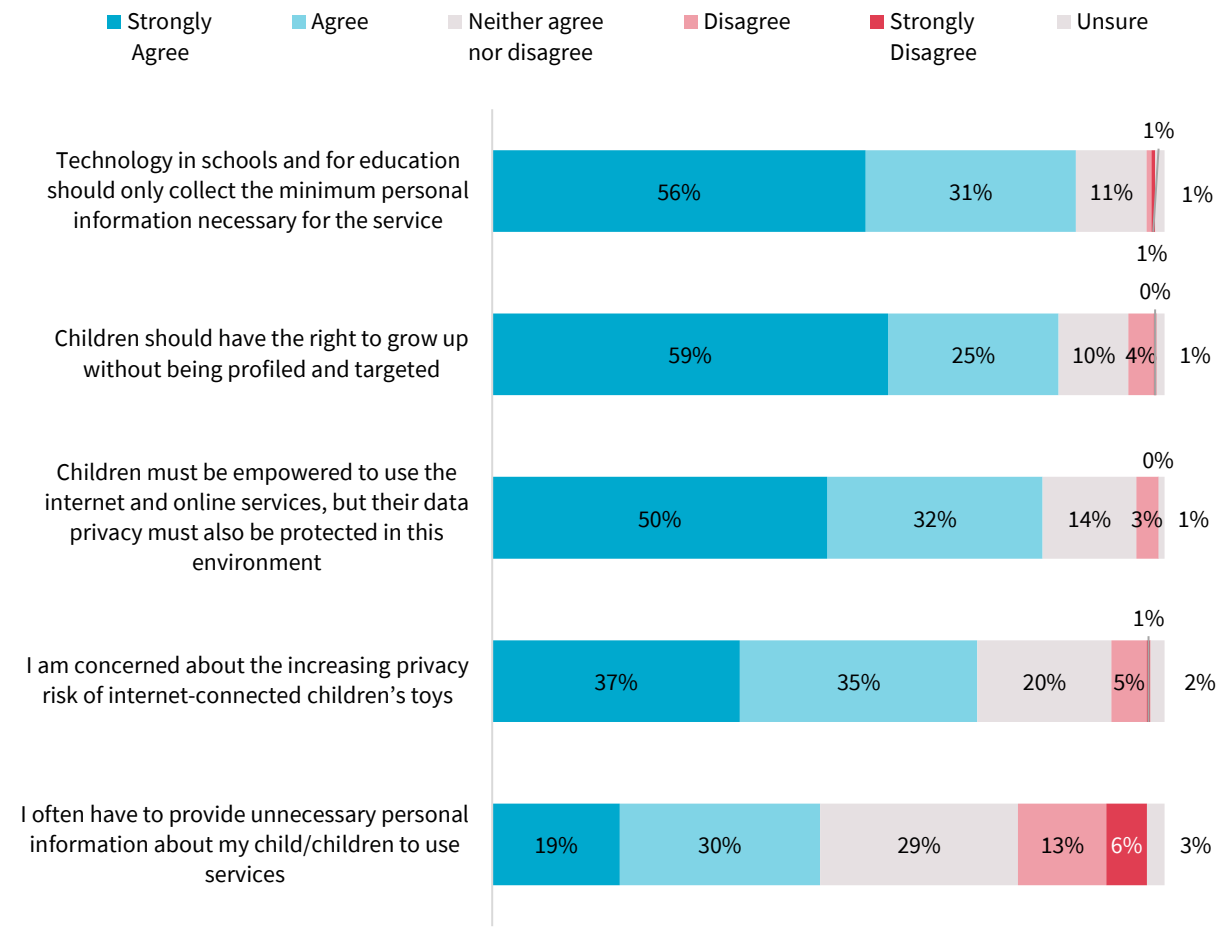
C3. To your knowledge, which of the following do they currently have? - Ownership of devices and social media accounts. Base: Australian parents of children 2-5 years (n=223), 6-9 years (n=173), 10-13 years (n=173), 14-17 years (n=220)

Attitudes to children's privacy

The majority of parents (82%) believe children must be empowered to use the internet and online services, but their data privacy must also be protected in this environment – a view held more strongly by parents of boys (85%) than girls (79%). Over 4 in 5 parents (84%) believe children should have the right to grow up without being profiled and targeted.

Half (49%) of parents agree they often have to provide unnecessary personal information about their child/children to use services (19% disagree). This may be a causal factor in why the majority (87%) of parents consider that technology used in schools and for education purposes should only be collecting the minimum amount of personal information necessary for the service.

Figure 72: Parents' beliefs on children's data privacy



C13. Thinking about children's data privacy, to what extent do you agree or disagree with each of the following statements? Base: Australian parents (n=789)

Measures implemented by parents to protect their child's privacy

Parents of children up to 5 years of age are the least likely to take any measures to protect their child's personal information. When they do, they tend to use parental control software (33%) or restricted access to specific apps, programs or websites (32%).

Parents implement more protective measures after their child turns 6. This includes an increased use of passwords (40% 6-8 years cf. 32% 2-5 years), banning the use of certain apps, programs or websites (50% 6-8 years cf. 21% 2-5 years), talking to them about the risks of the internet (51% 6-8 years cf. 18% 2-5 years) and checking privacy settings are set appropriately (41% 6-8 years cf. 22% for 2-5 years).

The most measures are taken by parents of children aged 9-11. This is the age when parents most commonly talk to their children about the risks of the internet (78%), check that privacy settings are set appropriately (56%) and ban the use of certain apps, programs or websites (51%).

Figure 73: Measures taken to protect child's privacy

% parents taking each measure by age of child	2-5 years	6-8 years	9-11 years	12-14 years	15-17 years
Device restriction settings					
Use a password to restrict unsupervised access to a device	28%	40%	34%	33%	23%
Use a parental control software	33%	37%	23%	28%	19%
Restricted access to specific apps, programs or websites	32%	40%	36%	36%	27%
Talk and Interactions					
Banned the use of certain apps, programs or websites	21%	50%	51%	46%	24%
Talked to them about the risks of the Internet	18%	51%	78%	66%	65%
Restrict internet access to devices in public parts of the household	17%	29%	30%	28%	16%
Details privacy verifications					
Checked the privacy settings are set appropriately	22%	41%	56%	41%	29%
Read the terms and conditions of any apps or programs they use or have downloaded	18%	31%	30%	25%	23%
None of the above	27%	10%	9%	9%	21%

C4. Thinking just about this child and their use of digital devices. What measures are you currently taking, if any, to protect [his/her] privacy? Base: Australian parents of children 2-5 years (n=223), 6-8 years (n=134), 9-11 years (n=114), 12-14 years (n=138), 15-17 years (n=180)

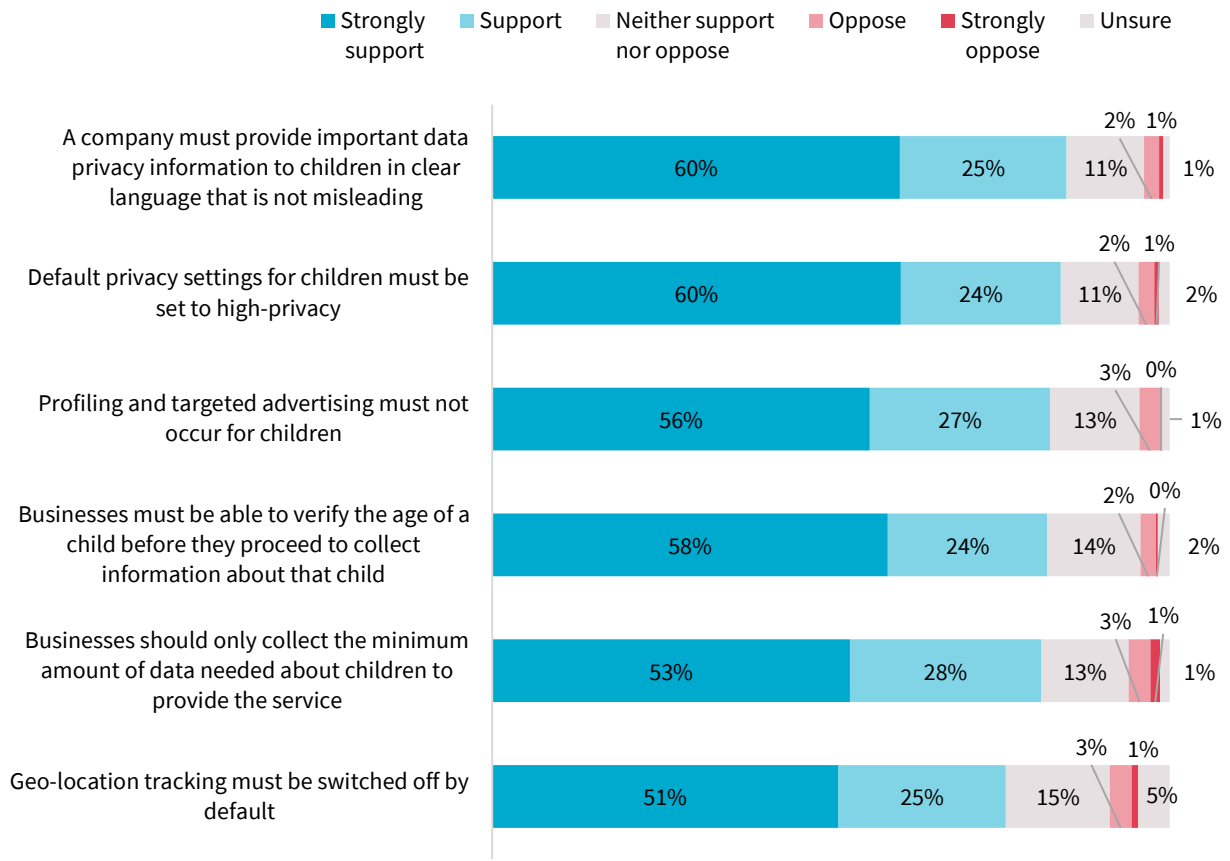
Measures to increase children's data privacy online

The majority of parents strongly support more restrictions on companies and devices to protect the data privacy of children online – all measures listed are supported by at least 3 in 4 parents and strongly supported by more than half. Furthermore, there are very low levels of opposition to all the tested measures.

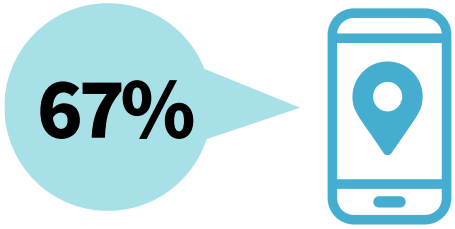
Parents are most likely to support the compulsory provision of important data privacy information to children in clear language that is not misleading (85% support, 60% strongly support). Support for this measure is strong across the board and highest for children aged 14-17 (90%), who are more likely to be managing their own privacy.

There is slightly less support (76%) for geo-location tracking to be switched off by default.

Figure 74: Measures to increase the data privacy of children online



C12. How much do you support or oppose each of the following measures to increase the data privacy of children online? Base: Australian parents (n=789)

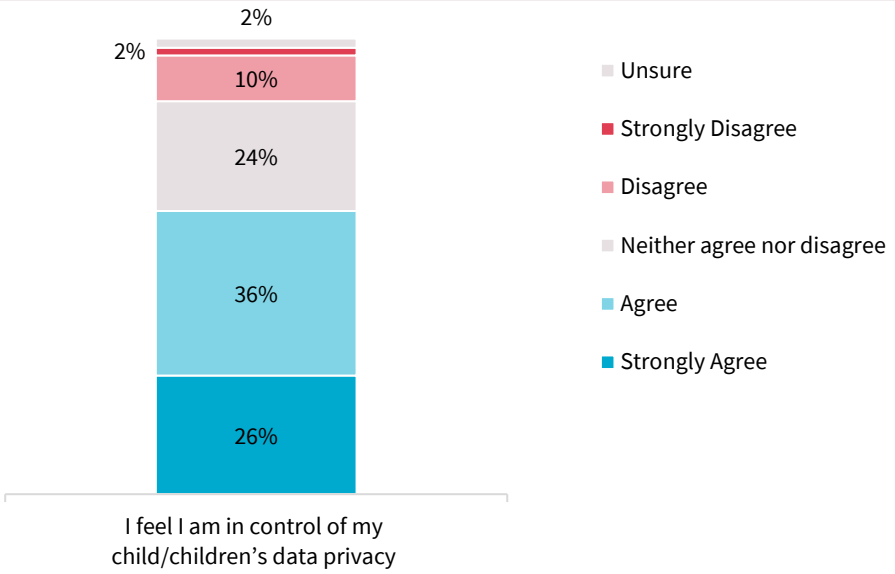


67% of parents are uncomfortable with businesses tracking their child's location without their permission or selling their information to third parties

Perceptions of control over children's privacy

While parents are concerned about their children's data privacy, the majority (62%) feel that they are in control of their child/children's data privacy and only 12% don't think they have control. These numbers are similar across ages and gender of children.

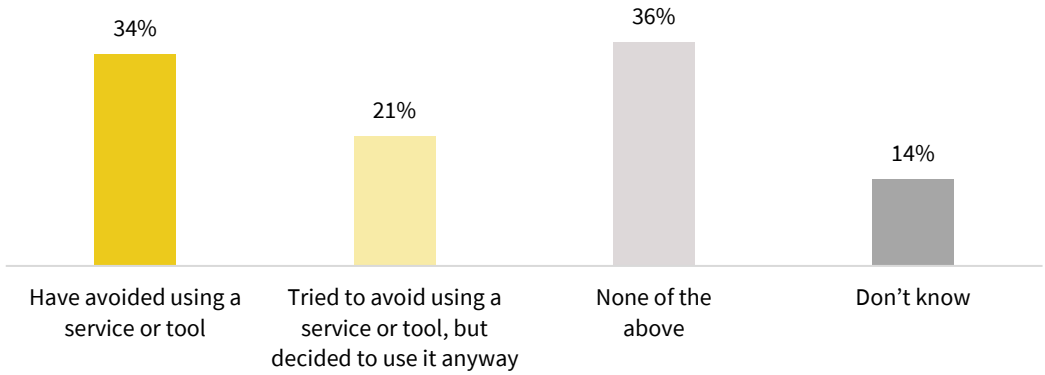
Figure 75: Proportion of parents who feel they are in control of their child's data privacy



C13. Thinking about children's data privacy, to what extent do you agree or disagree with each of the following statements? Base: Australian parents (n=789)

Overall, a third of parents have avoided using a service or tool to protect their child's personal information. One in 5 (21%) have tried to avoid using a service or tool to protect their child's personal information but decided to use it anyway. This is much higher (37%) among parents of children who have a connected toy or device (such as a Fitbit or a robot toy).

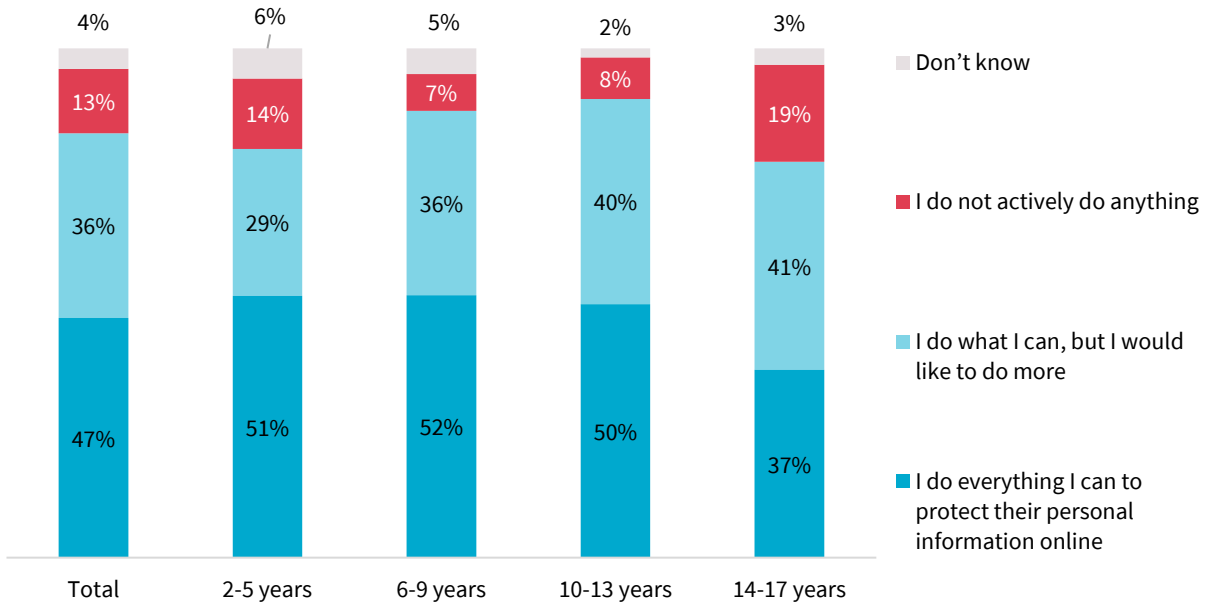
Figure 76: Parents who avoided using a service to protect their child's personal information



C7. Have you ever avoided, or tried to avoid using a service or tool to protect your [child's] personal information? Base: Australian parents (n=789)

Half of parents (47%) believe that they are doing everything they can to protect the personal information of their child and only 13% do not actively do anything about this, a pattern which holds until children reach their mid-teenage years (14-17 years).

Figure 77: Parents protecting child's personal information online

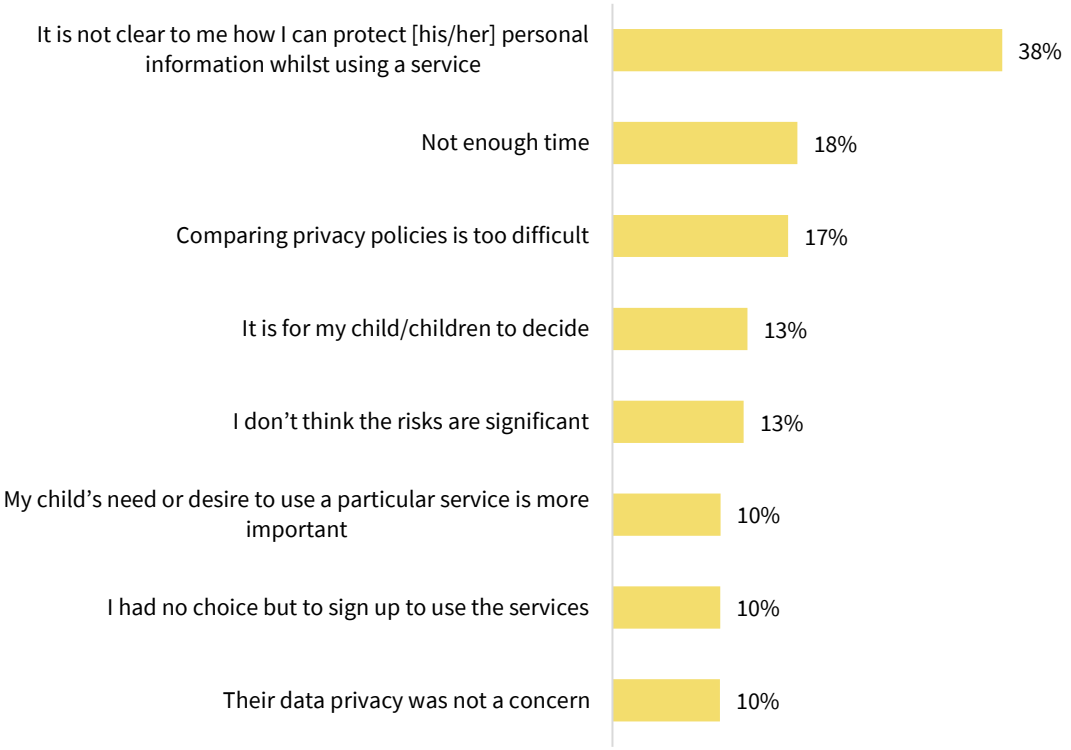


C8. Thinking about protecting your child's personal information online, which of the following best applies to you? Base: Australian parents of children 2-5 years (n=223), 6-9 years (n=173), 10-13 years (n=173), 14-17 years (n=220)

Reasons for not doing more to protect their child's privacy

Of those who acknowledge they are not doing everything they can, the top reasons for not doing so across all age groups and demographics are lack of knowledge, lack of time and the difficulty of the process. Two in 5 (38%) parents feel it is not clear to them how they can protect the personal information of their child while using a service. This is likely intertwined with being time poor (18%) and finding the task of comparing policies too difficult (17%).

Figure 78: Reasons for not doing more to protect personal information of their child



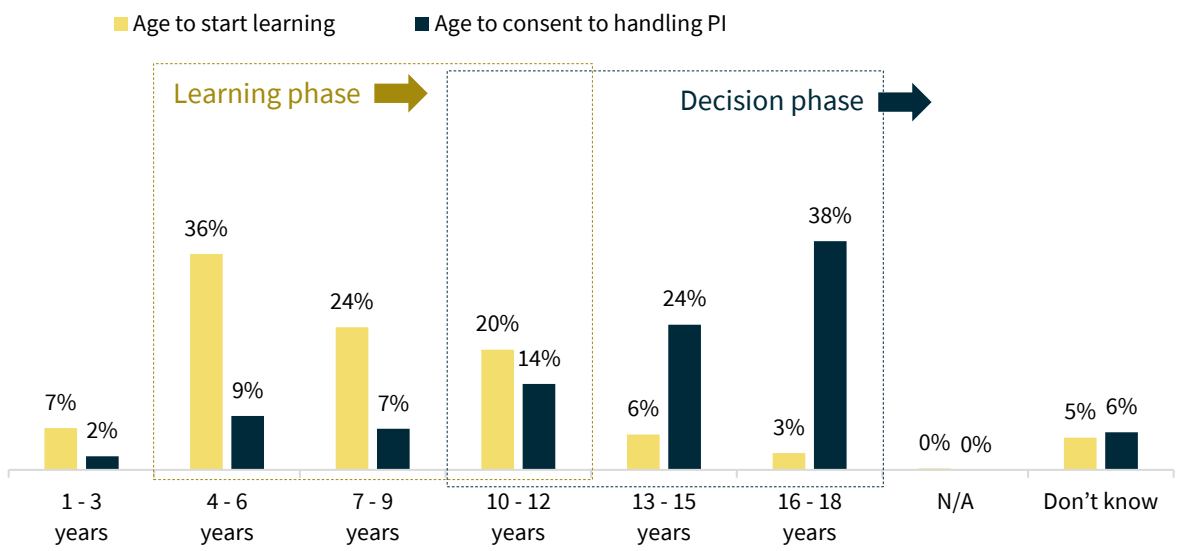
C9. What are the main reasons for not doing more to protect the personal information of your child? Base: Parents who are not doing everything they can to protect the privacy of their children (n=420)

The ideal age for children to take responsibility for their own privacy

The average age parents believe children should be able to consent to handing over their personal information in exchange for an online service is 13 years and 62% consider it should be after the age of 13.

Parents believe children should start learning about data privacy earlier, at an average age of 8. Two-thirds (66%) of parents believe children should start learning about this before the age of 10. No parents in our survey (0%) considered that there was no need for them learn about privacy.

Figure 79: Appropriate age for children to start learning about data privacy

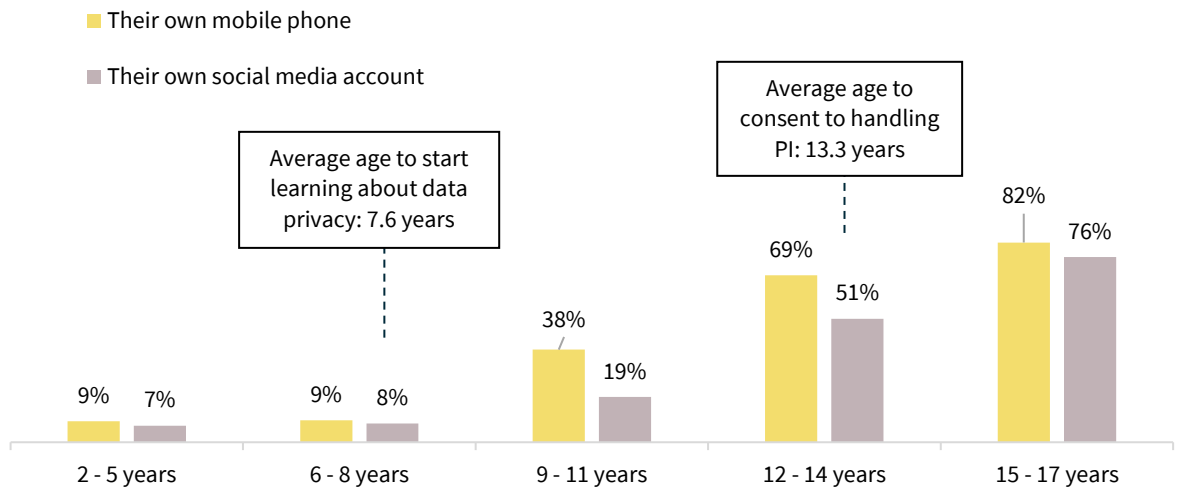


C10. At what age do you think is most appropriate for children to start learning about data privacy and the protection of their personal information?

C11. What age do you think is most appropriate for your child to consent to handing over their personal information in exchange for an online service? Base: Australian parents (n=789)

The average age a child acquires a mobile phone is 13.1 years. This is also very close to the average age (13.3 years) parents consider it appropriate for a child to consent to handing over their personal information in exchange for an online service. Nineteen percent of children have their own mobile phone and 13% have their own social media account before the age of 13.

Figure 80: Children's ownership of devices and social media accounts



C3. To your knowledge, which of the following do they currently have? - Ownership of devices and social media accounts Base: Australian parents (n=789)

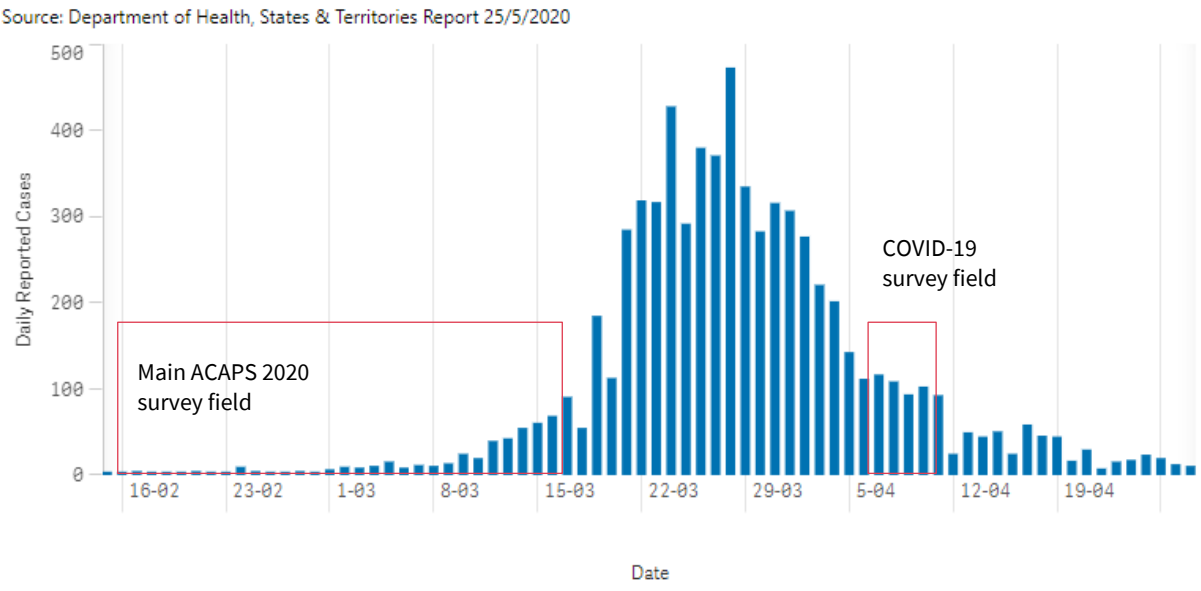
Part 7: Attitudes to privacy in the context of the COVID-19 outbreak

The majority of the fieldwork for the main survey was conducted prior to the COVID-19 pandemic having a significant impact on Australians. As reporting for the survey got underway, physical distancing rules were enacted and enforced in all Australian states and territories. In-person school attendance significantly shifted to remote learning and workplaces shifted to work from home where possible. Australians used different ways to work, study and stay in touch with their loved ones and adapted their routine with activities that can be done at home rather than outside. Increased use of telehealth was also facilitated.

The change in behaviours had a series of privacy implications, with many Australians being required by circumstances to use a large range of new digital tools. Furthermore, governments around the world and in Australia sought data and technology approaches to prevent and manage the spread of COVID-19, encompassing both the treatment and management of patients and measures to prevent the disease spreading.

To understand how these unprecedented circumstances were impacting Australian views on privacy, an additional survey to the main ACAPS was conducted between 7 April and 9 April 2020.

Figure 81: ACAPS fieldwork timelines in relation to timelines of confirmed COVID-19 cases in Australia



https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert/coronavirus-covid-19-current-situation-and-case-numbers

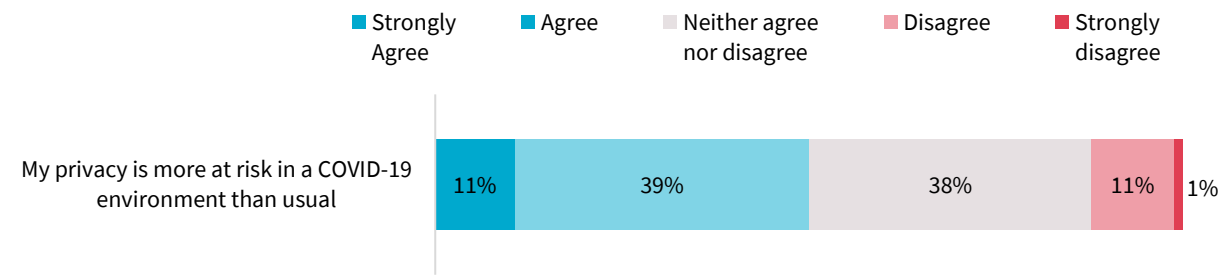
The additional survey found the majority of Australians (60%) agree that some concessions must be made to privacy protections to combat COVID-19 for the greater good. The same proportion (60%) agree that these concessions can be made so long as they are not permanent. Three-quarters (75%) of Australians believe COVID-19 does not excuse business or government from meeting their usual obligations under privacy laws.

COVID-19 has required those Australians who can, to work or study from home, necessitating greater reliance on new and existing technology. While Australians tend to trust the new digital services they have been using, the speed of change has left many Australians unaware of the privacy implications of the services they use. Australians are, however, more likely to read the privacy policies of the apps they have downloaded as a result of COVID-19 and they are increasingly vigilant when it comes to their location data.

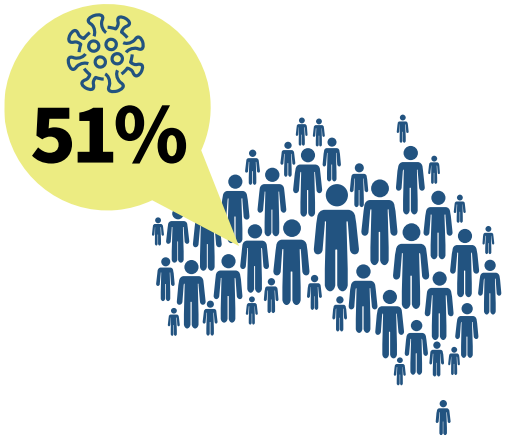
Concerns over privacy in a COVID-19 environment

Half (50%) of Australians agree that their privacy is more at risk in a COVID-19 environment than usual. This is driven by over half (55%) of males and 3 in 5 young Australians (62%) and students (64%), who are all significantly more likely than their counterparts to feel this way. Comparatively 45% of females, 48%, of 35-49-year-olds and 42% of those over 50 feel the same way.

Figure 82: Privacy concerns since COVID-19



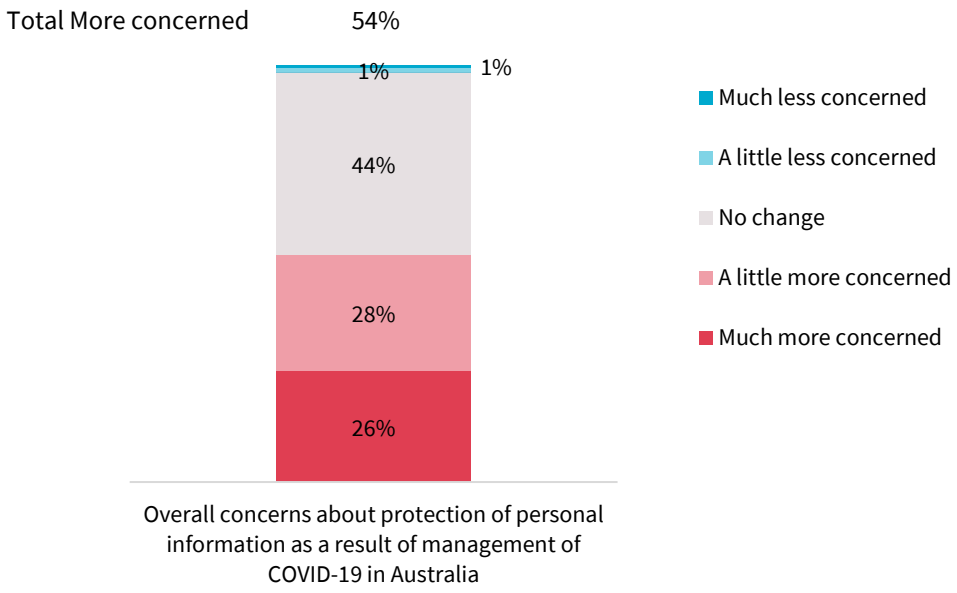
A10. To what extent do you agree or disagree with each of the following statements? Base: Australians 18+ (n=1004)



Over half of all Australians are more concerned about the protection of their personal information following the COVID-19 outbreak

Over half (54%) of Australians are more concerned about the protection of their personal information as a result of the management of COVID-19 in Australia, including a quarter (26%) who are much more concerned. Australians who reside in capital cities are more likely than their counterparts to be more concerned (58%; rest of Australia 48%), as are younger Australians with two-thirds (68%) being concerned compared to 55% of those aged 35-49 and 44% of older Australians (50+ years).

Figure 83: Changes in concerns about the protection of their personal information overall

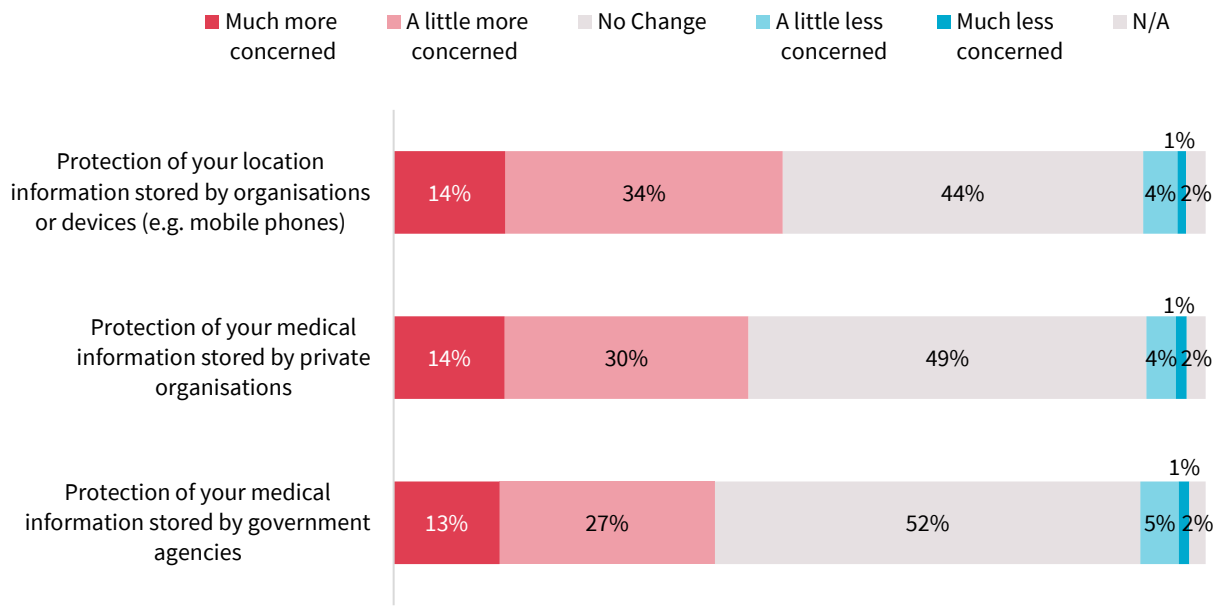


A1. How much more or less concerned are you about the protection of your personal information overall as a result of the management of COVID-19 in Australia? Base: Australians 18+ (n=1004)

Almost half (48%) of Australians are more concerned about the protection of their location information as a result of COVID-19, followed by their medical information stored by private organisations (44%) and their medical information stored by government agencies (40%).

Concerns around the protection of medical information have not changed for nearly half of Australians (49% where stored by private organisations, 52% where stored by government agencies). A small minority is less concerned about the protection of all these types of information during the pandemic than they were before the start of the pandemic.

Figure 84: Concerns about protection of personal information since the COVID-19 outbreak



A8. Since the COVID-19 outbreak began, do you feel more or less concerned about each of the following? Base: Australians 18+ (n=1004)

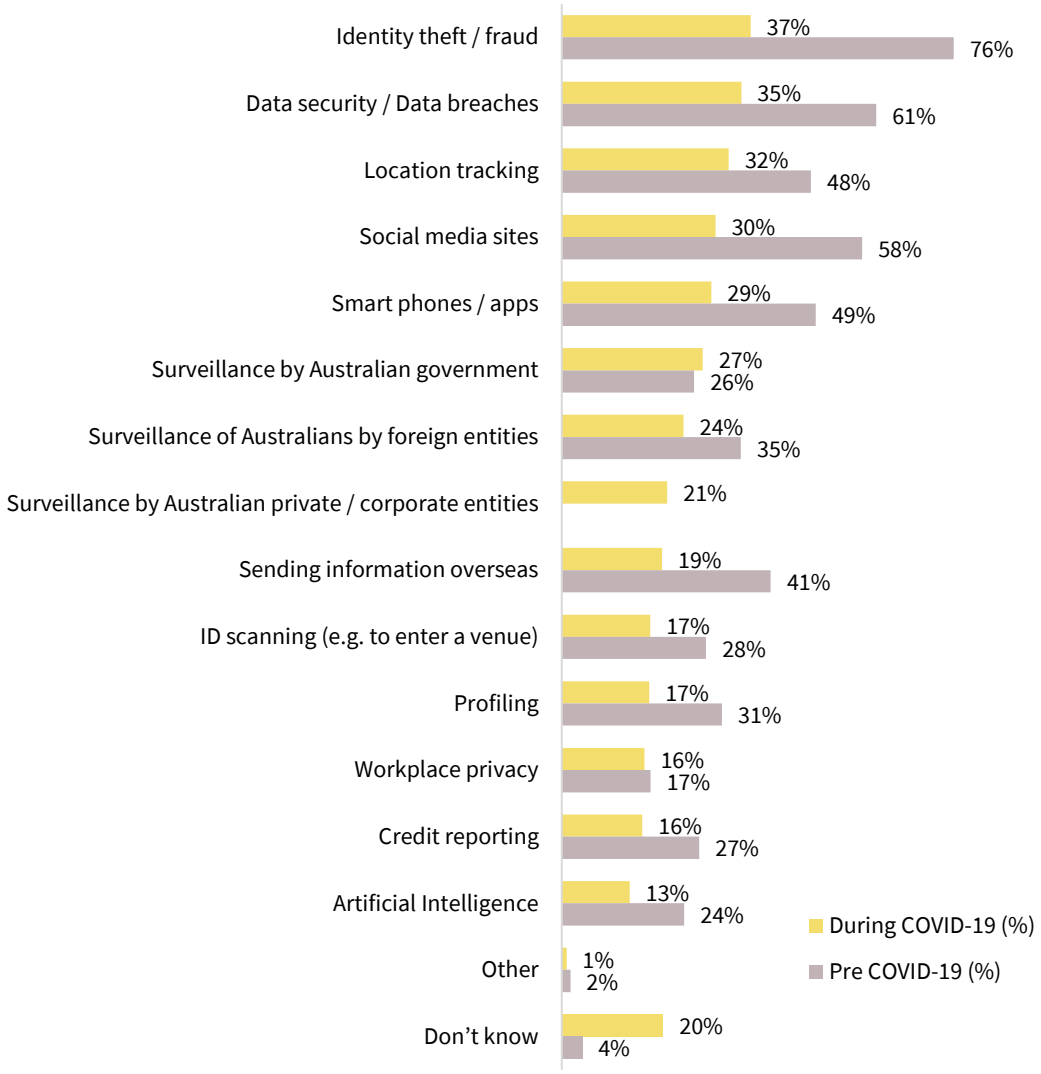
Perception of privacy risks

The biggest privacy risks perceived by Australians have changed since the outbreak of COVID-19. Location tracking is now the third biggest privacy risk perceived by Australians. It was previously ranked fifth.

Surveillance by the Australian Government is ranked higher as a concern since the outbreak of COVID-19. It was perceived as the 11th biggest risk prior to COVID-19 and is now the sixth biggest risk. Workplace privacy has risen by two places (from 13th pre-COVID to 11th in the context of COVID-19).

The top two concerns remain identity theft/fraud (ranked first) and data security/breaches (ranked second).

Figure 85: Biggest privacy risks people face in the context of COVID-19 crisis

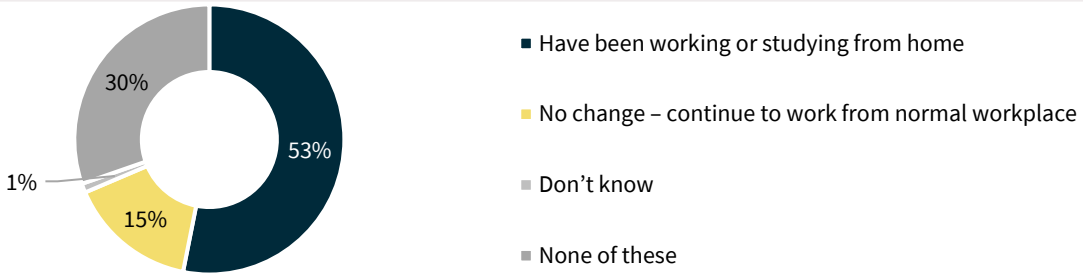


A2. What do you think are the biggest privacy risks that face people in the context of the COVID-19 crisis? Base: Australians 18+ (n=1004) / A8. What do you think are the biggest privacy risks that face people today? Base: Australians 18+ (n=1,510)

Change in behaviour in Australian households

At least 53% of Australians had at least one person in their household having to work or study at home as a result of the pandemic.

Figure 86: Proportion of Australians working or studying from home as a result of COVID-19

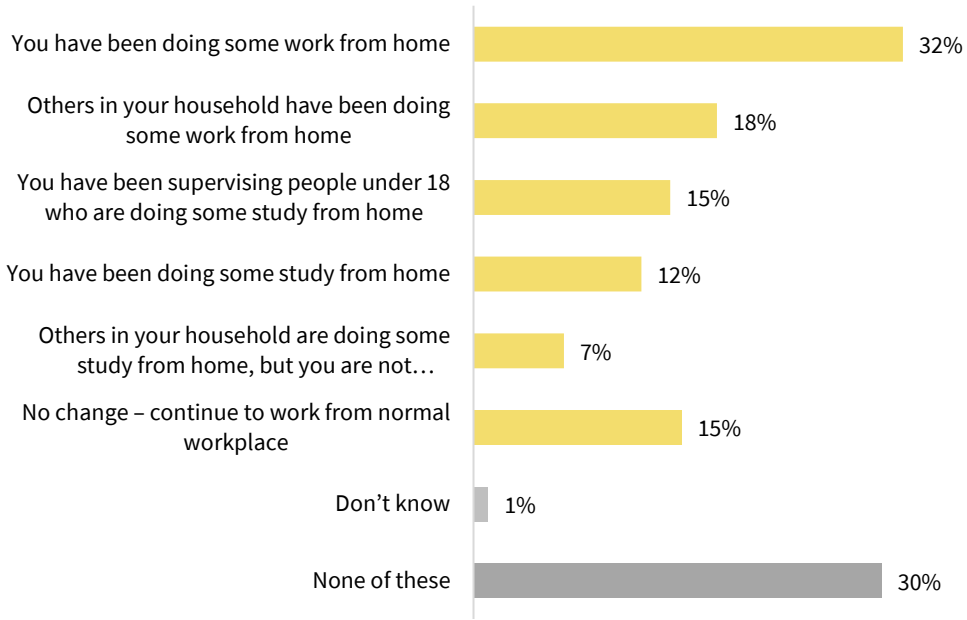


A3. Since the COVID-19 pandemic began, which of the following apply to you? Base: Australians 18+ (n=1004)

This includes 2 in 5 Australians (40%) who have been doing some work from home or have had others in their household working from home. Australians who reside in capital cities (47%) and young Australians (56%) are the most likely to have worked from home, compared to those who live in regional areas (29%) and older Australians aged 35-49 years (47%) and 50+ years (25%).

Fifteen percent of Australians continued to work from their normal workplace, which increased to a quarter among full-time workers (24%) and those aged 35-49 (22%), while only 11% of younger Australians aged 18-34 years and 15% of those aged 50 or over continued to work from their normal workplace.

Figure 87: Changes in work/study made since the COVID-19 pandemic



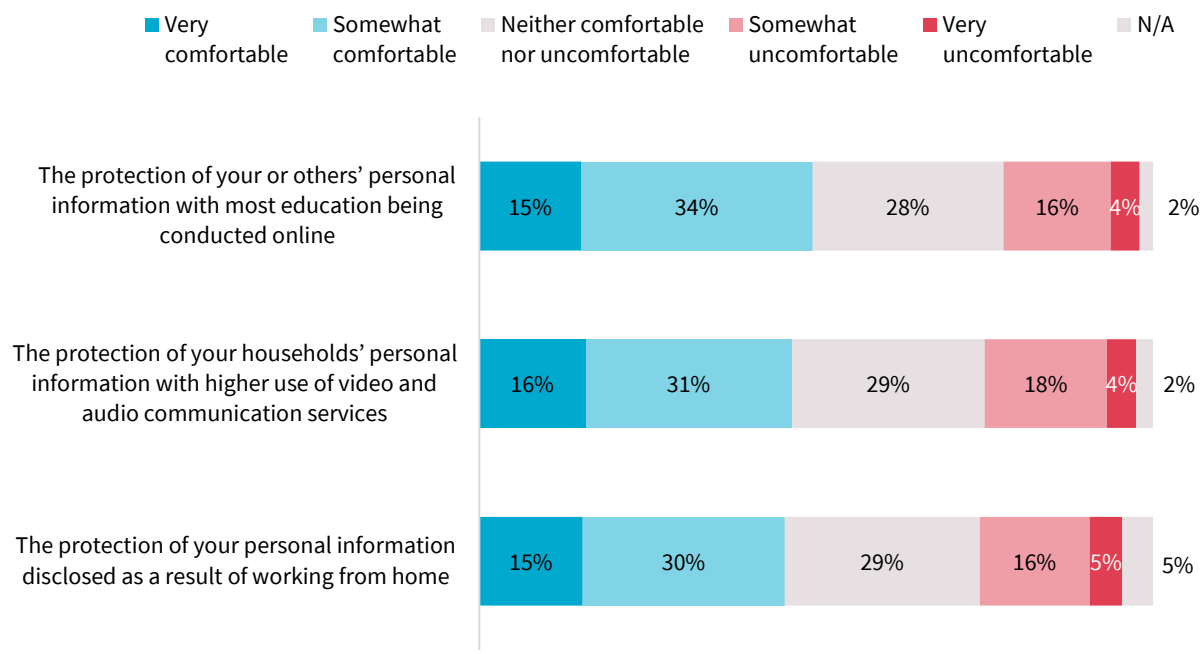
A3. Since the COVID-19 pandemic began, which of the following apply to you? Base: Australians 18+ (n=1004)

Attitudes to protection of personal information while at home

Australians are more likely to feel comfortable than uncomfortable with the protection of their personal information while using digital services at home in the midst of the COVID-19 pandemic, whether it is for work, studying or personal use (45% to 49% comfortable; cf. 20% to 22% uncomfortable). However, close to 1 in 5 feel uncomfortable.

Those studying at home are more likely to feel comfortable with the protection of their personal information (49% comfortable, 20% uncomfortable) than those working from home (45% comfortable, 21% uncomfortable). Half (46%) of workers are comfortable with the protection of their households' personal information with higher use of video and audio communication services (22% uncomfortable).

Figure 88: Comfort with protection of personal information while working/studying at home



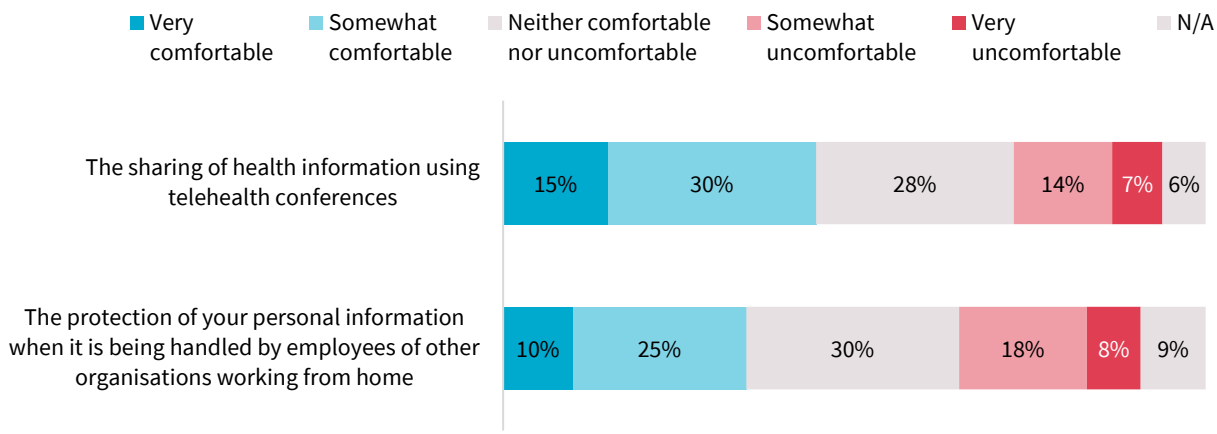
A4. How comfortable do you feel about the following aspects of your privacy, with some members of your household working and / or studying from home? Base: Australians who are working or studying from home (household or themselves) (n=528) Australians who are studying from home (household or themselves) (n=272)

Over a third of Australians (35%) are comfortable with employees of other organisations handling their personal information while these employees work from home, however 25% are uncomfortable with this.

Males (39%) are more comfortable with the protection of their personal information when it is being handled by employees of other organisations working from home than females (30%), as are full-time workers (47%) compared to others (28%). Younger Australians (50%) are twice as likely as the oldest Australians (21%) to feel comfortable and are more likely than those aged 35-49 years (39%).

Almost half (45%) of Australians are comfortable with the sharing of health information using telehealth conferences. This is also driven by full-time workers (53%; cf. others 40%) and younger Australians, with 54% feeling comfortable compared to 2 in 5 of their older counterparts, those aged 35-49 (43%) and those older than 50 (39%).

Figure 89: Comfort with protection of personal information in telehealth conferences or by employees working from home



A5. Since the COVID-19 outbreak began, there have been many changes in the way people work, across a large number of companies and government departments. In this context, how comfortable or uncomfortable are you with? Base: Australians 18+ (n=1004)

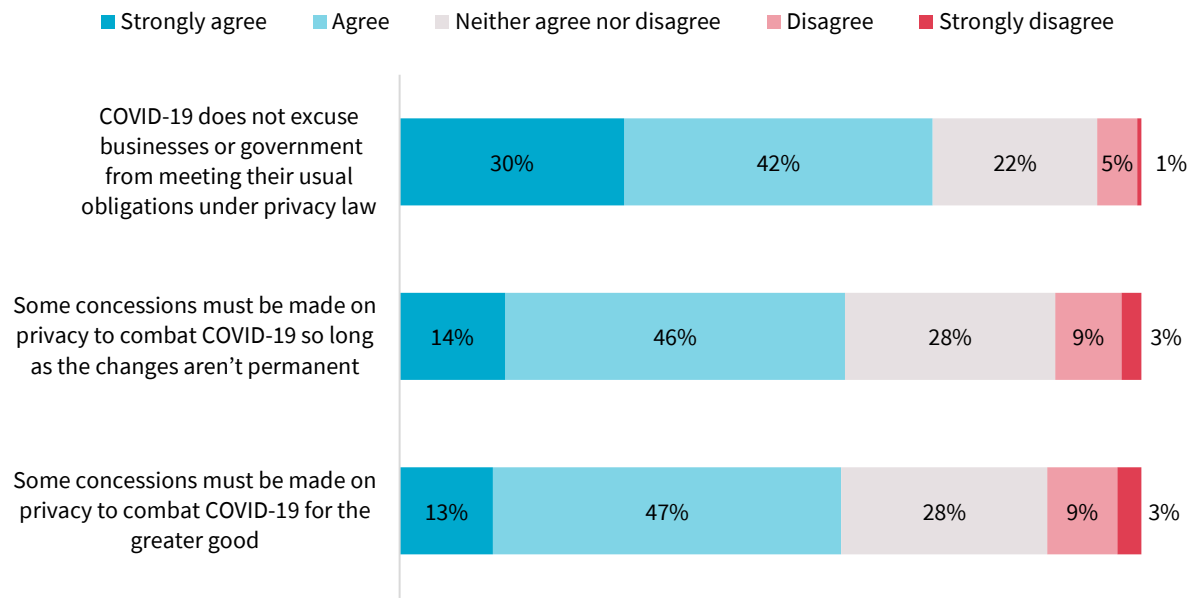
Privacy concessions during the COVID-19 outbreak

The majority of Australians (60%) agree that some privacy concessions must be made to combat COVID-19 for the greater good. The same proportion agree that some concessions must be made so long as the changes are not permanent (60%; cf. 12% disagree).

There is a strong belief among Australians that COVID-19 does not excuse business or government from meeting their usual obligations under privacy laws, with close to three-quarters (72%) agreeing with this sentiment.

Older Australians (50+ years) are more likely to feel some concessions must be made on privacy to combat COVID-19 as long as they are not permanent (64%), this is followed by 18-34 year-olds (60%) and then by those aged 35-49 (54%). There is also a correlation between age and the agreement that COVID-19 does not excuse the government from meeting their usual obligations under privacy laws, with three-quarters (76%) of those 50+ years old agreeing, followed by 71% of those aged 35-49 and 67% of 18-34 year-olds.

Figure 90: Beliefs around the concessions that must be made during the COVID-19 outbreak

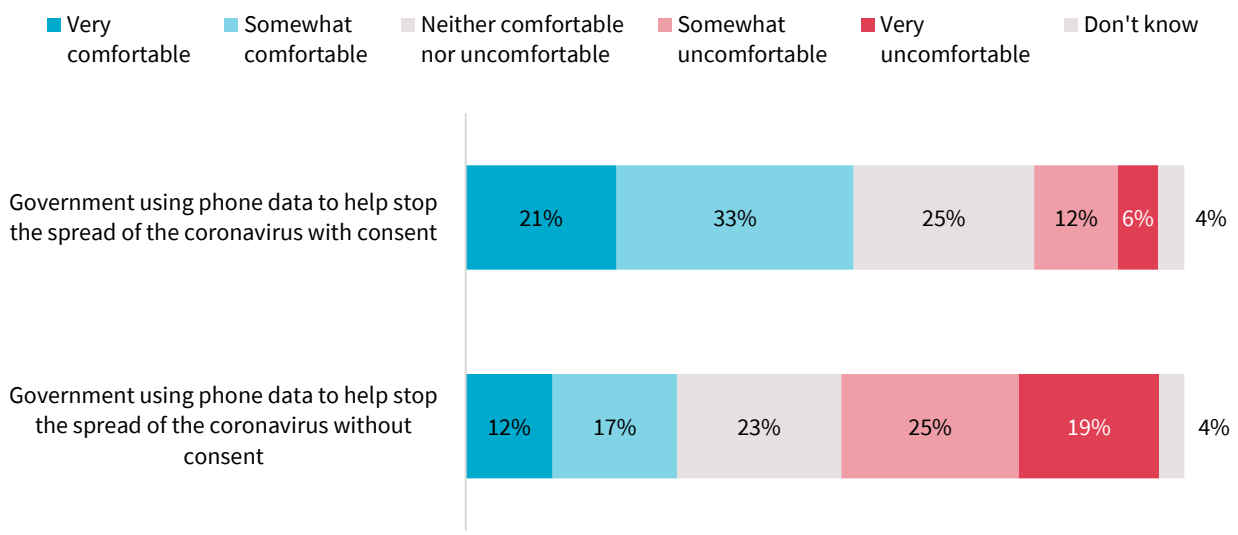


A10. To what extent do you agree or disagree with each of the following statements? Base: Australians 18+ (n=1004)

Over half (53%) of Australians are comfortable with their personal information, including health information being shared to combat coronavirus, while 19% are uncomfortable. Levels of comfort are much lower with the government using the same data practice without users' consent (29% comfortable and 44% uncomfortable).

Males are much more likely to be comfortable with government using phone data without consent to help stop the spread of the coronavirus (36%; cf. females 23%). There are few differences across other demographics.

Figure 91: Comfort with organisations using phone data to stop COVID-19 with or without consent



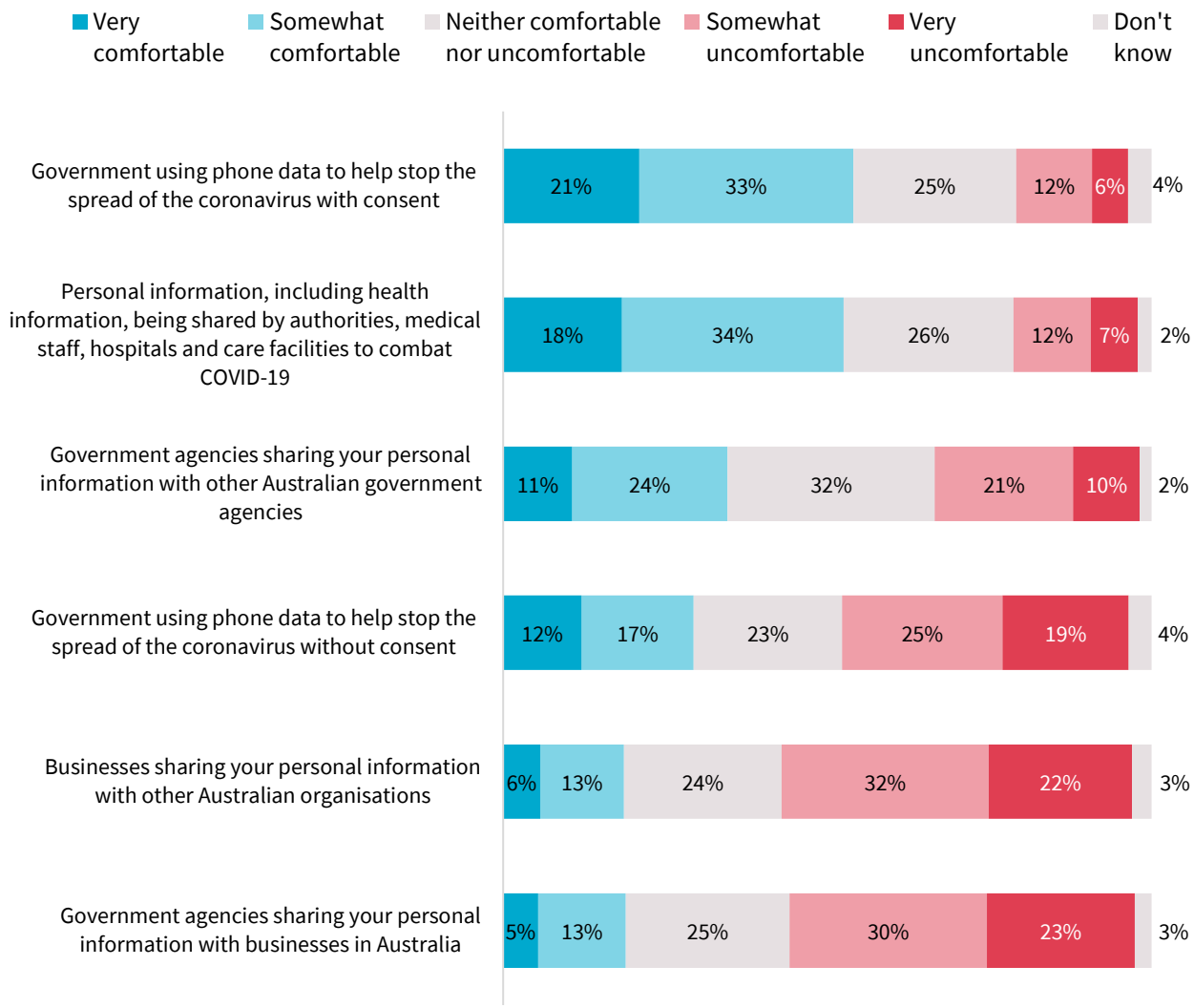
A6. Overall, considering all the changes as a result of COVID-19, how comfortable or uncomfortable are you with each of the following? Base: Australians 18+ (n=1004)

Australians are more divided on their levels of comfort with government agencies sharing their personal information with other Australian government agencies, with a similar proportion comfortable (35%) as uncomfortable (32%).

Levels of comfort with information sharing are slightly higher during the COVID-19 pandemic than immediately prior to it, and levels of discomfort are lower. There is a higher proportion of Australians who are neutral about each action, which may reflect a population still coming to terms with the privacy implications of the evolving government response to COVID-19.

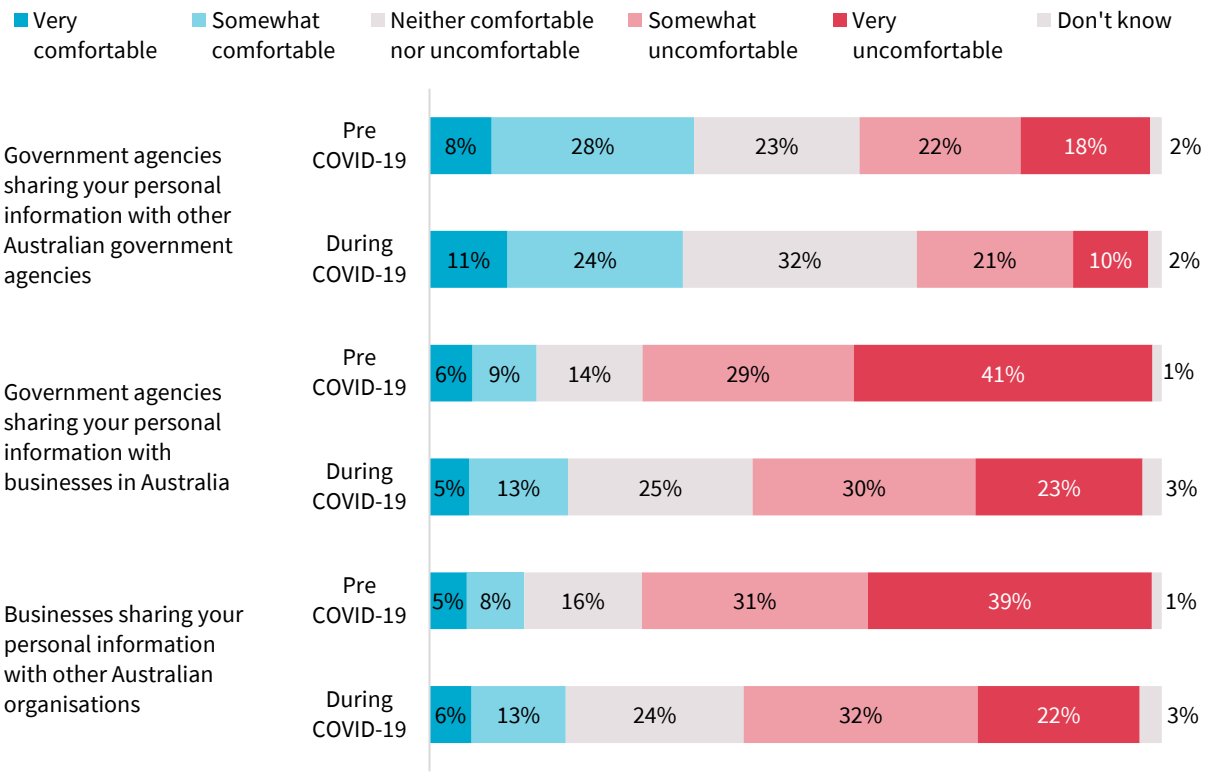
When Australian businesses are introduced, Australians are much more likely to become uncomfortable. Fewer than 1 in 5 Australians (19%) are comfortable with government agencies sharing personal information with businesses in Australia with the majority (53%) uncomfortable. The same proportion (19%) are comfortable with businesses sharing personal information with other Australian organisations, with 54% uncomfortable.

Figure 92: Comfort with different organisations sharing personal information



A6. Overall, considering all the changes as a result of COVID-19, how comfortable or uncomfortable are you with each of the following? Base: Australians 18+ (n=1004)

Figure 93: Comfort levels with organisations sharing personal information before and during COVID-19



A6_During COVID-19. Overall, considering all the changes as a result of COVID-19, how comfortable or uncomfortable are you with each of the following? Base: Australians 18+ (n=1,004) / B14. How comfortable or uncomfortable are you with… Base: Australians 18+ (n=1,506)

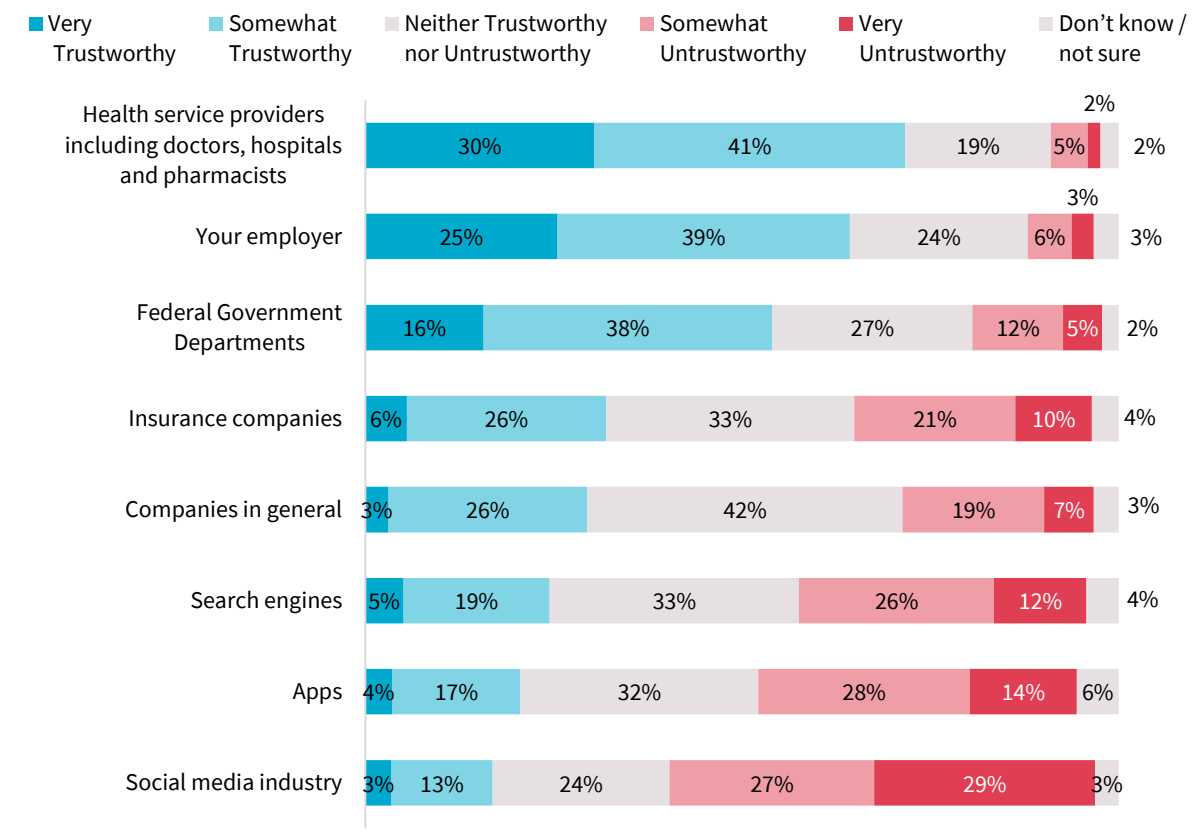
Implications for trust in organisations

Health service providers are the most trusted organisations with regard to how they protect Australians' personal information during the COVID-19 outbreak (72% trustworthy), followed by their employer (64% trustworthy) and Federal Government Departments (54% trustworthy).

Roughly the same proportion of Australians trust as distrust insurance companies (32% trustworthy, 32% untrustworthy) and companies in general (29% trustworthy, 25% untrustworthy). However, Australians are less likely to trust search engines (24% trustworthy, 38% untrustworthy), apps (21% trustworthy, 42% untrustworthy) and the social media industry (17% trustworthy, 58% untrustworthy).

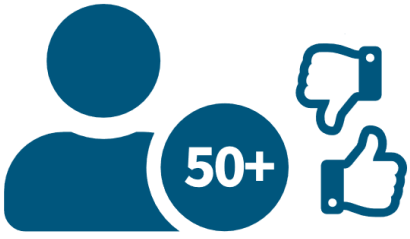
Younger Australians are more likely to trust digital services (27% of 18-34 and 22% of 35 to 49-year-olds cf. 7% of those 50 years or older do so). They are also more likely to trust search engines (33% of 18 to 34 and 28% of 35 to 49 year-olds cf. 16% of those 50 and over) and apps (32% of 18 to 34 and 24% of 35 to 49 year-olds cf. 10% of those 50 and over). However, employers are more likely to be trusted by Australians aged 50 and over (72%) than younger Australians (66% of those 35 to 49 and 57% of those 18 to 34).

Figure 94: Trust in organisations with regard to how they protect personal information in the context of the COVID-19 crisis



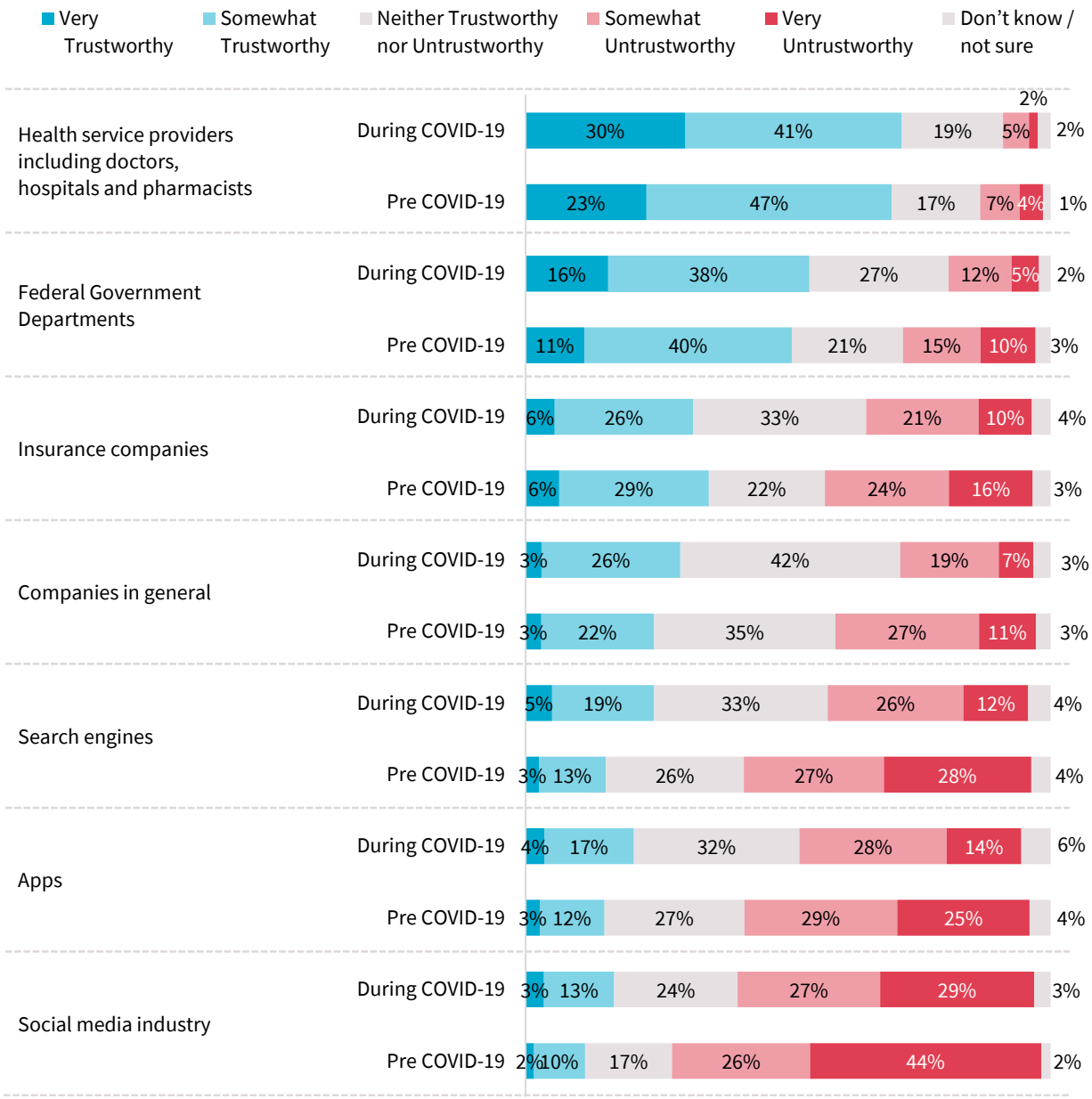
A9. Thinking now about trustworthiness. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information in the context of the COVID-19 crisis? Base: Australians 18+ (n=1,004)

Except for insurance companies (where the overall pattern is unclear), the proportion who trust each organisation type has increased slightly, whereas the proportion who distrust each organisation type has dropped more substantially. Notably, trust in Federal Government Departments has increased 3% and distrust has dropped 8%. Trust in search engines has increased 9%, with distrust down by 17%. Trust in the social media industry is up 6%, with distrust down by 14%.



Australians 50+ trust digital services, search engines and apps the least in the context of COVID-19, and trust employers the most

Figure 95: Trust in organisations with regard to how they protect personal information before and during the COVID-19 crisis

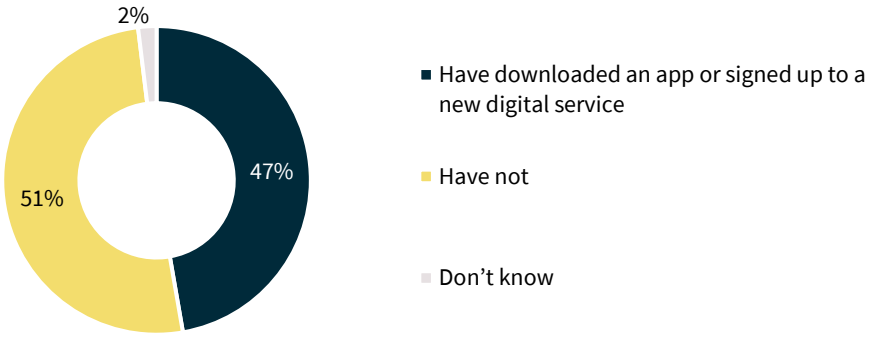


A9. Thinking now about trustworthiness. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information in the context of the COVID-19 crisis? Base: Australians 18+ (n=1004)

Attitudes to digital services during the COVID-19 outbreak

Close to half (47%) of Australians have downloaded an app or signed up to a new digital service as a result of COVID-19. Young Australians (18-34 years, 68%), students (69%), full time workers (57%) and those whose work status has changed as a result of COVID-19 (60%) are substantially more likely to have downloaded an app or signed up to a digital service as a result of COVID-19.

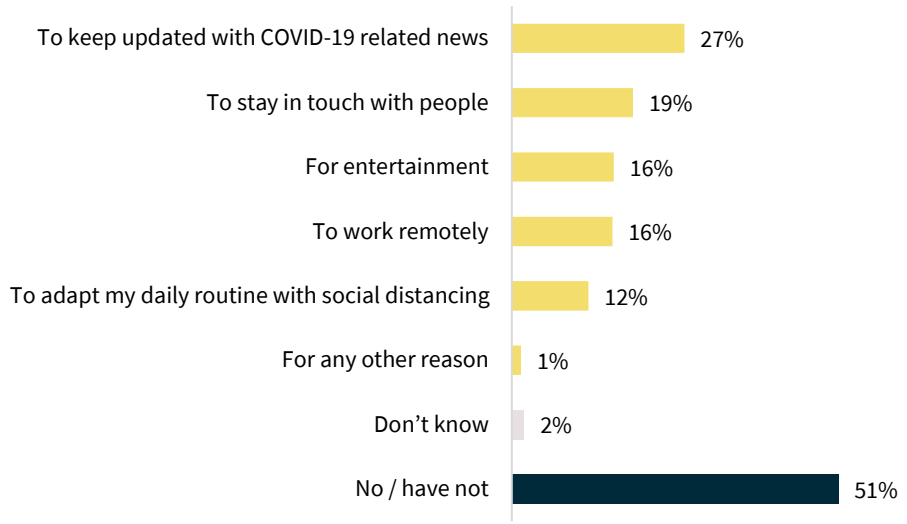
Figure 96: Proportion of Australians who have downloaded an app or signed up to a digital service as a result of COVID-19



A11. Have you downloaded any app or signed up to a new digital service as a result of COVID-19 for any of the following purposes? Base: Australians 18+ (n=1,004)

The main reason for downloading a new app was to keep updated with COVID-19-related news (27%), followed by staying in touch with people (19%), entertainment (16%) or to work remotely (16%). Those who downloaded an app listed on average 1.9 reasons for doing so, suggesting each person may have downloaded multiple apps as a result of COVID-19.

Figure 97: Reasons why apps were downloaded as a result of COVID-19

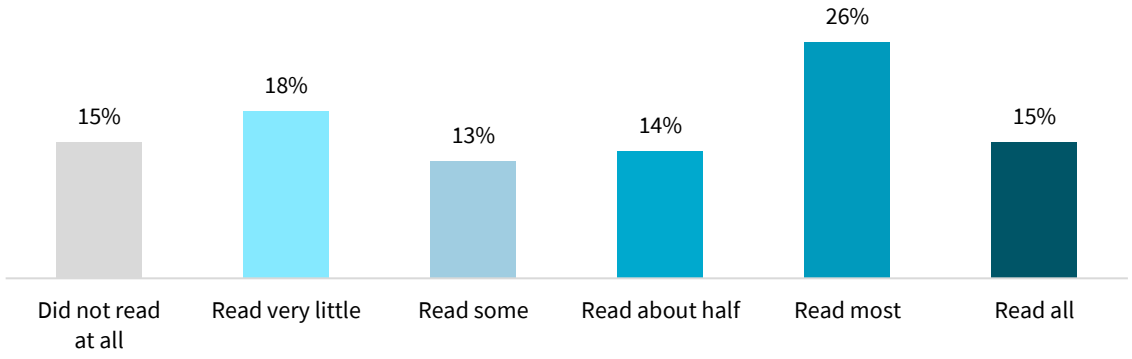


A11. Have you downloaded any app or signed up to a new digital service as a result of COVID-19 for any of the following purposes? Base: Australians 18+ (n=1004)

Of those who downloaded an app or signed up to a digital service since the start of the pandemic, 40% have read most or all of the privacy policies attached to these. This is higher than the proportion of Australians who claimed to normally read privacy policies attached to an internet site before the outbreak (34%).

Forty-five percent of Australians read half or less of the policy and 18% read very little. Over 1 in 10 Australians (15%) did not read the policy at all, with this response higher among females (20%).

Figure 98: Extent to which Australians read the privacy policies associated with new apps and services



A12. How much of the privacy policies associated with these apps or services did you read? Base: Australians who downloaded any app or signed a new digital service as a result of COVID-19 (n=467)

Figures and charts

Figure 1: What privacy means to Australians (unprompted, categorised by researchers) 14
Figure 2: What privacy means to Australians (Word cloud) 16
Figure 3: Percentage of Australians concerned about personal information protection 17
Figure 4: Importance of privacy when choosing a digital service 18
Figure 5: Importance of aspects when choosing an app or program to download 19
Figure 6: Reasons privacy is important in digital services 20
Figure 7: Percentage of Australians who experienced mishandling of personal information 21
Figure 8: Beliefs around the proportion of businesses that use targeted advertising techniques 24
Figure 9: Beliefs around the proportion of smartphone apps that collect information about people who use them — by year 25
Figure 10: Biggest privacy risks Australians are facing today 26
Figure 11: Comfort with information sharing by organisation type 28
Figure 12: Comfort with government agencies sharing information with other Australian government agencies over time 28
Figure 13: Comfort with digital platforms' data practices 29
Figure 14: High discomfort (% very uncomfortable) with digital platform/online business data practices by age 30
Figure 15: How Australians feel about data privacy 31
Figure 16: Levels of comfort of Australians with business use of data 33
Figure 17: Levels of comfort of Australians with government bodies/law enforcement using data 34
Figure 18: Comfort with personal information provided to government agencies and departments being used for research, service development or policy development purposes 35
Figure 19: Australians' beliefs that each data practice is a misuse 37
Figure 20: Proportion of Australians who consider each data practice is a misuse 2013-2020 38
Figure 21: Concerns of Australians regarding their personal information being sent overseas 39
Figure 22: Concerns of Australians regarding their personal information being sent overseas 40
Figure 23: Australians' beliefs about protecting their data 42
Figure 24: Australians' knowledge of data protection and privacy rights 43
Figure 25: Australians' beliefs on protecting their personal information 44
Figure 26: Actions taken by Australians out of concern for their data privacy 45
Figure 27: Australians' participation in data protection activities 46
Figure 28: Measures of protection of privacy always or often taken in 2017 and in 2020 50
Figure 29: Australians' beliefs on data privacy 52
Figure 30: Australians' beliefs about data privacy and businesses 52
Figure 31: The extent to which Australians can access and use data 53
Figure 32: Percentage of Australians who are aware they can request access to personal information 54
Figure 33: Australians' beliefs on how trustworthy organisations are with personal information 55
Figure 34: Proportion of Australians considering each organisation trustworthy from 2007 to 2020 56
Figure 35: Percentage of Australians who are aware of the Privacy Act 57
Figure 36: Awareness of sectors covered by the Privacy Act 58
Figure 37: Awareness of sectors covered by the Privacy Act in 2017 and 2020 – filtered to those aware of the Privacy Commissioner 59
Figure 38: Belief that each sector should be covered by the Privacy Act 60

Figure 39: Awareness of the Privacy Commissioner over time 61
Figure 40: Australians' point of contact to report misuse of personal information 62
Figure 41: Organisations people would report a misuse of personal information to in 2017 and 2020 63
Figure 42: Perception of levels of protection regarding specific privacy rights 64
Figure 43: Australians' beliefs that the government should do more to protect the privacy of their data 65
Figure 44: Australians' beliefs that the government should do more to protect the privacy of their data – organisation type breakdown 66
Figure 45: Australians' beliefs that they should or should not have specific privacy rights 67
Figure 46: Groups of Australians that should have additional protection under the Privacy Act 68
Figure 47: Proportion of Australians who normally read privacy policies on internet sites 69
Figure 48: Reasons Australians don't read privacy policies 70
Figure 49: Confidence in comprehension of privacy policies after reading 71
Figure 50: Confidence in comprehension of privacy policies after reading – reading habit breakdown 71
Figure 51: Impacts of reading a privacy policy 73
Figure 52: Importance of specific attributes of privacy policies to Australians 74
Figure 53: What Australians think a privacy policy should include 75
Figure 54: Suggestions to improve privacy policies 76
Figure 55: Suggestions to improve privacy policies among those who don't understand them 76
Figure 56: Impact of privacy certification on trust in organisations 77
Figure 57: Australians' comfort with businesses tracking location 79
Figure 58: Protection of location data 80
Figure 59: : Type of information Australians are reluctant to provide to any organisation 81
Figure 60: How comfortable Australians feel with collection of biometric information 82
Figure 61: Trustworthiness of organisations using biometric information 83
Figure 62: How comfortable Australians feel with uses of biometric information 84
Figure 63: Protection of biometric information 85
Figure 64: General beliefs about AI technology 86
Figure 65: Attitudes towards being informed when AI technology is used 87
Figure 66: Attitudes towards human oversight of decisions made by AI 88
Figure 67: Comfort with organisations using AI to make decisions 89
Figure 68: Parents' concerns about the protection of personal information 90
Figure 69: Parents' levels of comfort with businesses using their child's personal information 91
Figure 70: Children's ownership of devices and social media accounts 92
Figure 71: Children's online accounts 93
Figure 72: Parents' beliefs on children's data privacy 94
Figure 73: Measures taken to protect child's privacy 95
Figure 74: Measures to increase the data privacy of children online 96
Figure 75: Proportion of parents who feel they are in control of their child's data privacy 97
Figure 76: Parents who avoided using a service to protect their child's personal information 98
Figure 77: Parents protecting child's personal information online 98
Figure 78: Reasons for not doing more to protect personal information of their child 99
Figure 79: Appropriate age for children to start learning about data privacy 100
Figure 80: Children's ownership of devices and social media account 101

Figure 81: ACAPS fieldwork timelines in relation to timelines of confirmed COVID-19 cases in Australia 102
Figure 82: Privacy concerns since COVID-19 103
Figure 83: Changes in concerns about the protection of their personal information overall 104
Figure 84: Concerns about protection of personal information since the COVID-19 outbreak 105
Figure 85: Biggest privacy risks people face in the context of COVID-19 crisis 106
Figure 86: Proportion of Australians working or studying from home as a result of COVID-19 107
Figure 87: Changes in work/study made since the COVID-19 pandemic 107
Figure 88: Comfort with protection of personal information while working/studying at home 108
Figure 89: Comfort with protection of personal information in telehealth conferences or by employees working from home 109
Figure 90: Beliefs around the concessions that must be made during the COVID-19 outbreak 110
Figure 91: Comfort with organisations using phone data to stop COVID-19 with or without consent 111
Figure 92: Comfort with different organisations sharing personal information 112
Figure 93: Comfort levels with organisations sharing personal information before and during COVID-19 113
Figure 94: Trust in organisations with regard to how they protect personal information in the context of the COVID-19 crisis A9. Thinking now about trustworthiness. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information in the context of the COVID-19 crisis? Base: Australians 18+ (n=1,004) 114
Figure 95: Trust in organisations with regard to how they protect personal information before and during the COVID-19 crisis 115
Figure 96: Proportion of Australians who have downloaded an app or signed up to a digital service as a result of COVID-19 116
Figure 97: Reasons why apps were downloaded as a result of COVID-19 117
Figure 98: Extent to which Australians read the privacy policies associated with new apps and services 117