



Australian Government  
Office of the Australian  
Information Commissioner

# Australian Community Attitudes to Privacy Survey

August 2023



OAIC

## OAIC research

The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency established to promote and uphold privacy and information access rights. We have a range of regulatory responsibilities and powers under the *Privacy Act 1988*, *Freedom of Information Act 1982* and *Australian Information Commissioner Act 2010*.

Our research helps to inform our approach to regulation, law reform, strategy and education. OAIC research is available at: [oaic.gov.au/research](https://oaic.gov.au/research)

For enquiries about OAIC research, please contact [corporate@oaic.gov.au](mailto:corporate@oaic.gov.au)

## Acknowledgements

The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

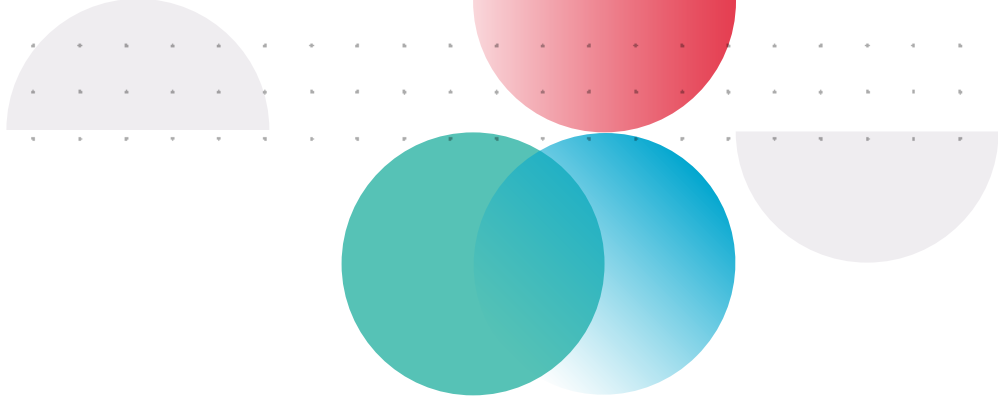
The OAIC would like to thank [Loneragan Research](#) who conducted this research on our behalf and co-developed this report.

## Copyright

This work is licensed under the [Creative Commons Attribution 4.0 International Licence](#), with the exception of the Commonwealth Coat of Arms, logos, any third-party material, any material protected by a trademark and any images and photographs.

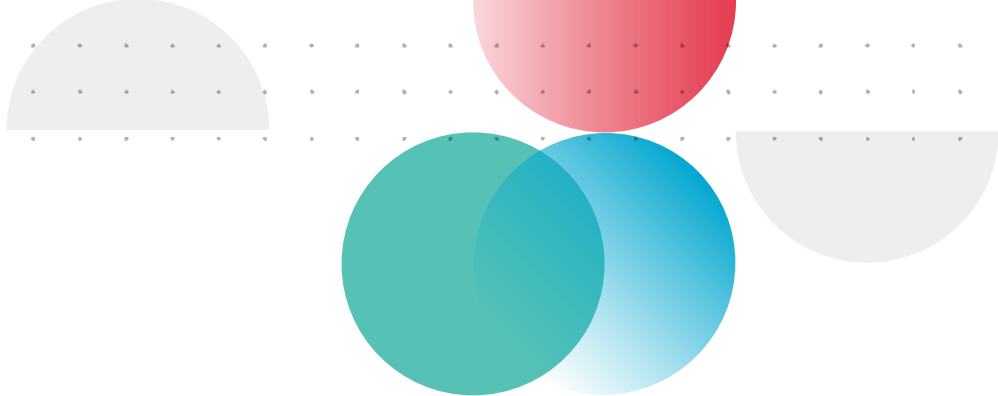
## Suggested reference

Office of the Australian Information Commissioner (2023) *Australian Community Attitudes to Privacy Survey 2023*, Office of the Australian Information Commissioner, Australian Government.



# Contents

<b>Commissioner’s foreword</b>	<b>5</b>
<b>Overview</b>	<b>7</b>
Main findings .....	8
<b>Part 1: Introduction to privacy</b>	<b>13</b>
What privacy means to Australians.....	14
Beliefs about protecting personal information .....	16
Beliefs around control over personal information.....	18
Knowledge of privacy rights.....	19
Actions Australians take to protect their privacy .....	21
Perceived privacy risks .....	24
Role of privacy in purchasing decisions .....	25
<b>Part 2: Privacy legislation</b>	<b>30</b>
Awareness of the Privacy Act .....	31
Awareness and engagement with the Privacy Commissioner .....	32
Awareness of organisation types covered by the Privacy Act.....	33
Belief that organisation types should be covered by the Privacy Act .....	34
Extent Australians can access and use data .....	35
Access to personal information.....	36
Additional rights under the Privacy Act .....	37
Privacy certification .....	38
Desired content in privacy policies.....	38
<b>Part 3: The role of organisations</b>	<b>41</b>
Responsibility for protecting personal information.....	42
Beliefs about organisations’ personal information handling practices .....	43
Concern about information being sent overseas.....	44
Comfort dealing with local vs overseas organisations.....	45
Trust in organisations.....	46
Information considered fair and reasonable to provide.....	49
Government use of personal information for research and service and policy development .....	51
Beliefs about whether certain practices are fair and reasonable.....	51
<b>Part 4: Privacy breaches and harm</b>	<b>54</b>
Privacy breaches.....	55
Data breaches .....	60
Ways for organisations to protect personal information .....	68



<b>Part 5: Digital technologies</b>	<b>71</b>
Biometric technology.....	71
Artificial intelligence .....	77
Acceptance of targeted advertising.....	79
<b>Part 6: Children’s privacy</b>	<b>81</b>
Concern and control over children’s privacy.....	83
Parents’ actions to protect their children’s privacy online .....	84
Children’s access to and ownership of devices.....	85
Children’s use of online accounts and services .....	86
Importance of children’s privacy when choosing services.....	88
Appropriate ages for children to learn about privacy and provide consent.....	88
Beliefs about accessing children’s services .....	89
Beliefs about children’s privacy.....	90
Comfort with businesses using children’s personal information.....	92
Organisational measures to increase children’s privacy .....	94
Technology measures to increase children’s privacy .....	95
Responsibility for the protection of children’s information.....	96
<b>Methodology</b>	<b>99</b>
Overview .....	99
Questionnaire development .....	99
Questionnaire length, sample size and modularisation .....	99
Weighting .....	100
Fieldwork .....	100
<b>Glossary and shortened forms</b>	<b>101</b>
Glossary.....	101
Shortened forms.....	103
<b>List of figures</b>	<b>104</b>

## Commissioner's foreword

Three years since our last Australian Community Attitudes to Privacy Survey (ACAPS), several significant events have pushed privacy into the community spotlight, including the COVID-19 pandemic, high-profile data breaches and the speed of tech innovation.

These events have intensified the focus on the role privacy plays in our sense of control and autonomy, human dignity, freedom and other key values.

As we release our latest ACAPS, we are at a pivotal moment for privacy in Australia, where we can seize the opportunity to ensure laws and practices uphold this fundamental human right into the future.

Our survey provides a valuable window into the sentiment of the community and a snapshot of how recent events have impacted them. For example, just under half of Australians surveyed told us they were affected by a data breach in the previous year, and three-quarters experienced harm as a result.

The advent of technologies like artificial intelligence (AI) and facial recognition have introduced the potential for new privacy risks, some that deeply intersect with our human rights. While AI has the potential to provide major economic benefits, we know Australians are cautious about the use of AI to make decisions that might affect them, and there are low levels of comfort in the use of the technology.

Despite the heightened awareness and concern about privacy among the community, there is limited knowledge of what to do about it.

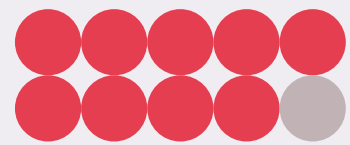
Nine in ten Australians have a clear understanding of why they should protect their personal information, up from 85% in 2020.

Some take action out of concern for their privacy, like checking emails, texts and calls are not scams before providing their information and using unique passwords and not sharing them.

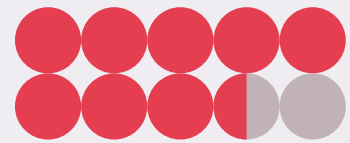
But only 21% say their privacy knowledge is 'very good' or 'excellent', and 57% say they care about their data privacy, but do not know what to do about it.

Providing Australians with the right information and offering real privacy choices will empower them to protect their privacy.

Only 2 in 5 people feel most organisations they deal with are transparent about how they handle their information, and 58% say they do not understand how it is used.



**9 in 10** Australians have a clear understanding of why they should protect their personal information



**Up from 85%** in 2020

Half of Australians surveyed believe that if they want to use a service, they have no choice but to accept what the service does with their data.

Yet 84% want more control and choice over the collection and use of their information.

This highlights the need to support individuals to take control of their privacy, for example, through privacy education and being clear about how their information is used, so they can make informed choices. However, it also emphasises the need for personal information handling practices to be inherently fair and reasonable.

Not only is good privacy practice the right thing to do and what the community expects, it is a precondition for the success of an innovative economy and gaining Australians' trust and confidence.

The findings point to several areas where organisations can do more to build consumer trust. Trust is essential, as we know from our survey the level of trust in an industry sector impacts what information the community considers fair and reasonable to provide.

The most trusted sectors are also more likely to be relied on to do the right thing when it comes to specific practices, such as only collecting the information necessary to provide the service.

And consumers place a high value on privacy when choosing a product or service, with it ranking only after quality and price. They are even prepared to experience some inconvenience if their privacy is guaranteed.

We are on the cusp of the most significant changes to our privacy framework in over a decade, which presents an opportunity to ensure the protections the community expects are reflected in the law.

The survey points to ongoing opportunities to enhance Australia's privacy framework, and there is strong support for government legislation that protects personal information.

We need to consider the laws and practices that will uphold our fundamental human right to privacy and meet community expectations, while enabling innovation and economic growth.

The OAIC will use the findings of ACAPS 2023 to inform our ongoing input into the review of the Privacy Act and to target our activities at areas of high concern among the community. We look forward to working closely with regulated entities to increase community trust and confidence in the protection of their personal information.

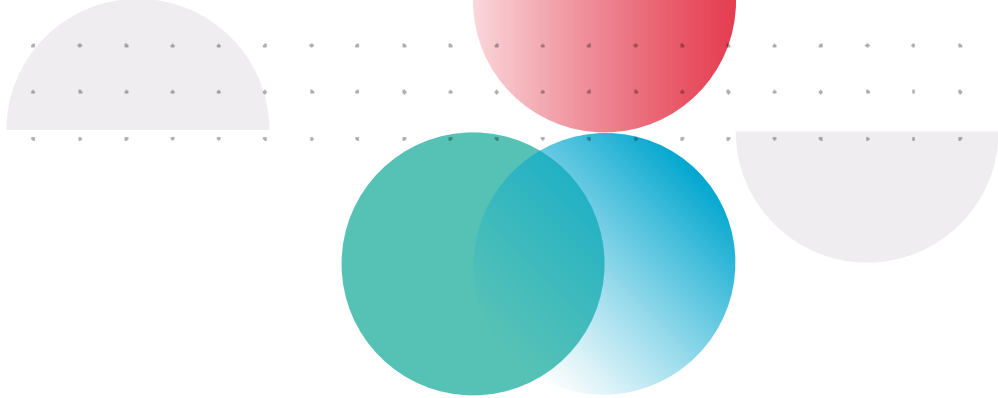
**Angelene Falk**

Australian Information Commissioner and Privacy Commissioner



**84%**

want more control and choice over the collection and use of their information.



## Overview

The [Australian Community Attitudes to Privacy Survey \(ACAPS\)](#) is a longstanding study commissioned by the OAIC to evaluate the awareness, understanding, behaviour and concerns about privacy among Australians.

Since the last report in 2020, there have been some notable shifts in Australians' awareness and attitudes towards privacy, driven by several events.

High-profile data breaches have drawn attention to the collection, retention and protection of personal information.

New applications and the increasing prevalence of technologies such as artificial intelligence and facial recognition have also presented new privacy considerations.

The research was first conducted in 1990 and took on its current form in 2001. It provides longitudinal information on Australians' attitudes to key privacy issues, their experiences and perspectives around the use and protection of their personal information and the action they take to safeguard their privacy.

Since the last report in 2020, there have been some notable shifts in Australians' awareness and attitudes towards privacy, driven by several events.

High-profile data breaches have drawn attention to the collection, retention and protection of personal information.

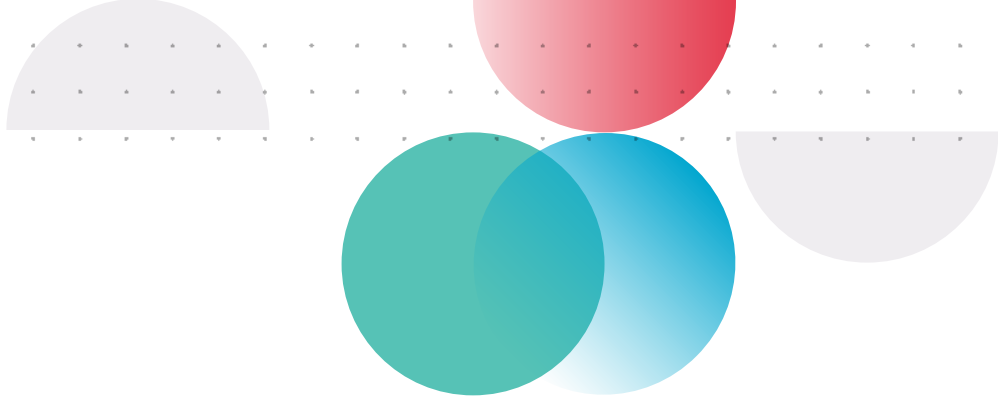
New applications and the increasing prevalence of technologies such as artificial intelligence and facial recognition have also presented new privacy considerations.

ACAPS 2023 has continued to evolve from earlier surveys. In particular, this survey explores biometrics and data breaches and harms that can result in more detail.

The main objectives of the 2023 survey are to:

- provide insights on Australians' privacy attitudes and behaviours
- identify Australians' awareness of and concerns about key and emerging privacy issues
- understand how Australians' privacy awareness, attitudes and behaviours have changed over time
- collect data to assist the OAIC as the national privacy regulator across enforcement, compliance, policy, education and communications initiatives.

The OAIC commissioned [Lonergan Research](#) to undertake ACAPS 2023. The survey was conducted in March 2023 with a nationally representative sample of 1,916 unique respondents aged 18 and older.



## Main findings

### Introduction to privacy

Three in five (62%) Australians see the protection of their personal information as a major concern in their life.

Eight in ten (82%) people care enough about protecting their personal information to do something about it, however 57% do not know what to do.

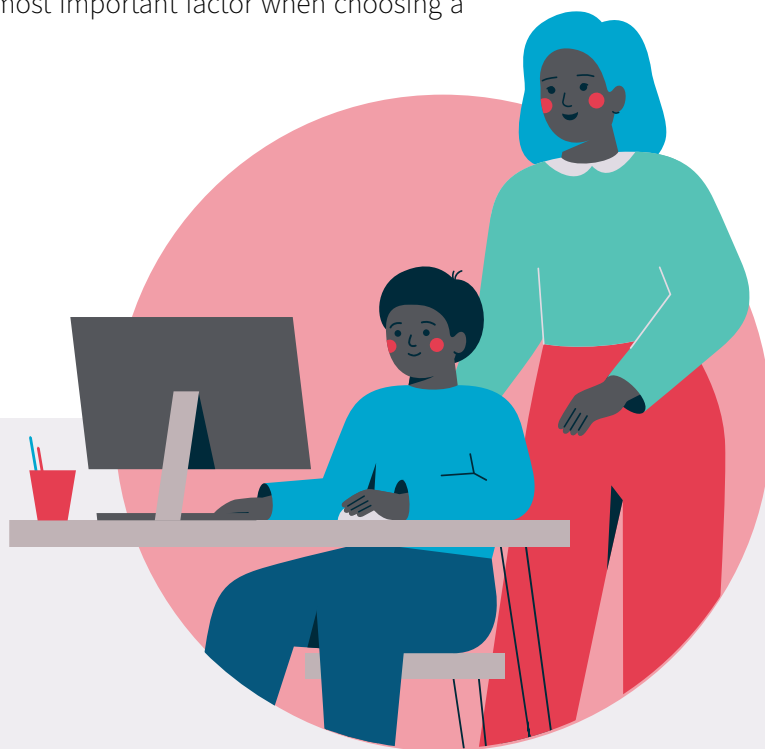
Only a third (32%) of Australians feel in control of their data privacy, and 84% want more control and choice over the collection and use of their personal information.

The 2 most common steps Australians are taking out of concern for their data privacy are checking an email, text message or phone call is not a scam before providing their information, and using unique passwords and not sharing them.

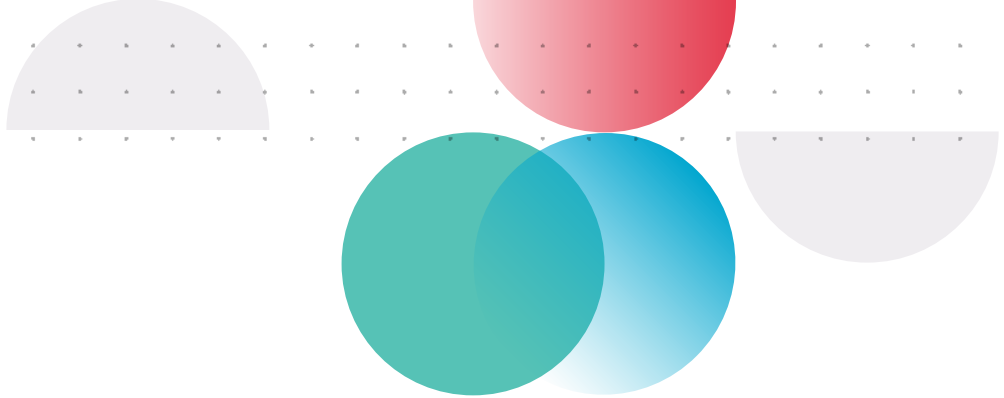
Three-quarters (74%) of Australians feel data breaches are one of the biggest privacy risks they face today. This has increased by 13 percentage points since 2020.

Most Australians place a high level of importance on their privacy when choosing a product or service, with 70% saying it is extremely or very important and another 26% stating it is quite important.

After quality and price, data privacy is the third most important factor when choosing a product or service.







## Privacy legislation

While many Australians do not know exactly how they can protect their own personal information, the majority would like business and government agencies to do more in this area.

Seven in ten (69%) Australians said they are aware of the Australian privacy law that promotes and protects the privacy of individuals, and 89% want the government to provide more legislation in this area.

Almost all Australians think they should have additional rights under the Australian Privacy Act. These include the right to:

- ask a business to delete their personal information (93% believe they should have this right)
- object to certain data practices while still being able to access and use the service (90%)
- seek compensation in the courts for a breach of privacy (89%)
- know when their personal information is used in automated decision-making if it could affect them (89%)
- ask a government agency to delete their personal information (79%).

Australians are generally unaware some organisation types are exempt from the Privacy Act. The majority believe political parties and representatives (82%), businesses collecting work-related information about employees (81%), media organisations in relation to their journalism activities (78%) and small businesses (77%) should be required to protect personal information in the same way as federal government agencies and larger businesses.

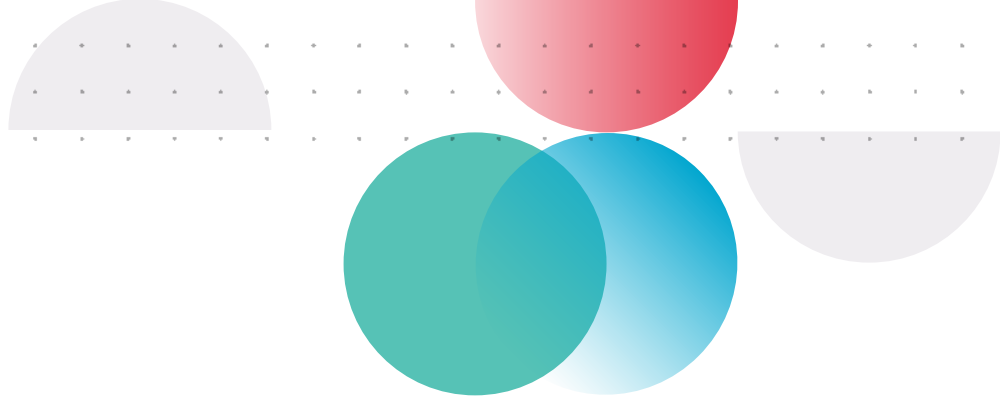
## The role of organisations

Three in five (58%) Australians do not know what organisations do with their data. People often feel they have no choice but to hand over their personal information if they want to access a service (50% agree or strongly agree).

Australians trust health service providers and federal government agencies the most and social media companies and real estate agencies the least when it comes to the protection and use of their personal information.

Less than half of people trust organisations to only collect the information they need, use and share information as they state, store information securely, give individuals access to their personal information and delete information when no longer needed.

Most Australians (91%) are concerned about the prospect of their personal data being sent overseas.



Over half (55%) of Australians consider having to share some personal information if they want to use a service fair enough. However, they generally only consider it fair and reasonable to provide their name (81%) and email address (77%) to organisations and, to a lesser extent, their phone number (68%), date of birth (62%) and physical address (61%).

There are certain practices Australians consider not fair and reasonable, including the online tracking, profiling and targeting of advertising to children (89% not fair and reasonable).

## Privacy breaches and harm

Almost half (47%) of Australians said they had been informed by an organisation that their personal information was involved in a data breach in the 12 months prior to completing the survey in 2023.

Three-quarters (76%) said they experienced harm as a direct result. Half (52%) saw an increase in scams and spam and almost a third (29%) said they had to replace key identity documents, such as a driver's licence or passport. One in ten (12%) experienced emotional or psychological harm.

Almost half (47%) of people say they would stop using a service if their data was involved in a breach, but this drops to a third for people who have recently experienced a breach.

When it comes to dealing with the impacts of a breach, only 1 in 10 (12%) people said there was nothing an organisation could do to appease them. Most Australians are willing to remain with an organisation that has suffered a data breach, provided the organisation quickly takes action, such as putting steps in place to prevent customers from suffering harm.

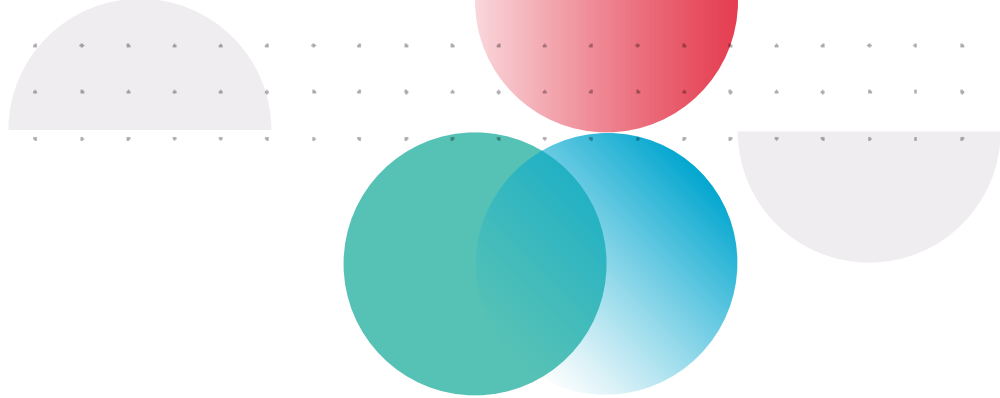
A quarter (26%) of Australians believe the most important way an organisation can protect their personal information is by only collecting the information necessary to provide the product or service. Australians view the second most important action organisations can take is proactive steps to protect the information they hold (24%).

## Digital technologies

Australians' level of comfort with biometric information being collected and used depends largely on the type of organisation and the context.

People are generally more comfortable with one-to-one uses of their biometric information (such as to go through passport control at an airport) than they are with one-to-many uses and biometric analysis.

Australians are most comfortable with the collection and use of their biometric information in border security and law enforcement contexts, and they are more likely to trust the public sector to collect and use this kind of information than businesses.



When it comes to artificial intelligence (AI), 96% of Australians want some conditions in place before the technology is used to make a decision that might affect them, such as the right to have a human review the decision.

Australians are more comfortable with government agencies using AI to make decisions about them that use personal information than they are with businesses (20% comfortable for government agencies, cf. 15% for businesses).

## Children's privacy

Protecting their child's personal information is a major concern for 79% of parents. However, only half (50%) feel they are in control of their child's data privacy.

Eighty-five per cent of parents agree children must be empowered to use the internet and online services, but their data privacy must be protected.

For 91% of parents, the privacy of their child's personal information is of high importance when deciding to provide their child with access to digital devices and services.

There is a great deal of discomfort around children's privacy, especially with businesses tracking a child's location without permission (79% uncomfortable) and businesses obtaining a child's personal information and selling it to third parties (79% uncomfortable). Parents overwhelmingly (92%) believe children should have the right to grow up without being profiled or targeted.

The vast majority of parents support organisations adopting a child-centric approach to handling personal information about children. This includes organisations considering what is in the best interests of children when handling their personal information (93% support) and providing important data privacy information to children in clear language that is not misleading (91% support).





# Part 1

## Introduction to privacy

## Part 1: Introduction to privacy

Australians understand why they should safeguard their personal information and care enough about their privacy to do something about it, taking a variety of actions to protect themselves.

At the same time, only half of people say they have a clear understanding of how to protect their personal information, and only a third feel in control of their privacy.

People are mainly concerned about data breaches and organisations not storing their personal information securely, as well as scammers trying to get their personal information.

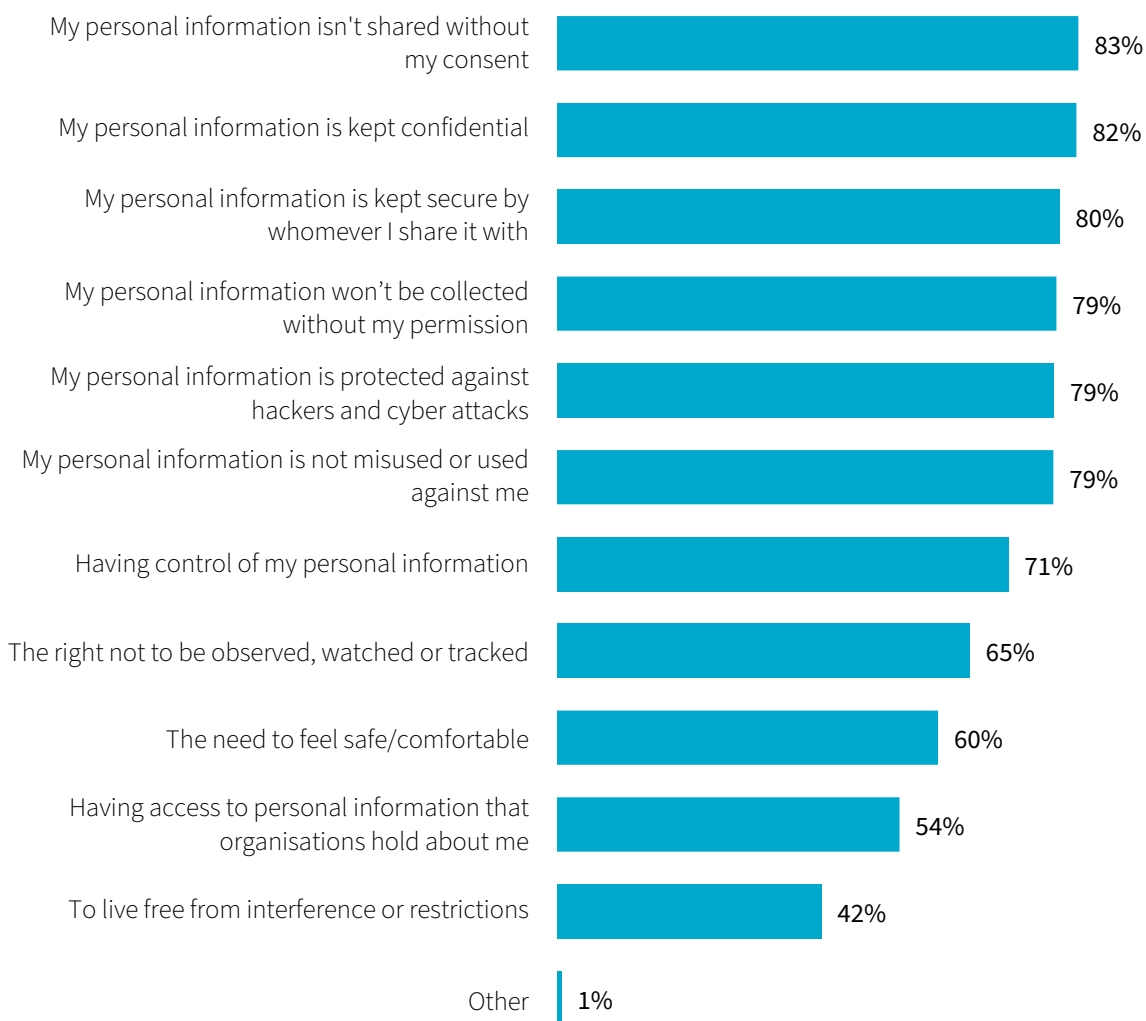
Australians see privacy as important when they are looking to purchase products and services, rating it as the third most significant factor after quality and price.



## What privacy means to Australians

Primarily, when Australians think about the privacy of their personal information, they identify a framework for how their information should be handled by others. Most Australians consider privacy to mean their information is kept confidential and secure, not collected without their permission and not used against them.

**Figure 1: What privacy means to Australians**



G1. Thinking specifically about your personal information, what does 'privacy' mean to you. Select all that apply. Base: Australians 18+ years (n=1,916)

Older Australians are more likely to express a wider range of ideas when defining privacy. Those aged 65 and over are significantly more likely to select more responses to the question compared to the those aged under 65 (8.8 responses on average for 65+ years, cf. 7.7 for 35–64 years, 7.1 for 18–24 years).

- Introduction to privacy

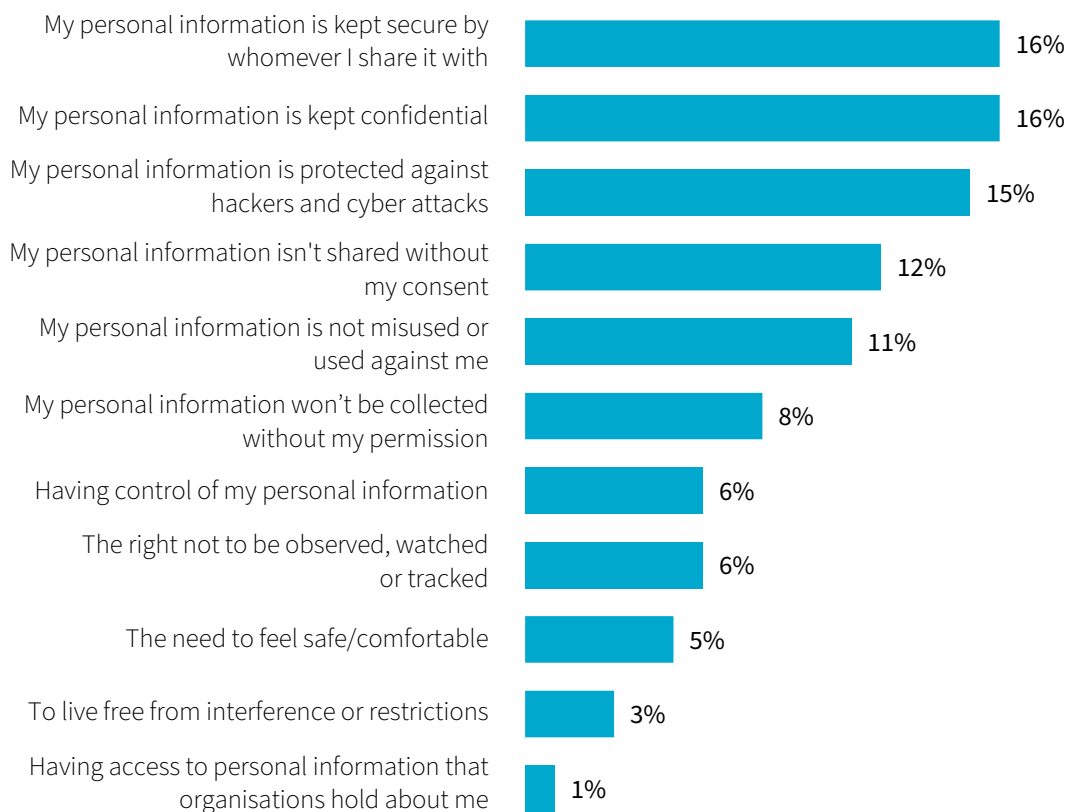
Age also impacts people's definition of privacy. Ninety-one per cent of people aged 65 and over say privacy should mean their information is not shared without their consent, compared to 84% of those aged 35 to 64 and 76% of those aged 18 to 34.

Similarly, 89% of people aged 65 and over define privacy as their information being kept confidential, compared to 82% of those aged 35 to 64 and 78% of those aged 18 to 34.

From the initial list of definitions, respondents were then asked to select the aspect of privacy of most importance to them.

This elevated the significance of the protection of personal information, with the key definitions selected being the need for their personal information to be kept secure, confidential and protected against hackers and cyber attacks, with 47% of Australians choosing one of these 3 options.

**Figure 2: The most important aspects of privacy**



G2. And which one is the most important to you? Select one. Base: Australians 18+ years (n=1,916)

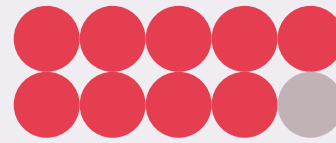
Australians hold consistent views on the most important aspects of privacy, with no significant variation based on their age, gender or other demographics.

## Beliefs about protecting personal information

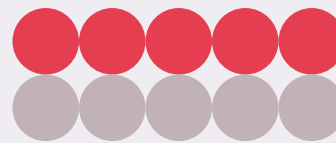
Nine out of ten (90% ‘agree’ and ‘strongly agree’) Australians say they have a clear understanding of **why** they should protect their personal information, but only half (51% ‘agree’ and ‘strongly agree’) understand **how** they can protect it.

This creates a gap of 39% between those who understand why they should protect their personal information and those who know how.

The proportion of people who understand why they should protect their information increased from 85% in 2020, while the understanding of how to protect their information remained relatively steady (51% in 2023, cf. 49% in 2020).

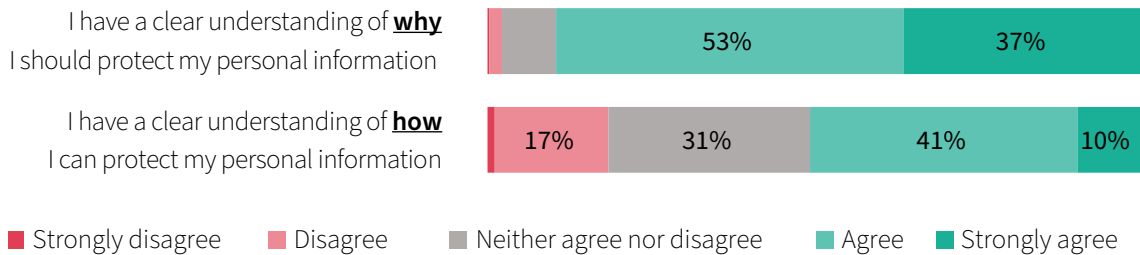


**9 in 10** Australians have a clear understanding of why they should protect their personal information



**Only half** understand how they can protect it

**Figure 3: Beliefs about protecting personal information**



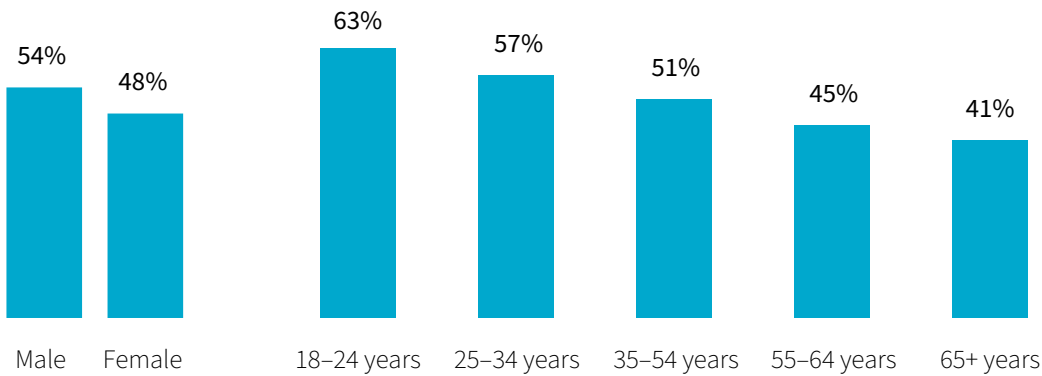
G4. Thinking about data privacy, to what extent do you agree or disagree with the following? Base: Australians 18+ years (n=1,916)

Younger Australians are more likely to consider they know how to protect their personal information compared to older age groups (63% ‘agree’ and ‘strongly agree’ 18–24 years, cf. 41% 65+ years).

Males are more likely to say they know how to protect their privacy than females (54% ‘agree’ and ‘strongly agree’ males, cf. 48% females).



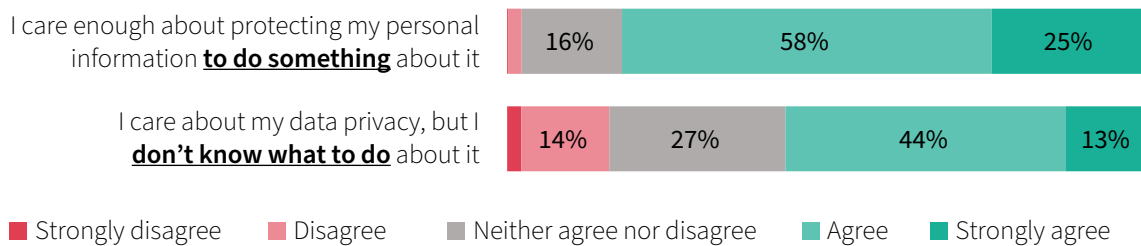
**Figure 4: Percentage that understand how to protect personal information by gender and age**



G4. Thinking about data privacy, to what extent do you agree or disagree with the following: I have a clear understanding of how I can protect my personal information? ‘Agree’ and ‘strongly agree’. Base: Australians 18+ years, males (n=936), females (n=978), 18–24 years (n=211), 25–34 years (n=352), 35–54 years (n=677), 55–64 years (n=278), 65+ years (n=398)

There was an increase in the proportion of Australian adults (82% in 2023, up from 75% in 2020) who care enough about protecting their personal information to do something about it. However, 3 out of 5 (57%) said they care about their data privacy, but do not know what to do about it.

**Figure 5: Concern about protecting personal information**



G4. Thinking about data privacy, to what extent do you agree or disagree with the following? Base: Australians 18+ years (n=1,916)



**4 out of 5** Australian adults care enough about protecting their personal information to want to do something about it



**3 out of 5** do not know how to go about it

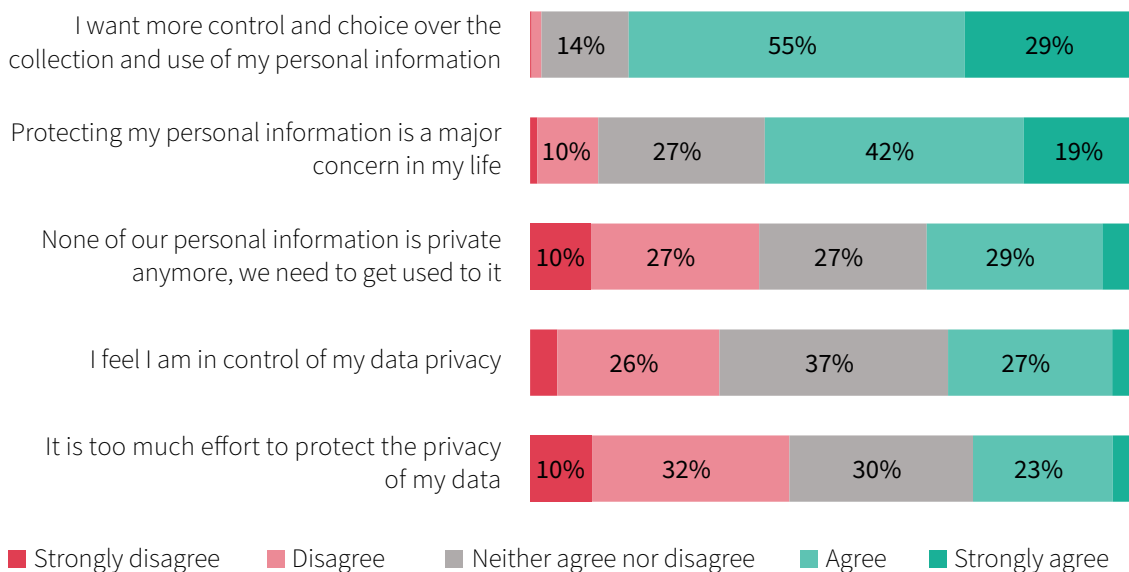
Similar to the beliefs around protecting their information, females are more likely than males to acknowledge they do not know what to do to protect their personal information (60% females, cf. 53% males). This data should be considered in the context of males claiming a higher level of privacy knowledge than females, while scoring lower when tested.

## Beliefs around control over personal information

More than 4 out of 5 (84%) Australians want more control over the collection and use of their personal information, and this proportion is consistent across all demographic segments. This is a slight decline from 2020 when 87% ‘agreed’ or ‘strongly agreed’ with this statement.

Three out of five (62%) said protecting their personal information is a major concern in their life.

**Figure 6: Beliefs around control over personal information**



G5, G6. Thinking about data privacy, to what extent do you agree or disagree with the following?  
Base: Australians 18+ years (n=1,916)

- Introduction to privacy

Younger Australians are most likely to feel in control of their data privacy (40% 18–34 years ‘agree’ or ‘strongly agree’, cf. average 32%), but often find it is too much effort to protect the privacy of their data (35% ‘agree’ or ‘strongly agree’, cf. average 28%).

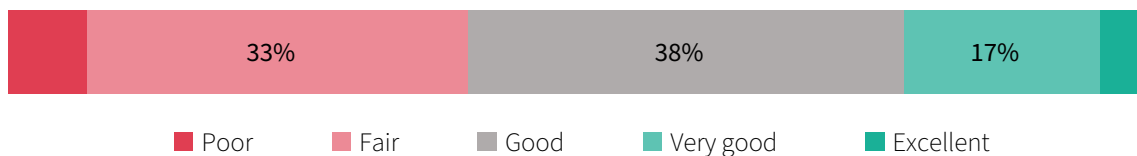
Older Australians are least likely to feel in control of their data privacy (25% 55+ years ‘agree’ or ‘strongly agree’, cf. average 32%) and are less likely to say it is too much effort to protect their data (19% 55+ years ‘agree’ or ‘strongly agree’, cf. average 28%).

People aged 35 and older have an increasing perception of wanting more control and choice over the collection and use of their personal information (86% 35+ years ‘agree’ or ‘strongly agree’, cf. average 84%).

## Knowledge of privacy rights

One in five (21%) Australians claim to have ‘very good’ or ‘excellent’ knowledge of data protection and privacy rights, down slightly from 23% in 2020.

**Figure 7: Self-rated knowledge of data protection and privacy rights**



G3. Before today, how would you rate your knowledge of data protection and privacy rights? Base: Australians 18+ years (n=1,916)

The perceived level of knowledge decreases with age, with younger adults claiming to have the most knowledge (29% 18–24 years claim ‘very good’ or ‘excellent’ knowledge, cf. 13% 65+ years).

Males are also more likely to claim a better understanding of privacy rights, with 26% saying they have ‘very good’ or ‘excellent’ knowledge (cf. 17% females).

Self-rated early adopters of technology are also more likely to claim a better understanding of privacy rights compared to the rest of the population. Sixty-six per cent of people who said they are ‘generally the first to try a new technology product’ stated they have ‘very good’ or ‘excellent’ knowledge, compared to 21% of those who said they are ‘generally the last to try a new technology product’.

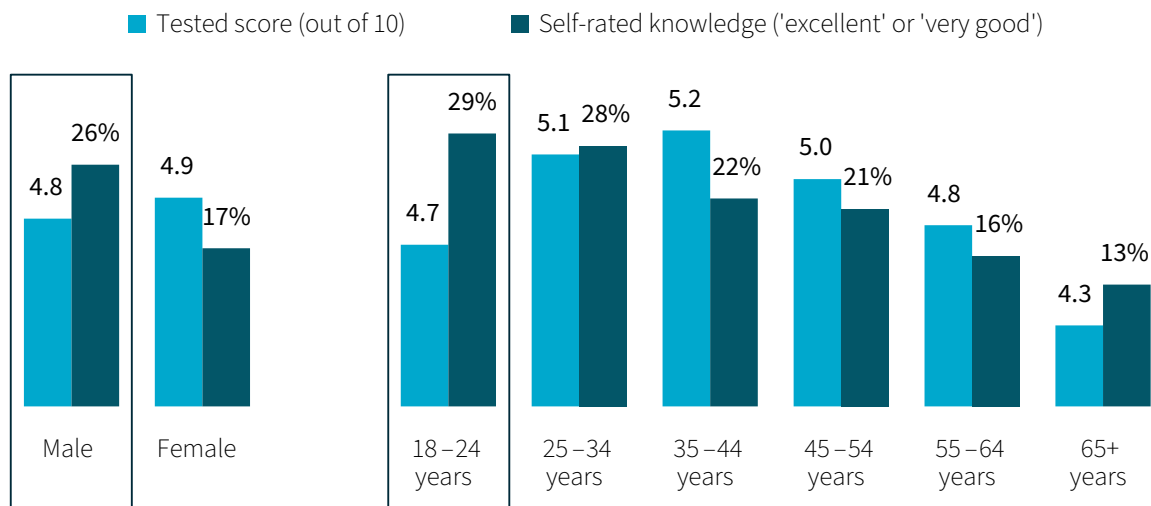
In addition to being asked to self-rate their knowledge of privacy rights, respondents were tested

- Introduction to privacy

on their understanding of organisations’ obligations under the Australian Privacy Act.

Respondents were shown 10 statements and were asked to indicate whether each statement was true, false or they did not know either way. Out of the 10 statements, 7 were true and 3 were false. This was not disclosed to the respondent, and the order of the statements was randomised for each person.

**Figure 8: Self-rated and tested knowledge of privacy rights by gender and age**



G3. Before today, how would you rate your knowledge of data protection and privacy rights? ‘Very good’ or ‘excellent’.

G14. Thinking about your privacy rights, which of the following do you think are true and which are false? Respondents were shown 10 statements about organisations’ responsibilities under the Australian Privacy Act.

Base: Australians 18+ years (n=1,916)

Respondents who had completed higher education and those with annual household incomes



over \$100,000 scored higher on average when tested.

People who classed themselves as early adopters of technology also scored higher on average than those who are the least likely to try new technology products, in line with the self-rated scores.

However, when viewed by respondent age and gender, there was disparity between the self-rated and tested results.

Younger Australians (18–24 years) rated their knowledge the highest (29% claiming ‘very good’ or ‘excellent’ knowledge), but scored lower than most other age groups.

A similar discrepancy exists between males and females, with males claiming a higher level of knowledge than females (26% males claiming ‘very good’ or ‘excellent’ knowledge, cf. 17% females), but with the tested scores coming in almost on par (4.8 males, cf. 4.9 females).

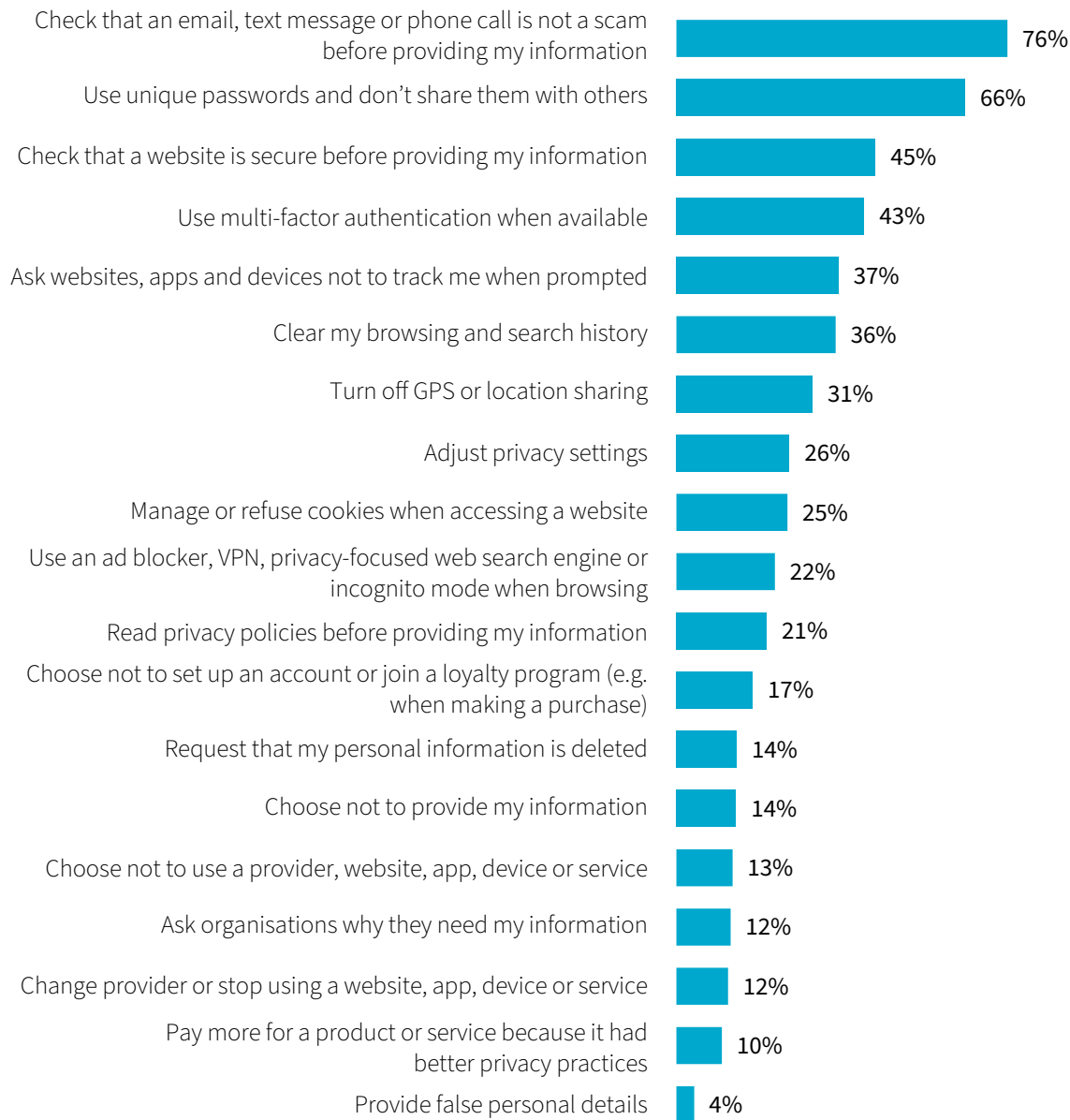
## Actions Australians take to protect their privacy

Out of concern for their data privacy, the 2 most common steps Australians take are checking an email, text message or phone call is not a scam before providing their information and using unique passwords and not sharing them.

Only  
**21%**

Only 21% of Australians always or often read privacy policies before providing their information

**Figure 9: Actions Australians always or often take out of concern for their data privacy**



G8, G9 and G10. How frequently do you do the following out of concern for your data privacy. 'Always or often'. Base: Australians 18+ years (n=1,916)

Both precautions are more likely to be taken by older Australians, with younger adults less likely to engage in these practices. Eighty-seven per cent of Australians aged 55 and older are 'always or often' taking precautions against scams, compared to 66% of those aged under 35. Similarly, 76% of Australians aged 55 and older 'always or often' use unique passwords compared to half (52%) of people under 35.

### Of Australians aged under 35



People under 35 are also less likely to read privacy policies before providing information compared to older Australians (17% <35 years, cf. 26% 65+ years).

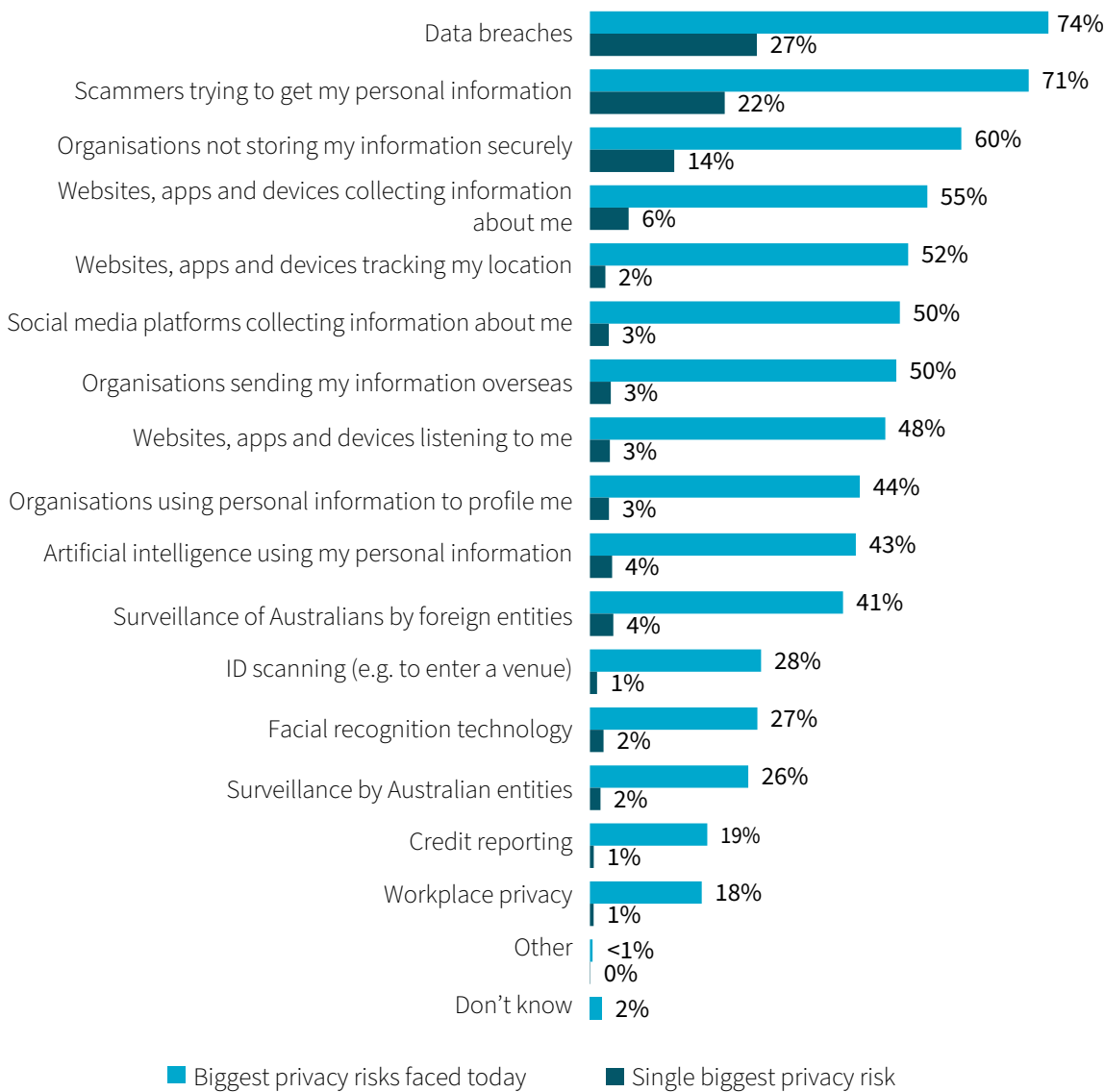
Males and females also differ slightly in the way they protect their information. Females are more likely to check for scams before handing over information (80% females, cf. 71% males) and are also more likely to turn off GPS or location sharing (36% females, cf. 26% males) and ask websites, apps and devices not to track them when prompted (41% females, cf. 33% males).

## Perceived privacy risks

Australians view data breaches and scammers as the top privacy risks they face.

Three-quarters (74%) of Australians feel data breaches are one of the biggest privacy risks they face today. This has increased by 13 percentage points since 2020 and is the most selected single biggest risk to privacy (27%).

**Figure 10: Perceived privacy risks**



P1. What do you think are the biggest privacy risks that you face today? Select all that apply.

P2. And of these, which one do you think is the biggest privacy risk? Select one.

Base: Australians 18+ years (n=1,626)



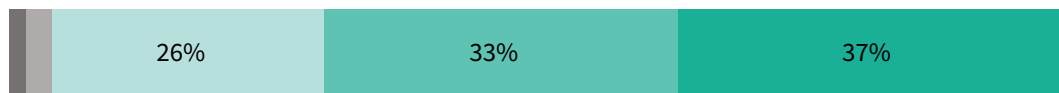
Concern about the risk of data breaches increases to 78% for Australians aged 35 and over, compared to 66% among those aged 18 to 34.

Seven in ten (71%) Australians say one of their biggest concerns is scammers trying to trick them into giving out personal information. This increases to 83% among Australians aged 55 and over, compared to 61% of those aged 18 to 34. One in five (22%) consider scammers the single biggest risk to privacy.

## Role of privacy in purchasing decisions

Most Australians place a high level of importance on their privacy when choosing a product or service, with 70% saying it is ‘extremely’ or ‘very important’ and another 26% stating it is ‘quite important’.

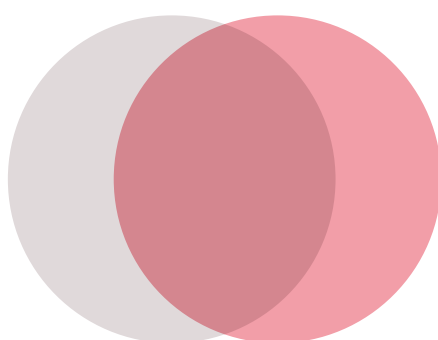
**Figure 11: Importance of privacy when choosing a product or service**



■ Don't know ■ Not important ■ Quite important ■ Very important ■ Extremely important

F9. Overall, how important is the privacy of your information when choosing a product or service? Base: Australians 18+ years (n=1,642)

Australians aged 18 to 34 are less likely to consider privacy ‘extremely important’ compared to those aged 45 and older (29% 18–34 years, cf. 43% 45+ years). This is in line with the younger cohort’s indifference towards taking measures to protect themselves, including regularly changing passwords and checking communications are not scams before interacting with them.



# 74%

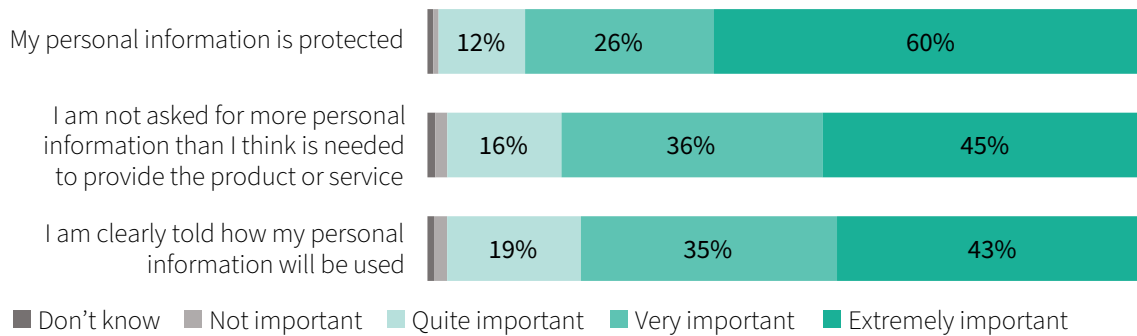
of Australians aged 45 and older place high importance on their privacy when choosing a product or service

- Introduction to privacy

The most important aspect of privacy Australians consider when selecting a product or service is that their information is protected. Three in five (60%) Australians say this component is ‘extremely important’ for them, with a further quarter (26%) saying it is ‘very important’.

Four in five Australians place high importance on not being asked for more personal information than they think is needed to provide the product or service (81% ‘extremely’ or ‘very important’) and being clearly told how their personal information will be used (79% ‘extremely’ or ‘very important’).

**Figure 12: Influences of privacy practices on choosing products and services**

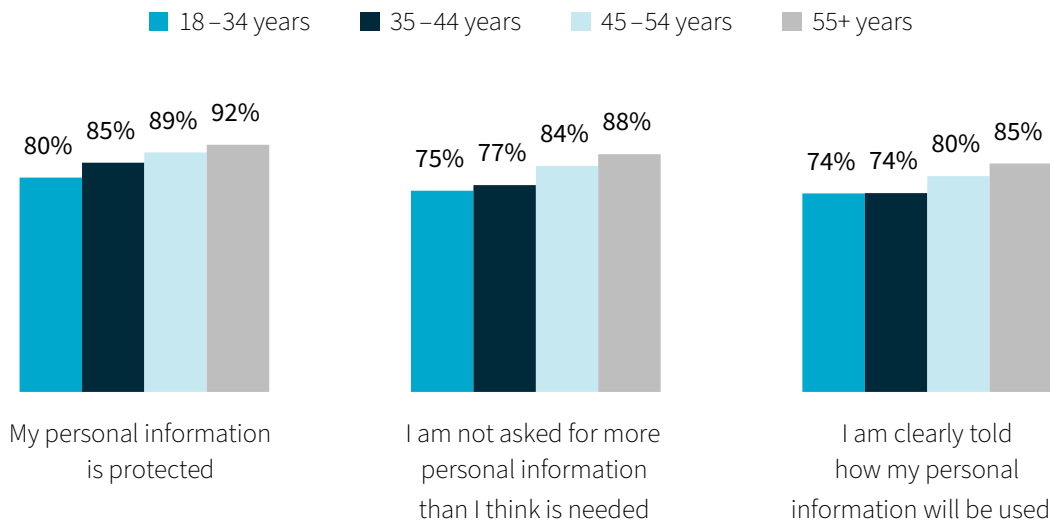


F10. How important are the following when choosing a product or service? Base: Australians 18+ years (n=1,642)

**4 in 5 Australians** place high importance on how their data is collected, used and protected when choosing a product or service

Females are more likely to place higher importance on the protection and amount of information required compared to males (information protected 89% ‘extremely’ or ‘very important’ for females, cf. 84% males; amount of information 84% females, cf. 79% males).

**Figure 13: Influences of privacy practices by age group**



F10. How important are the following when choosing a product or service? ‘Extremely important’ and ‘very important’. Base: Australians 18+ years (n=1,642)

As with other privacy measures, the importance when choosing a product or service of how data is collected, used and protected varies with age. Younger Australians still place a great deal of emphasis on privacy practices when choosing a product or service, with around three-quarters of those aged 18 to 34 indicating the aspects tested have a high level of importance to them.

However, as age increases, so does the importance of these privacy practices. For people aged 45 and over, there is a significant increase in the importance of their personal information being protected, not being asked for more information than they consider necessary and being clearly told how their information will be used.

### Where privacy sits among other purchase factors

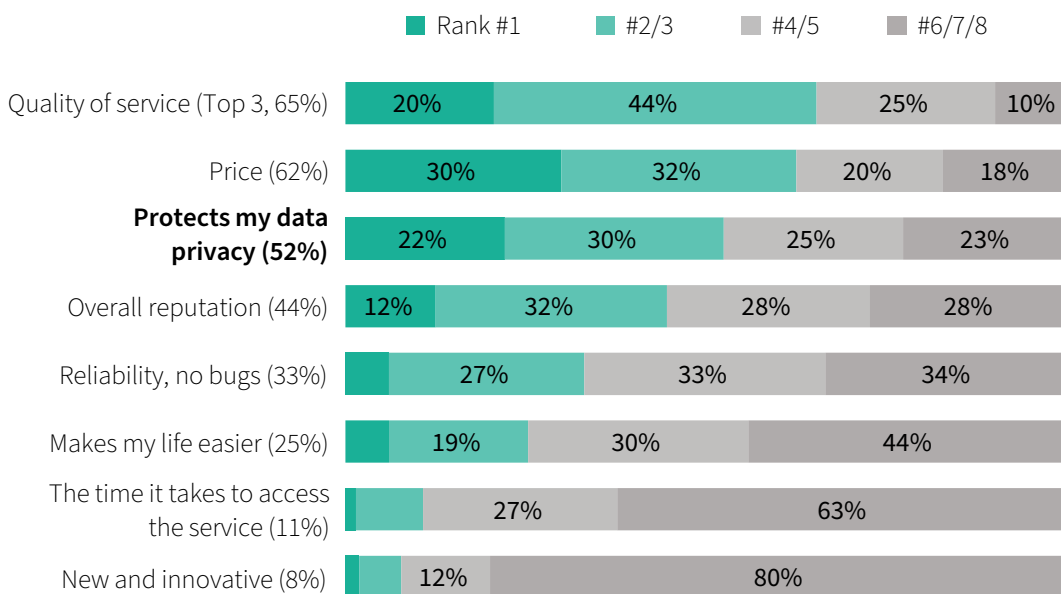
Quality and price are the key considerations for Australians when choosing a product or service. Half of Australians (52%) ranked data privacy in their top 3 considerations.

Privacy is seen as more important than ‘makes my life easier’ and ‘the time it takes to access the service’, indicating many people are prepared to experience some inconvenience in exchange for their privacy being protected.

## Important factors when choosing a product or service



**Figure 14: Important factors when choosing a product or service**



F8. Please rank each of the following in order of importance when choosing a product or service.  
Base: Australians 18+ years (n=1,642)

Younger age groups and males are less likely to rank privacy as high as older age groups and females, but regardless of demographic profile, it remains in the top 3 considerations for all segments.

Among Australians aged 65 and over, privacy becomes more important than price (63% ranked privacy in the top 3, cf. 57% price).



# Part 2

## Privacy legislation

## Part 2: Privacy legislation

Australians have low awareness of privacy legislation, notably around their rights to access information organisations hold about them and organisation types that are exempt from the Australian Privacy Act.

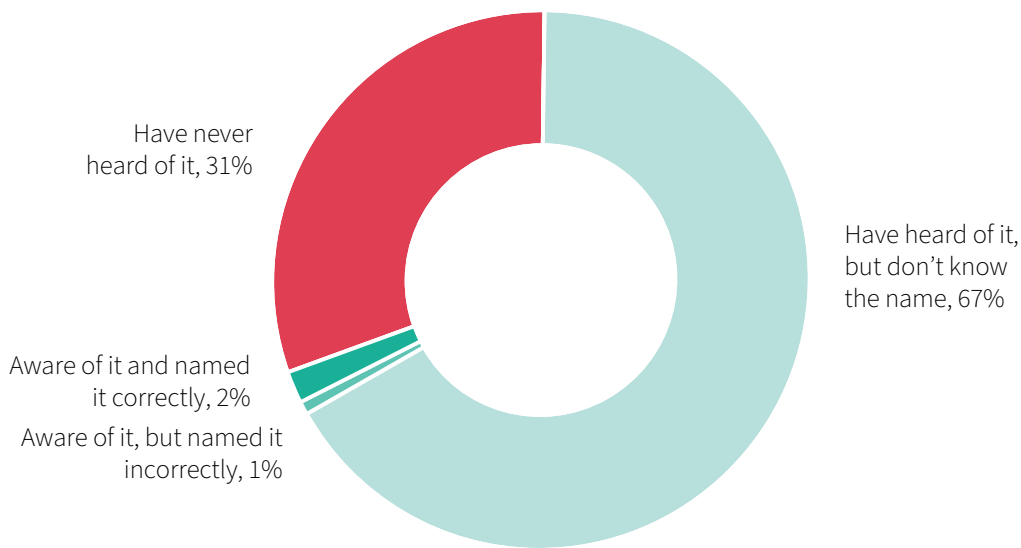
Most want more rights to control the way their personal information is collected, used and stored.



## Awareness of the Privacy Act

Seven in ten (69%) Australians said they are aware of the Australian privacy law that promotes and protects the privacy of individuals, a 3 percentage point increase from 2020, but only 2% correctly named it as the 'Privacy Act' or 'Australian Privacy Principles'.

**Figure 15: Awareness of the Privacy Act**



G11. Are you aware of the Australian privacy law that promotes and protects the privacy of individuals?  
Base: Australians 18+ years (n=1,916)

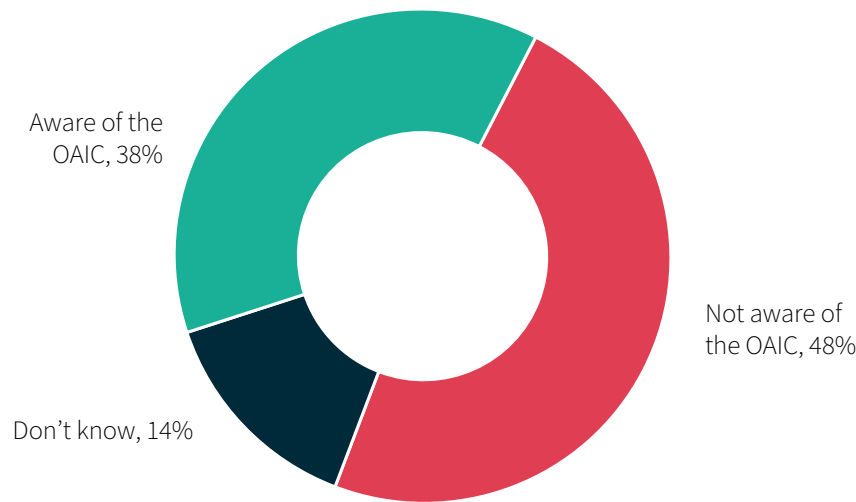
Australians aged 18 to 24 are the least likely to be aware of the Privacy Act, with 2 out of 5 (42%) saying they have never heard of it.

People in full-time employment have a higher awareness than the average Australian (70%), as do those who have completed a bachelor's degree or post-graduate qualification (72%) and early adopters of technology (70%).

## Awareness and engagement with the Privacy Commissioner

Awareness of the Privacy Commissioner has decreased 10 percentage points since 2020 (38% in 2023, cf. 48% in 2020, 44% in 2017). However, the wording of the question in the 2023 survey changed slightly to include a reference to the ‘Office of the Australian Information Commissioner’, making statistical tracking of this measurement unpredictable.

**Figure 16: Awareness of the Privacy Commissioner (OAIC)**



G12. Are you aware that the Privacy Commissioner (the Office of the Australian Information Commissioner) exists to uphold privacy laws and to investigate complaints about the misuse of personal information? Base: Australians 18+ years (n=1,916)

Males are more likely to be aware of the OAIC than females (41% males, cf. 35% females). There is also higher awareness of the OAIC among Australians who have completed tertiary education and who are tech savvy.

Twenty-nine per cent of Australians with no tertiary education are aware of the OAIC, compared to 44% of those with a bachelor’s or postgraduate qualification. Thirty per cent of people who consider themselves to be late adopters of technology are aware of the OAIC, compared to 53% for early adopters.





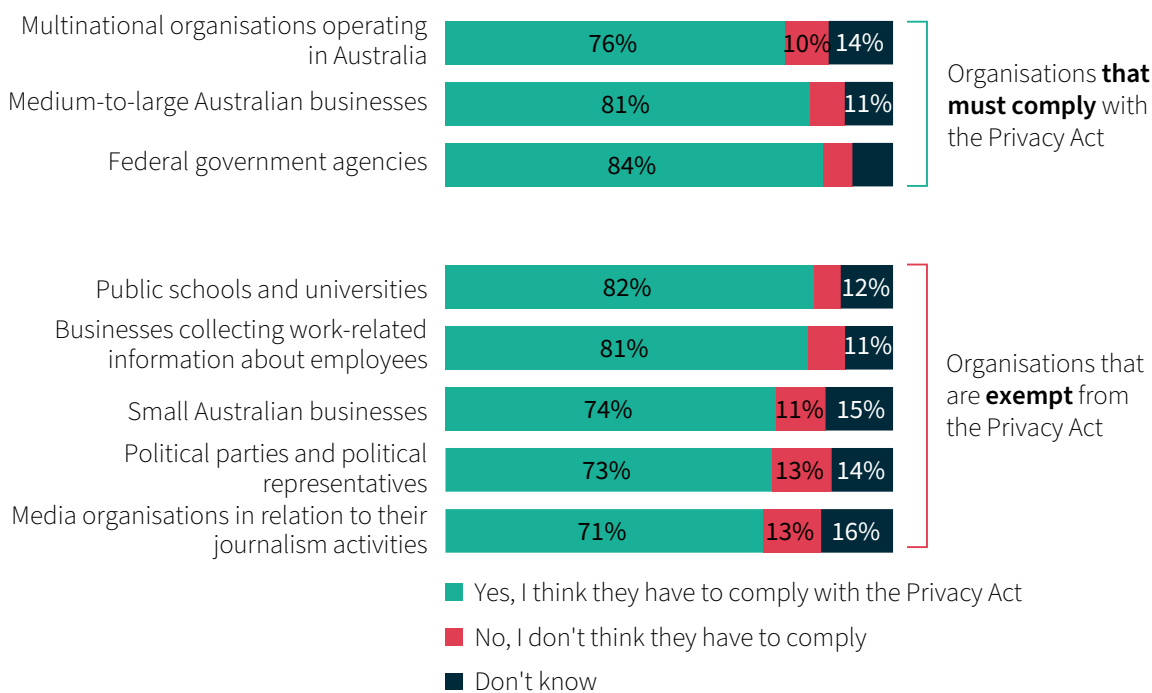
## Awareness of organisation types covered by the Privacy Act

Australians have limited understanding of which organisation types have to comply with the Privacy Act.

Federal government agencies, medium-to-large Australian businesses and multinational organisations operating in Australia have responsibilities under the Act. Public schools and universities, businesses collecting work-related information about employees, small Australian businesses (with a turnover of less than \$3 million), political parties and representatives, and media organisations in relation to their journalism activities do not.

Most Australians think all organisation types tested are covered by the Privacy Act.

**Figure 17: Awareness of organisation types covered by the Privacy Act**



L1. The Australian Privacy Act determines how organisations must handle your personal information. Which of the following do you think have to comply with the Privacy Act? Base: Australians 18+ years (n=1,653)

The organisation type most likely to be incorrectly identified as having to comply with the Privacy Act is public schools and universities (82%), however public schools and public universities may be covered under state or territory privacy legislation. Parents of children aged

- Privacy legislation

2 to 17 are more likely to believe public schools and universities are covered (86%) compared to those without children in this age bracket (80%).

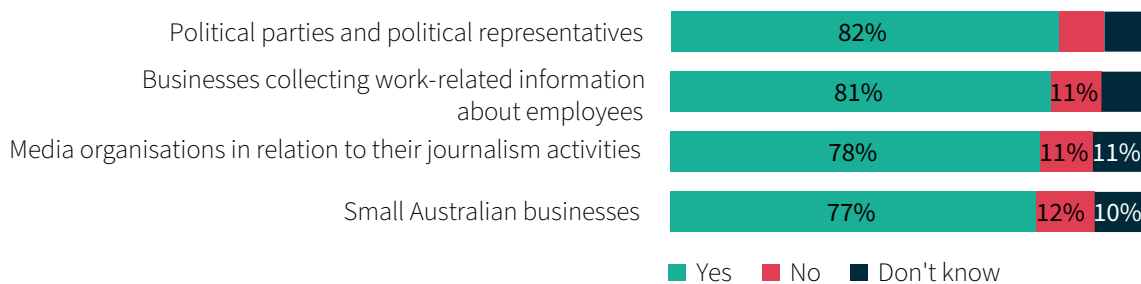
Awareness of exempt organisation types has decreased from 2020. In 2023, the proportion of people who could correctly identify exempt organisation types ranged between 6% and 13%, compared to between 12% and 17% in 2020.

The majority of people thought the exempt organisation types were covered by the Privacy Act, which is consistent with a population simply assuming most organisations are covered.

## Belief that organisation types should be covered by the Privacy Act

Four out of five people feel political parties and representatives (82%), businesses collecting work-related information about employees (81%) and media organisations in relation to their journalism activities (78%) should be required to protect personal information in the same way as federal government agencies and larger businesses. Three-quarters (77%) of Australians feel the same about small business.

**Figure 18: Belief that organisation types should be covered by the Privacy Act**



L2. The following sectors are currently exempt from the Australian Privacy Act. Should they have to handle your personal information in the same way as federal government agencies and larger businesses? Base: Australians 18+ years (n=1,653)

People aged 35 and over are more likely than younger Australians to think small businesses and businesses collecting work-related information about employees should be held to the same standards as larger businesses and government agencies (small businesses 80% 35+ years, cf. 71% 18–34 years; businesses collecting work-related information 83% 35+ years, cf. 75% 18–34 years).

- Privacy legislation

The proportion of people who think all specified organisation types *should not* have the same obligations as federal government agencies and larger businesses has not changed significantly since 2020. However, fewer people responded ‘don’t know’, resulting in a higher proportion of people in favour of removing the exemptions.

The share of people who think political parties and representatives should be held to the same standards as federal government agencies and larger business increased from 74% in 2020 to 82% in 2023, and for businesses collecting work-related information went from 73% to 81%. Media organisations and small businesses saw a 6 percentage point increase (media organisations 78% in 2023, cf. 72% in 2020; small businesses 77% in 2023, cf. 71% in 2020).

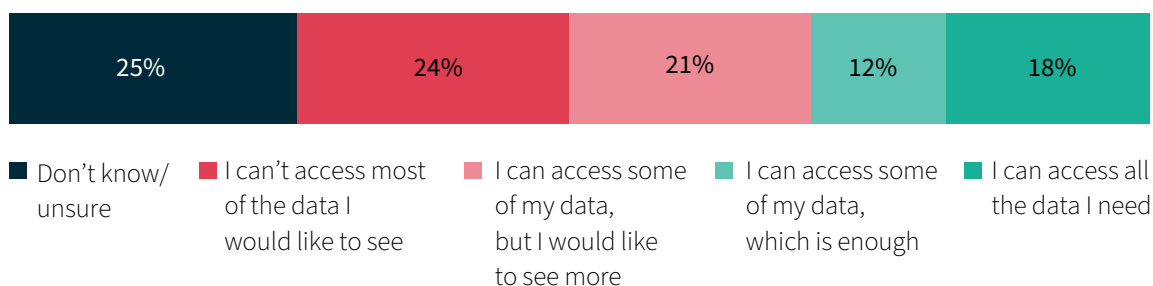
## Extent Australians can access and use data

Only 3 in 10 (30%) Australians are satisfied that they can access and use the data organisations hold about them.

A quarter (25%) of Australians do not know or are unsure about the extent they can access and use data organisations hold about them, and a quarter (24%) say that they cannot access most of the data they would like to see. A further fifth (21%) say they can access some of their data, but would like to see more.



**Figure 19: Extent Australians can access and use data**



L3. To what extent do you feel you can access and use the data organisations hold about you (e.g. your account and transaction/usage data held by banks, energy providers and telcos)? Select one. Base: Australians 18+ years (n=1,653)

- Privacy legislation

Dissatisfaction is similar across age and gender, however satisfaction is higher among those aged 18 to 34 compared to those aged 35 and older (can access all the data they need or some data, which is enough 37% 18–34 years, cf. 26% 35+ years).

Australians aged 35 and older are twice as likely as those aged 18 to 34 to not know the extent to which they can access and use their personal data (30% 35+ years, cf. 15% 18–34 years).

## Access to personal information

Less than half (47%) of Australians are aware they can request to access their personal information from an organisation, and only 1 in 10 (9%) Australians have requested access.

**Figure 20: Access to personal information held by organisations**



L4. Are you aware that you can request to access your personal information from organisations?

L5. Have you ever requested to access your personal information from an organisation?

Base: Australians 18+ years (n=1,653)

Half (51%) of males are aware they can request access, compared to 43% of females. Similarly, 52% of those aged 18 to 34 are aware compared to 44% for those aged 35 and over.

Australians aged 18 to 34 are twice as likely as people aged 35 and over to have made a request (15% 18–34 years, cf. 7% 35+ years). Age differences become even greater when comparing the youngest and oldest cohorts, with 16% of those aged 18 to 24 having requested access to personal information from organisations compared to 4% of those aged 65 and older.

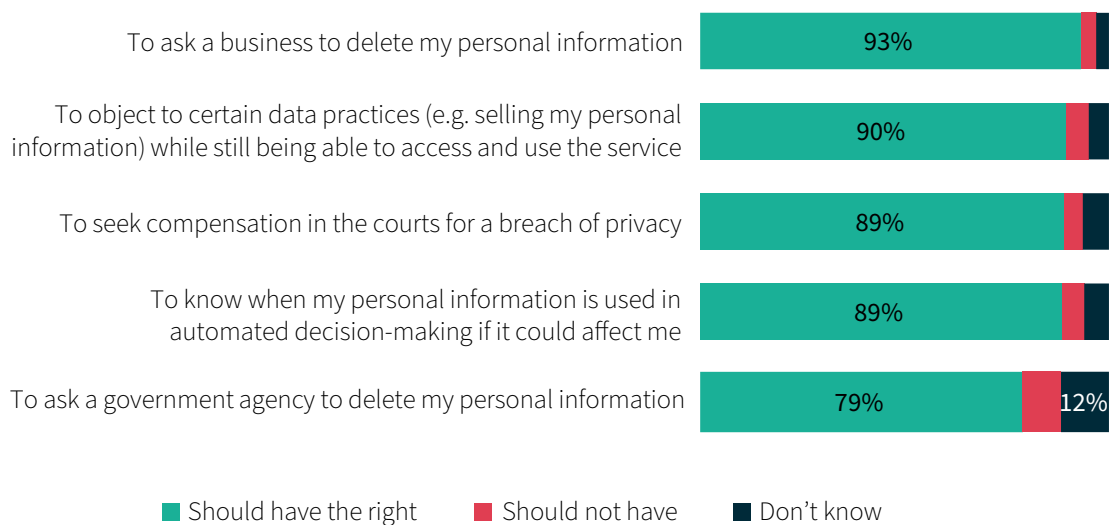
## Additional rights under the Privacy Act

Australians strongly believe they should have extra rights under the Privacy Act.

They are most likely to believe they should have the right to ask a business to delete their personal information (93%). This has strong and consistent support across age groups and genders.

Nine in ten Australians say they should have the right to object to certain data practices while still being able to access and use a service (90%), to seek compensation in the courts for a breach of privacy (89%) and to know when their personal information is used in automated decision-making if it could affect them (such as when information about their race is used to determine what information they see in their social media feed) (89%).

**Figure 21: Beliefs that Australians should have specific privacy rights**

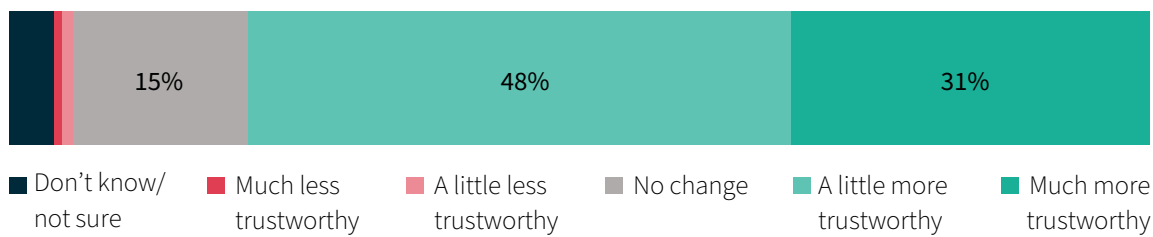


L6. Do you believe you should have these rights under the Australian Privacy Act? Base: Australians 18+ years (n=1,653)

## Privacy certification

A privacy certification system, where an independent body rates how well an organisation protects personal information, would make certified organisations more trustworthy to 4 in 5 (79%) Australians.

**Figure 22: Impact of privacy certification on trust in organisations**



L7. Consider if a privacy certification system was introduced in Australia, where an independent body rates how well an organisation protects your personal information. To what extent would this make certified organisations more or less trustworthy? Base: Australians 18+ years (n=1,653)

### 3 most important things to include in privacy policies



Females would see certified organisations as more trustworthy than males (83% females, cf. 75% males).

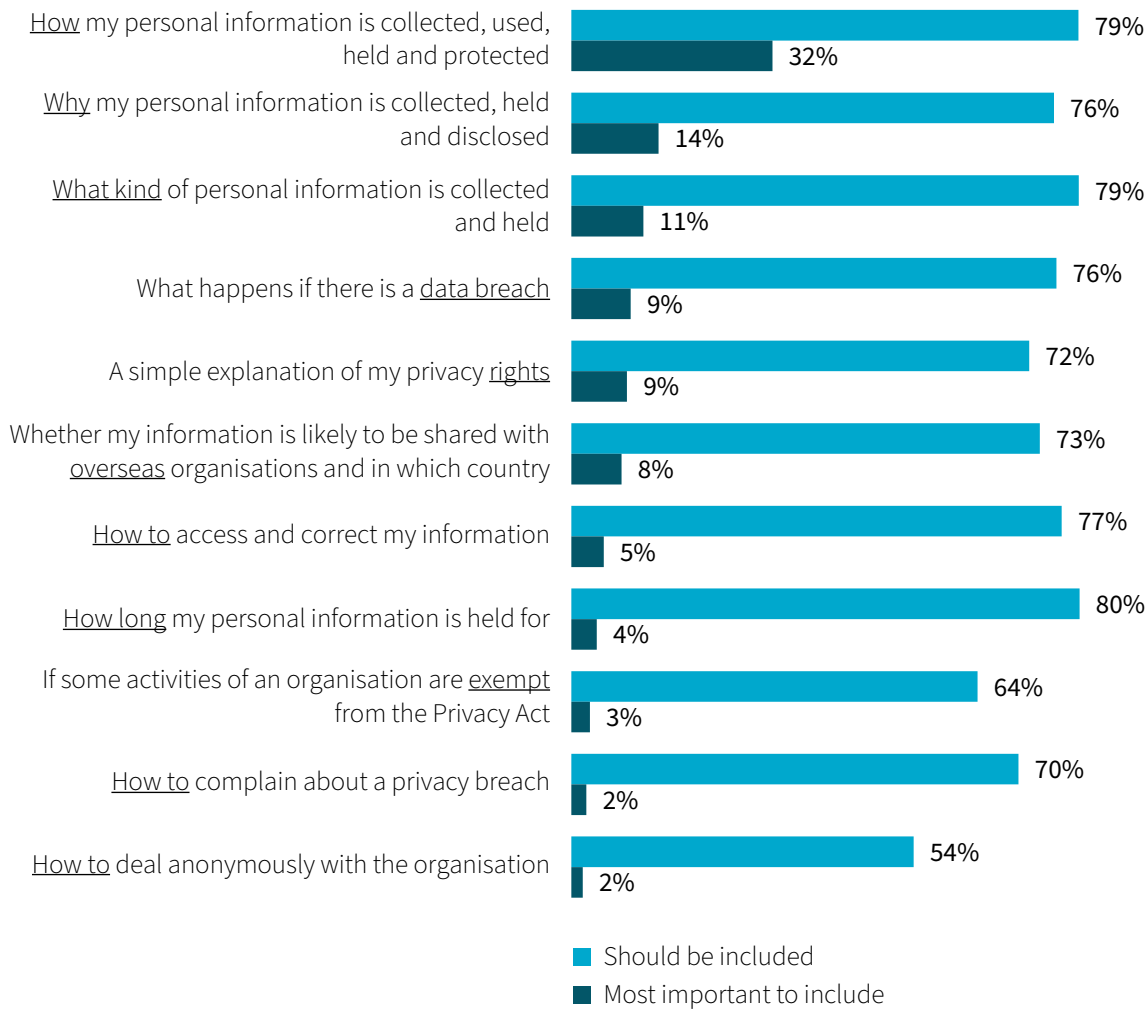
### Desired content in privacy policies

Australians want a wide range of information to be included in privacy policies. Of the options provided, 'how my personal information is collected, used, held and protected' is the 'most important' inclusion for a third (32%) of people.

There is also a strong desire for transparency around 'why' the data is being collected, held and disclosed (14% most important), as well as 'what kind' of information is being collected and held (11% most important).

Three in ten (29%) Australians believe all aspects listed should be included in privacy policies. Among this cohort, 35% believe 'how' the information is collected, used, held and protected is the most important thing to include.

**Figure 23: Desired content in privacy policies**



L8. 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? Select all that apply.

L9. Which of the following do you think is the most important thing to be in all privacy policies? Select one.

Base: Australians 18+ years (n=1,653)

Australians aged 18 to 34 are nearly twice as likely as people aged 35 and over to say a simple explanation of their privacy rights is the most important inclusion (13% 18–34 years, cf. 7% 35+ years).



# Part 3

## The role of organisations



## Part 3: The role of organisations

Australians want organisations to do more to protect their data and be transparent about what they do with their personal information. They frequently do not know what organisations do with their data and often feel they have no choice but to hand over personal information if they want to access a service.

While most Australians expect they might need to share some level of personal information to access a service, they generally only consider it fair and reasonable to provide their name and email address. The information considered fair and reasonable to provide varies by how trustworthy they consider the industry sector to be.

Health service providers and federal government agencies are generally considered the most trustworthy organisations when it comes to handling personal information, while social media companies and real estate agencies are the least trusted.

Most Australians are concerned about the prospect of their personal data being sent overseas, and the level of concern increases with age. It is also reflected in the trust associated with where an organisation is based. Australian businesses are more trusted than those based overseas, even if they have a presence in Australia.



- The role of organisations

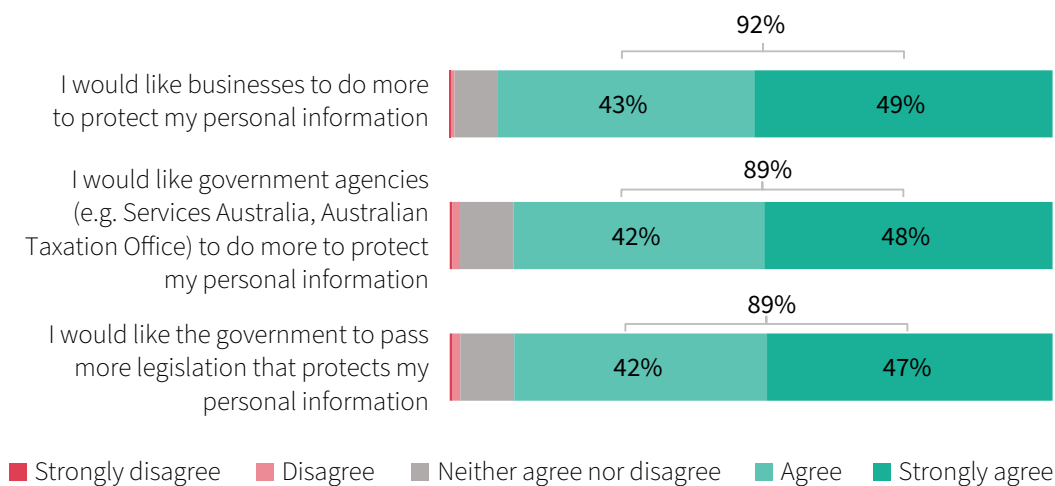
## Responsibility for protecting personal information

While many Australians do not know exactly how they can protect their own personal information, the majority would like organisations to do more in this area.

There is a common view that businesses should do more to protect Australians' personal information (92% 'agree' or 'strongly agree'), as should government agencies (89%).

Nine in ten (89%) respondents would like government to pass more legislation that protects their personal information.

**Figure 24: Beliefs that organisations should do more to protect personal information**



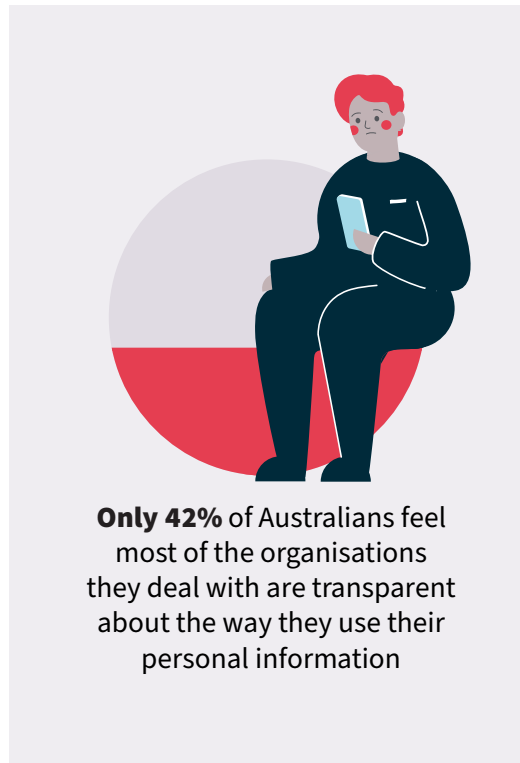
G7. To what extent do you agree or disagree with the following? 'Agree' and 'strongly agree'. Base: Australians 18+ years (n=1,916)

The only significant variation in this view lies with Australians aged 18 to 24, who see a similar need for government to pass more legislation to protect them (87%), but are less likely to expect businesses (84%) and government agencies (82%) to do more.

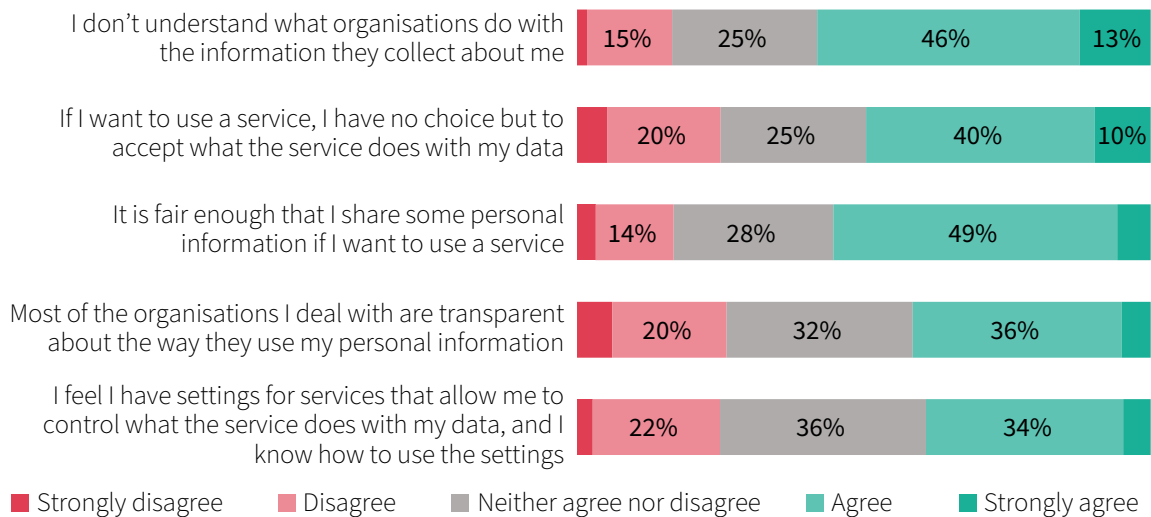
## Beliefs about organisations' personal information handling practices

Three in five (58% 'agree' or 'strongly agree') Australians do not understand what organisations do with the information that is collected about them.

Around half of people agree it is fair enough to share some information to use a service (55% 'agree' or 'strongly agree'), but a similar proportion (50%) feel they have no choice but to accept what a service does with their data.



**Figure 25: Beliefs about organisations' personal information handling practices**



G6. Thinking about data privacy, to what extent do you agree or disagree with the following? Base: Australians 18+ years (n=1,916)

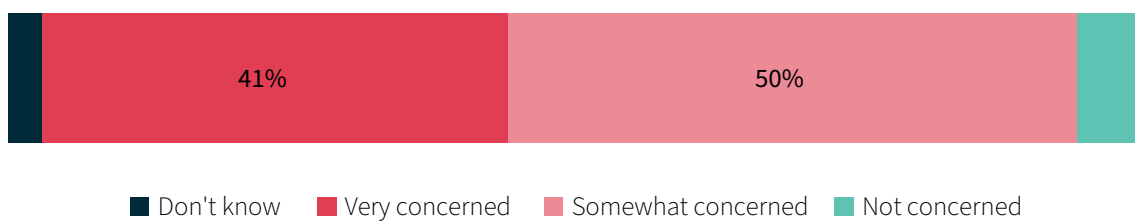
Australians aged 25 to 34 are more likely to believe if they want to use a service, they have no choice but to accept what the service does with their data (58% 'agree' or 'strongly agree', cf. average 50%).

Those aged 18 to 34 are more likely to feel they are able to control what the service does with their data through the use of settings (50% 'agree' or 'strongly agree', cf. average 39%).

## Concern about information being sent overseas

Most Australians (91%) are concerned about organisations sending their customers' information from Australia to overseas, with 2 in 5 (41%) 'very concerned'. Only 6% of people are 'not concerned'.

**Figure 26: Concern about organisations sending personal information overseas**

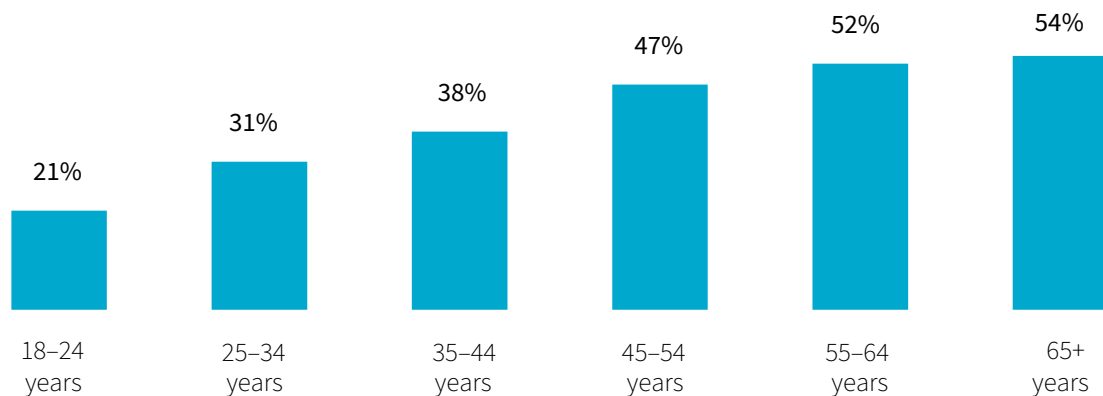


F4. How concerned are you about organisations sending their customers' personal information from Australia to overseas? Base: Australians 18+ years (n=1,642)

The higher levels of concern about privacy among older Australians can also be seen in their attitude to organisations sending their customers' personal information from Australia to overseas.

Over half (53%) of Australians aged 55 and over are 'very concerned' about Australians' personal information being sent overseas, decreasing to 21% among people aged 18 to 24.

**Figure 27: Concern about organisations sending personal information overseas by age**

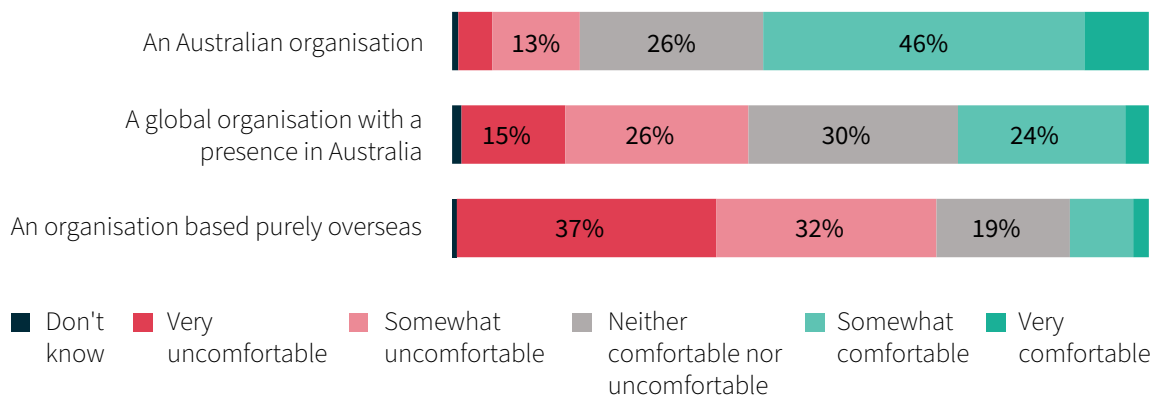


F4. How concerned are you about organisations sending their customers' personal information from Australia to overseas? 'Very concerned'. Base: Australians 18+ years (n=1,642)

## Comfort dealing with local vs overseas organisations

Most Australians (55%) are comfortable sharing their personal information with local organisations, but that level of comfort falls when dealing with overseas organisations, even if they have a local presence (27% global with an Australian presence, cf. 11% based purely overseas).

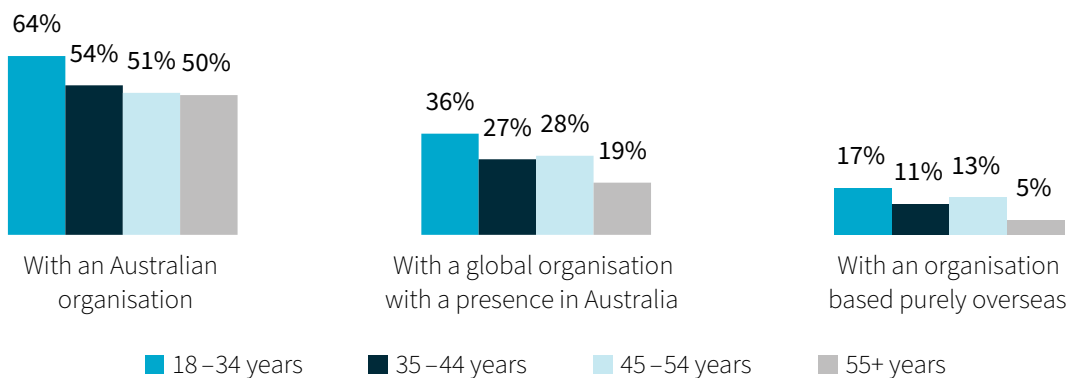
**Figure 28: Comfort sharing personal information with local and overseas organisations**



F5. How comfortable are you with sharing your personal information with the following? Base: Australians 18+ years (n=1,642)

Again, age has an impact on how at ease people feel. Australians aged 18 to 34 more likely to be comfortable sharing their data with local and overseas organisations (including those with a presence in Australia), although the majority (56%) are uncomfortable sharing data with an organisation based purely overseas.

**Figure 29: Comfort sharing personal information with local and overseas organisations by age**



F5. How comfortable are you with sharing your personal information with the following? 'Very comfortable' and 'somewhat comfortable'. Base: Australians 18+ years (n=1,642)

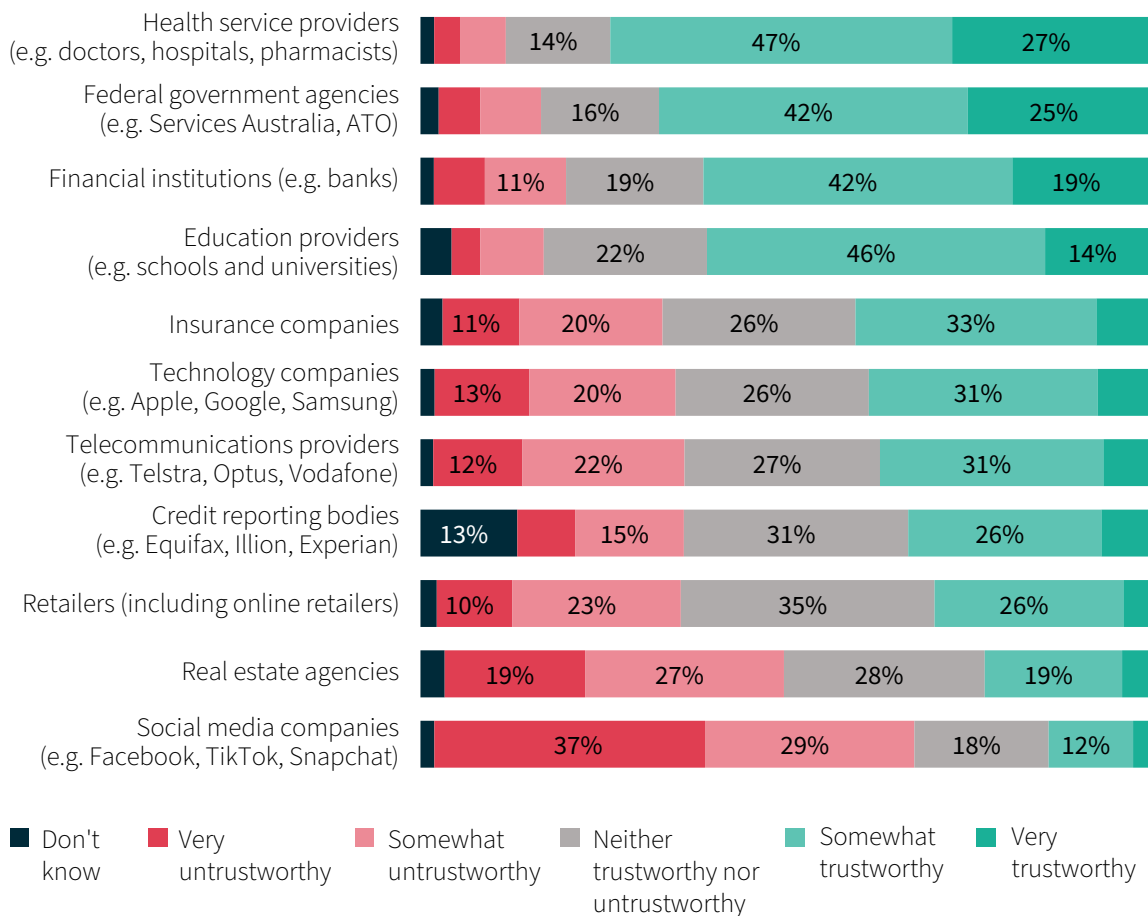
## Trust in organisations

### Trustworthiness by industry sector

Health service providers are the most trusted industry sector when it comes to the protection and use of personal information. This is especially true for older Australians, with those aged 55 and over more likely to rate health service providers as ‘very’ or ‘somewhat trustworthy’ (78% 55+ years, cf. 74% all adults).

Social media companies and real estate agencies are the least trusted industry sectors from the list surveyed. Two-thirds (66%) of Australians say they find social media companies to be ‘very’ or ‘somewhat untrustworthy’, with half (46%) saying the same of real estate agencies.

**Figure 30: Trustworthiness by industry sector**



F1. How trustworthy would you say the following organisations are with regard to how they protect and use your personal information? Base: Australians 18+ years (n=1,642)

- The role of organisations

Australians aged 55 and older are more likely to trust federal government agencies, financial institutions and telecommunications providers than the average person.

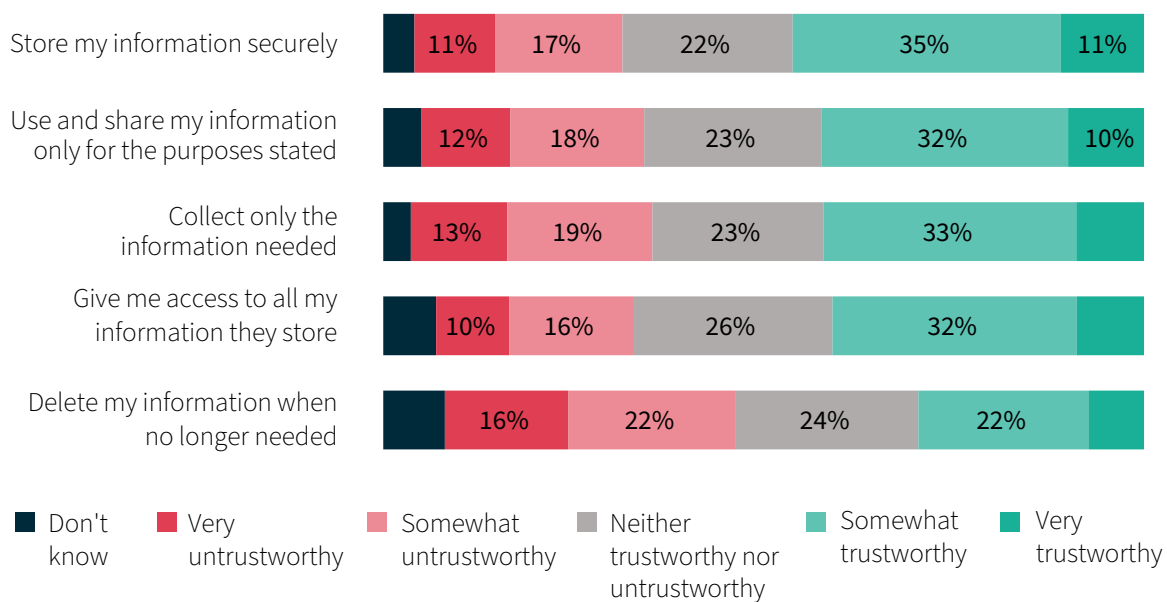
Australians under 35 are more likely to trust real estate agencies and social media companies than those aged 35 and older – although they still classify them as the least trustworthy on the list.

## Trust in aspects of personal information handling

There is a high level of distrust that organisations will do the right thing by Australians when it comes to the handling of personal information. Less than half of people trust organisations to:

- store their information securely (46% ‘very trustworthy’ or ‘somewhat trustworthy’)
- use and share their information only for the purposes stated (42%)
- collect only the information needed (42%)
- give people access to all their personal information stored (41%)
- delete their information when no longer needed (30%).

**Figure 31: Trust in aspects of personal information handling**



F3. How trustworthy would you say <sector> are with regard to the following? Aggregated across 9 industry sectors. Base: Australians 18+ years (n=1,642)

- The role of organisations

There is a widely held belief that health service providers, federal government agencies and financial institutions are trustworthy across most aspects of personal information handling tested.

Most sectors are not trusted to only collect the information they need, use and share information as they state, store information securely, give individuals access to their personal information and delete information when no longer needed. Retailers and social media companies are perceived as the least likely to do these things.

**Figure 32: Trust in aspects of personal information handling by industry sector**

	Health service providers	Gov agencies	Financial inst.	Insurance co.	Tech co.	Telcos	Retailers	Real estate agencies	Social media co.
Collect only the information needed	68%	57%	57%	41%	32%	38%	32%	36%	17%
Use and share my information only for the purposes stated	69%	61%	60%	42%	33%	35%	29%	34%	17%
Store my information securely	67%	67%	64%	49%	43%	39%	33%	31%	20%
Give me access to all my information they store	55%	55%	51%	43%	37%	39%	30%	35%	23%
Delete my information when no longer needed	46%	41%	40%	29%	26%	24%	22%	25%	14%

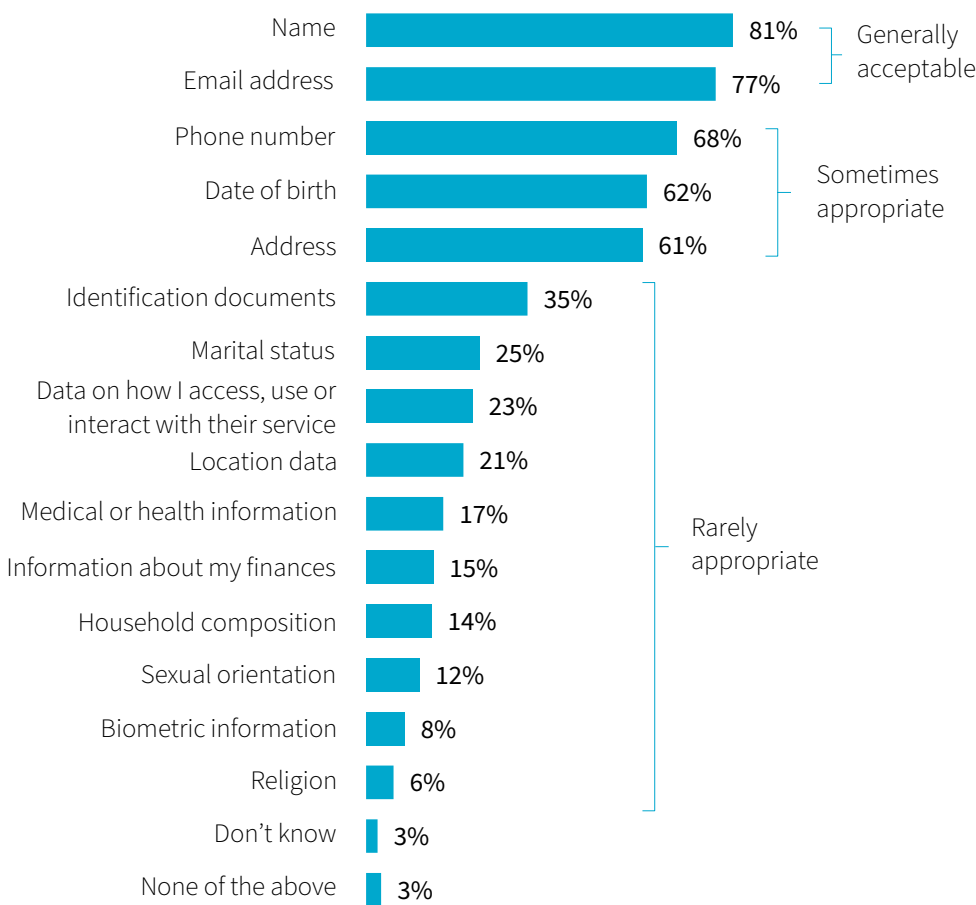
F3. How trustworthy would you say <sector> are with regard to the following? ‘Very trustworthy’ and ‘somewhat trustworthy’. Base: Australians 18+ years (n=1,642)



## Information considered fair and reasonable to provide

Australians are usually happy to divulge their name and email address when accessing a service, then, dependent on the type of organisation, generally consider providing their phone number, date of birth and address as fair and reasonable.

**Figure 33: Information considered fair and reasonable to provide when accessing services**



F2. What information would you consider to be fair and reasonable to provide <sector> when accessing services? Aggregated across 9 industry sectors. Base: Australians 18+ years (n=1,642)

While the majority of Australians consider it fair and reasonable to supply their name, email, phone number, date of birth and address when accessing services, this varies by industry sector.

There is more reluctance to supply some of these details, especially date of birth, to technology companies, retailers, real estate agencies and social media companies.

- The role of organisations

While real estate agencies are generally viewed with distrust, Australians consider a range of information is fair and reasonable to provide to them.

**Figure 34: Information considered fair and reasonable to provide when accessing services by industry sector**

	Health service providers	Gov agencies	Financial inst.	Insurance co.	Tech co.	Telcos	Retailers	Real estate agencies	Social media co.
Name	86%	79%	85%	85%	77%	84%	80%	83%	67%
Email address	72%	74%	81%	83%	80%	83%	80%	78%	60%
Phone number	79%	71%	79%	79%	58%	82%	64%	77%	25%
Date of birth	85%	79%	82%	80%	45%	66%	37%	41%	40%
Address	74%	76%	77%	81%	39%	69%	52%	67%	11%
Identification docs	38%	62%	66%	47%	14%	41%	10%	36%	6%
Marital status	35%	51%	34%	30%	14%	13%	12%	19%	15%
Interaction data	24%	28%	26%	21%	30%	28%	19%	13%	22%
Location data	20%	20%	22%	30%	21%	25%	15%	23%	16%
Medical/health info	81%	22%	8%	27%	3%	3%	4%	2%	4%
Financial info	4%	27%	48%	17%	3%	6%	5%	21%	2%
Household comp.	12%	23%	15%	22%	7%	10%	8%	24%	7%
Sexual orientation	29%	17%	11%	7%	10%	10%	6%	4%	12%
Biometric info	11%	15%	15%	5%	13%	7%	3%	1%	6%
Religion	13%	11%	5%	3%	5%	4%	4%	1%	8%

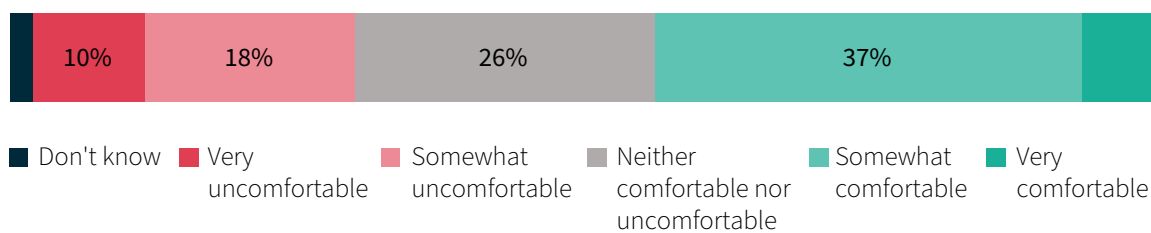
F2. What information would you consider to be fair and reasonable to provide to <sector> when accessing their services? Base: Australians 18+ years (n=1,642)

## Government use of personal information for research and service and policy development

There has been a growing level of comfort with the government using personal information for research and service and policy development over the last 6 years.

Around two-fifths (44%) of Australians are ‘very’ or ‘somewhat comfortable’ with the government using their personal information for research and service and policy development, up from 38% in 2017 and 40% in 2020.

**Figure 35: Comfort with the use of personal information for government research and development**



F7. How comfortable are you with the personal information that you’ve provided to government agencies being used for research, service development or policy development purposes? Base: Australians 18+ years (n=1,642)

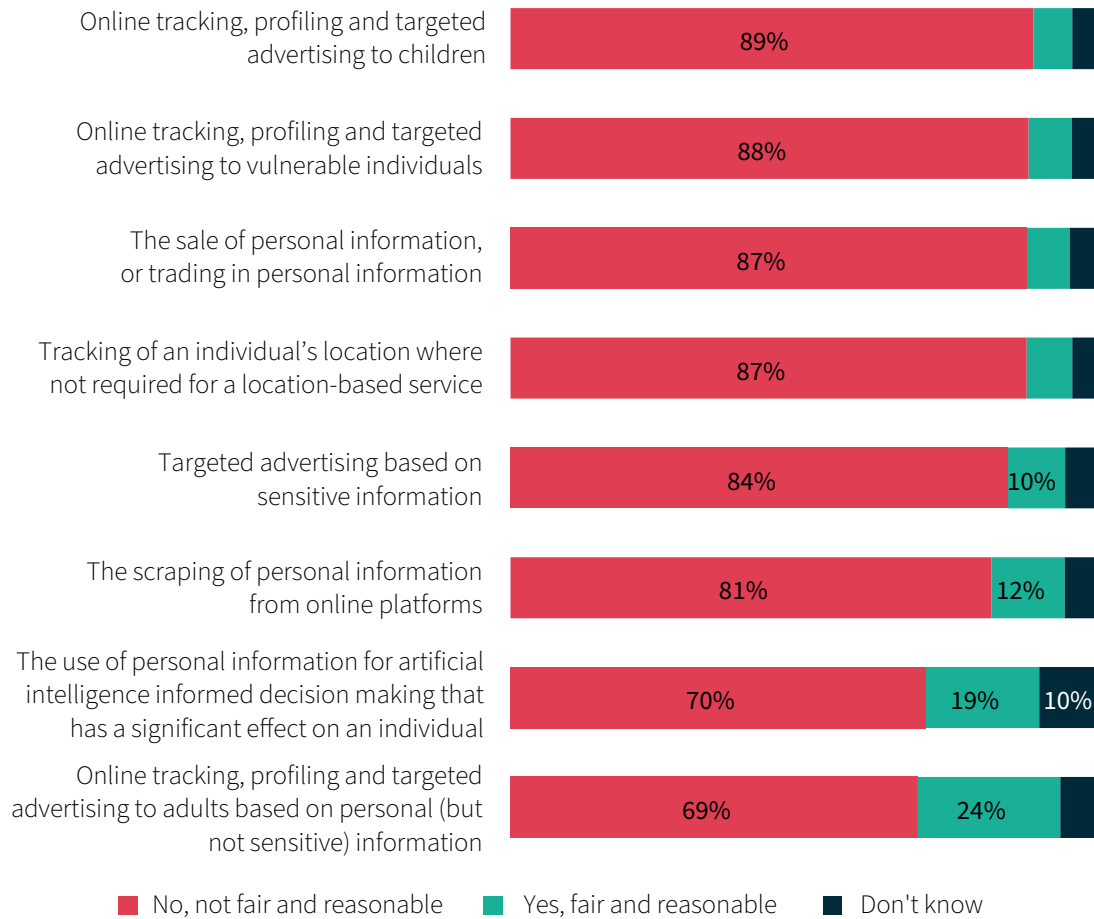
People aged 65 and older are more comfortable than the average Australian, with 53% ‘very’ or ‘somewhat comfortable’.

## Beliefs about whether certain practices are fair and reasonable

The definition of what is fair and reasonable can vary when it comes to the sharing of personal information, depending on the industry sector of the organisation the data is being shared with. However, there are some strong opinions around certain practices generally.

The majority of Australians consider the practices tested to be not fair and reasonable. The practices most likely to be considered ‘not fair and reasonable’ are the online tracking, profiling and targeting of advertising to children (89%) and vulnerable individuals (such as gambling companies targeting gamblers) (88%).

**Figure 36: Beliefs about whether certain practices are fair and reasonable**



F6. Do you consider the following to be fair and reasonable practices? Base: Australians 18+ years (n=1,642)



# Part 4

## Privacy breaches and harm

## Part 4: Privacy breaches and harm

New to ACAPS for 2023 is this section on privacy breaches and associated harms.

Most Australians had an issue with how their personal information was handled and almost half were directly impacted by a data breach in the 12 months prior to completing the survey.

Three-quarters of those who were involved in a data breach said they experienced some form of harm as a result. The most common harm experienced was an increase in scams or spam emails and texts. One in ten experienced emotional or psychological harm.

Almost half of people say they would stop using a service if their data was involved in a breach, but this drops to a third for people who have recently experienced a breach.

When it comes to dealing with the impacts of a breach, only 1 in 10 people said there was nothing an organisation could do to appease them. Most Australians are willing to remain with an organisation that has experienced a data breach, provided the organisation quickly takes action, such as putting steps in place to prevent customers from suffering harm.

To protect their data, Australians want organisations to only collect the data they need, take proactive steps to protect personal information they hold, and delete it when it is no longer needed.



- Privacy breaches and harm

## Privacy breaches

The term ‘privacy breach’ is used in this report to refer to a wide range of problems experienced with the handling of personal information. It is distinct from ‘[data breach](#)’ – respondents were shown a definition of ‘data breach’ before the relevant section of the survey.

### Problems experienced with the handling of personal information

Almost two-thirds (64%) of Australians experienced at least one problem with the handling of their personal information in the 12 months prior to completing the survey.

**Figure 37: Problems experienced with the handling of personal information**



P3. Have you experienced any of the following in the past 12 months. Select all that apply.

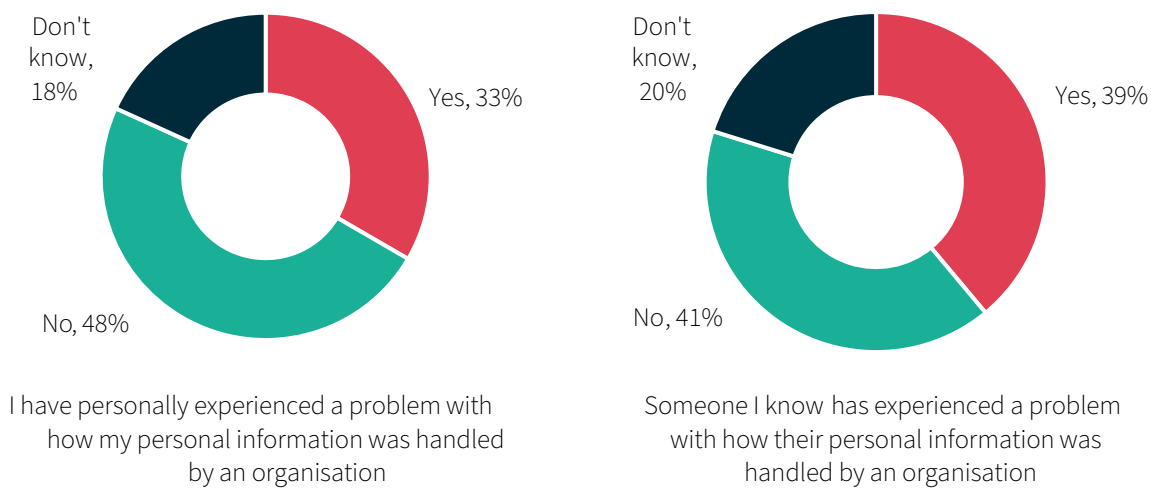
Base: Australians 18+ years (n=1,626)

- Privacy breaches and harm

## Incidence of privacy breaches

A third (33%) of Australians personally experienced a problem with how their personal information was handled by an organisation in the 12 months prior to completing the survey. This drops to a quarter (26%) among Australians aged 65 and over, compared to 35% for those aged 18 to 64.

**Figure 38: Incidence of privacy breaches**



P4. In the past 12 months, have you personally experienced a problem with how your personal information was handled by an organisation?

P5. Has someone you know experienced a problem with how their personal information was handled by an organisation?

Base: Australians 18+ years (n=1,626)

Two in five (39%) Australians know someone who has experienced a problem with how their personal information was handled by an organisation. Like personal experience, this is lower among those aged 65 and over (26%) compared to those aged 18 to 64 (42%).

A quarter (25%) of Australians have both had a problem with how their personal information was handled and know someone else who has experienced this.

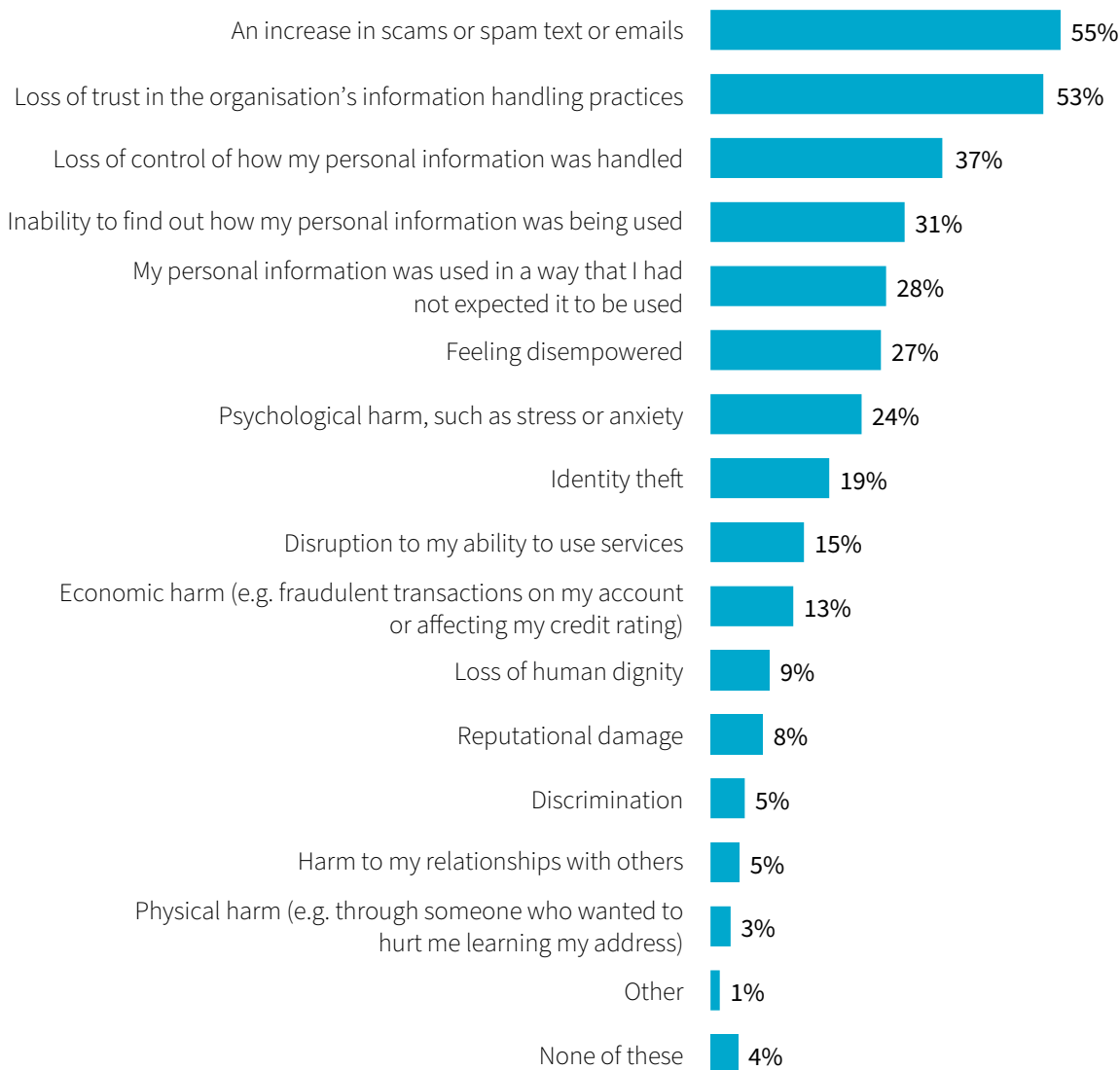


## Harms experienced from privacy breaches

Among Australians who personally experienced a problem with how their personal information was handled by an organisation in the 12 months prior to completing the survey, more than half (55%) reported an increase in scams or spam texts or emails. More than half (53%) said they lost trust in the organisation’s information handling practices.

Two in five (37%) experienced a loss of control of how their data was being handled, while nearly a third (31%) reported an inability to find out how their personal information was being used.

**Figure 39: Harms experienced from privacy breaches**



P6. Which of the following have you experienced because of a problem with how your personal information was handled by an organisation? Select all that apply. Base: Australians who have experienced a problem with how their personal information was handled by an organisation (n=540)



More females reported an inability to find out how their information was being used than males (38% females, cf. 24% males). Females are also more likely to say they feel disempowered because of a problem with how their personal information was handled by an organisation (32% females, cf. 22% males).

### **Harms Australians perceive could result from a privacy breach**

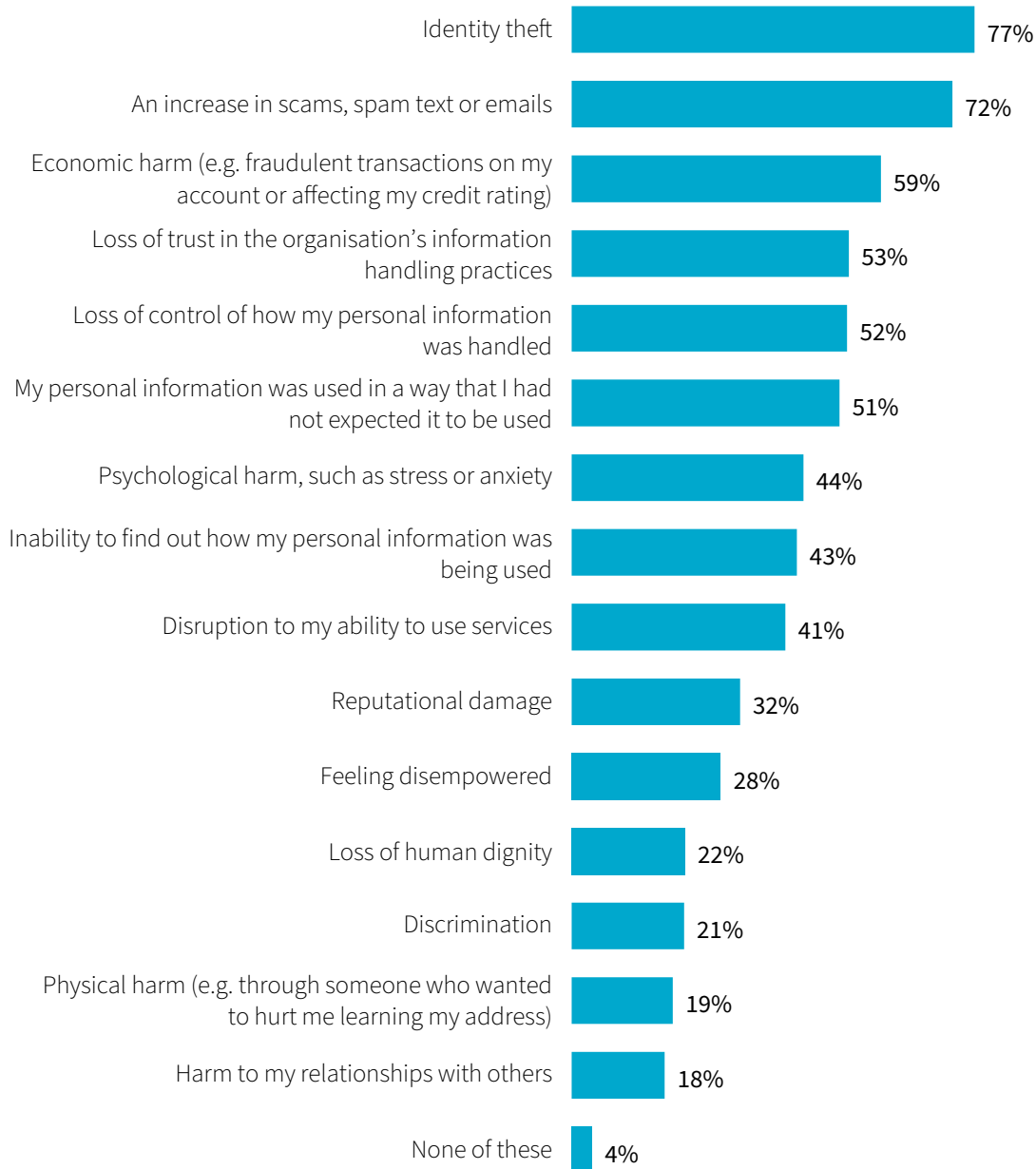
Among Australians who had not experienced a problem with how their personal information was handled by an organisation in the 12 months prior to completing the survey, around three-quarters believe identity theft (77%) and an increase in scams or spam texts or emails (72%) could result from their information being mishandled. The belief that identity theft could result from mishandled personal information increases with age (86% 55+ years, cf. 76% 35–54 years, 67% 18–34 years).

Females are much more likely to cite potential problems like loss of trust in the organisation’s information handling practices (57%, cf. 48% males), loss of control (57%, cf. 48% males), psychological harm, such as stress or anxiety (50%, cf. 38% males), feeling disempowered (33%, cf. 23% males) and physical harm (23%, cf. 15% males).

For Australians who have not recently had their personal information mishandled, there is an inflated expectation that a privacy breach is likely to result in identity theft (77% perceived harm, cf. 19% harm experienced) and economic harm (59% perceived harm, cf. 13% harm experienced).

An increase in scams, spam texts or emails was most likely to be experienced and the second highest perceived harm (72% perceived harm, cf. 55% harm experienced).

**Figure 40: Harms Australians perceive could result from a privacy breach**



P7. Which of the following do you think could result from a problem with how your personal information was handled by an organisation? Select all that apply. Base: Australians who haven't experienced a problem with how their personal information was handled by an organisation (n=1,086)

- Privacy breaches and harm

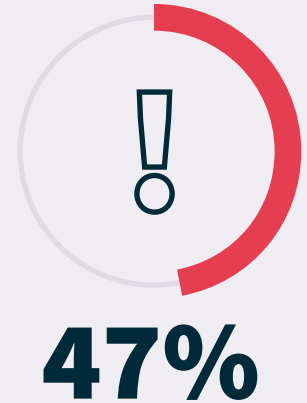
## Data breaches

A data breach is a type of privacy breach that occurs when personal information held by an organisation is accessed or disclosed without authorisation, or is lost. Data breaches may result from malicious actors, human error or errors in business or technology processes.

### Awareness and impact of data breaches

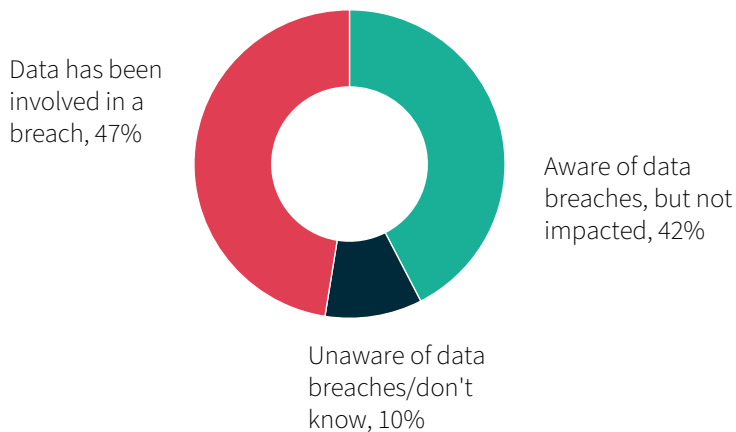
The majority (90%) of Australians were aware of data breaches occurring in Australia in the 12 months prior to completing the survey.

Almost half (47%) said they had been told by an organisation that their data was involved in a data breach in the prior year. A similar proportion (51%) know someone who was affected by a data breach in the same period.



of Australians were told by an organisation their information was involved in a data breach in the year prior

**Figure 41: Awareness and impact of data breaches**



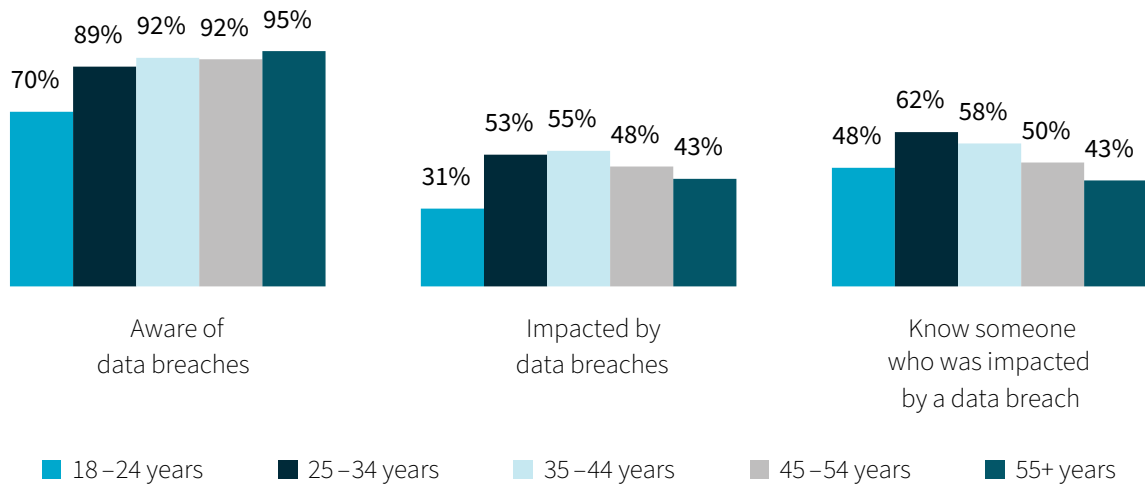
P9. Are you aware of any data breaches occurring in Australia in the last 12 months?

P10. In the past 12 months, has an organisation told you that your information was involved in a data breach?

Base: Australians 18+ years (n=1,626)

Awareness of data breaches is much higher among older Australians compared to the youngest age group (95% awareness 55+ years, cf. 70% 18–24 years). However, the age group most likely to be impacted directly by a data breach was Australians aged 25 to 44 (54%, cf. 43% 55+ years).

**Figure 42: Awareness and impact of data breaches by age**



P9. Are you aware of any data breaches occurring in Australia in the last 12 months?

P10. In the past 12 months, has an organisation told you that your information was involved in a data breach?

P11. Was someone you know affected by a data breach in the last 12 months?

Base: Australians 18+ years (n=1,626)

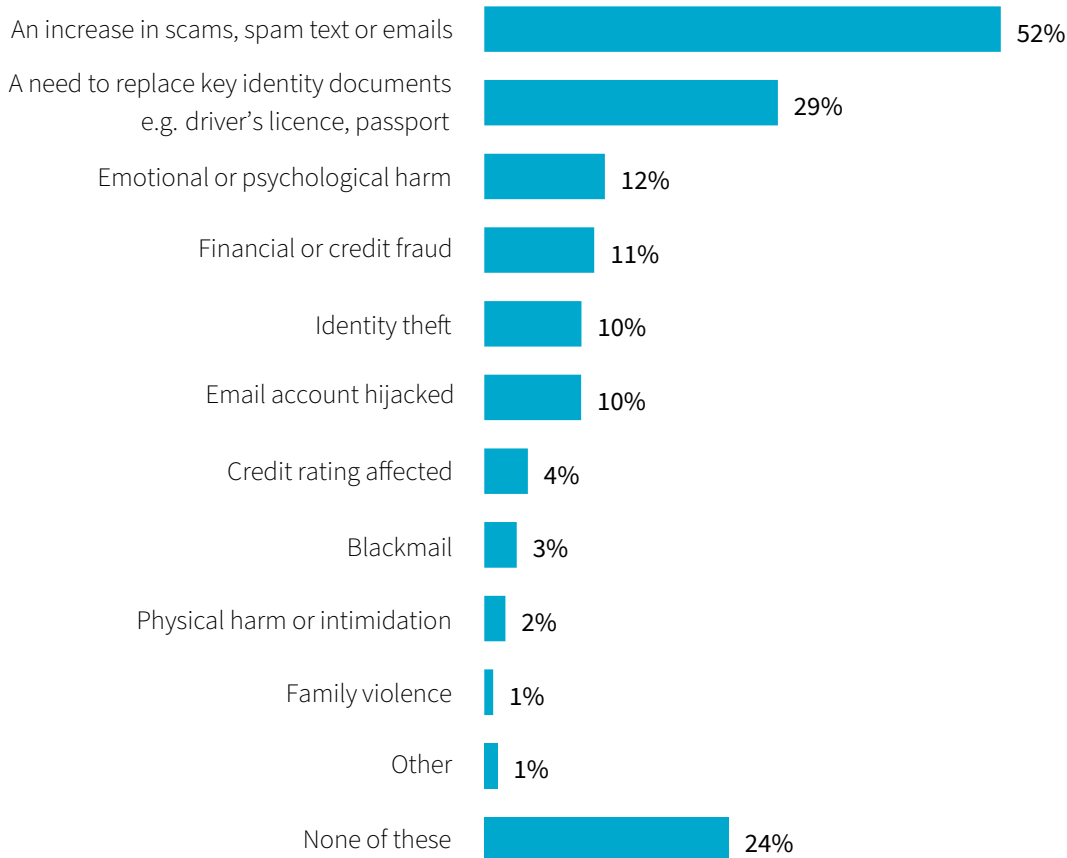
## Harms experienced from data breaches

Three-quarters (76%) of Australians whose data was involved in a breach said they experienced harm as a result.

More than half (52%) of Australians whose data was compromised in a breach reported an increase in scams, spam texts or emails. This is consistent with the experiences of those whose data was involved in a privacy breach.

Around 1 in 10 experienced significant issues such as emotional or psychological harm (12%), financial or credit fraud (11%) or identity theft (10%).

**Figure 43: Harms experienced from data breaches**



P12. Which, if any, of the following have you personally experienced because of a data breach of an organisation? Select all that apply. Base: Australians whose information was involved in a data breach (n=760)

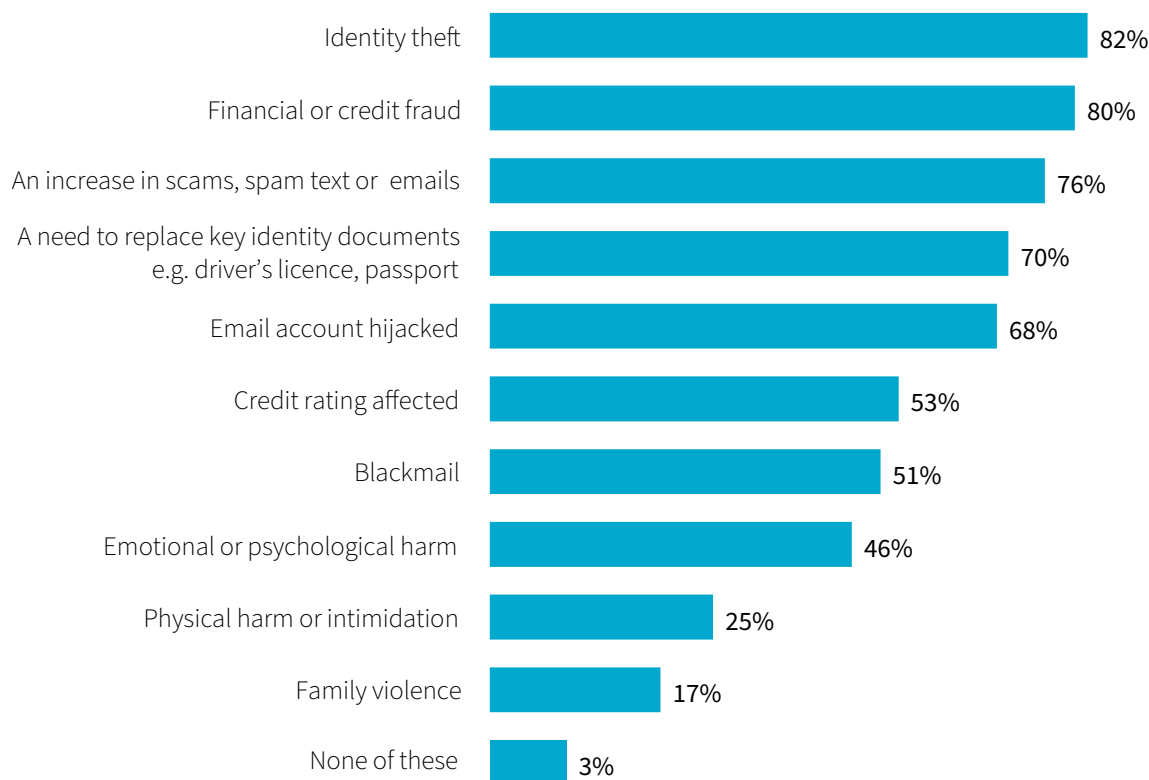
### Harms Australians perceive could result from a data breach

Four in five people who have not been affected by a data breach believe identity theft (82%) or financial or credit fraud (80%) could result from such a breach.

Australians aged 18 to 34 are much less likely than those aged 35 and over to think identity theft (70% 18–34 years, cf. 88% 35+ years) or financial or credit fraud (70% 18–34 years, cf. 85% 35+ years) could result from a data breach.

As with privacy breaches, the harms experienced from a data breach are different to the harms people think could result. The expectations are similar in that they often focus on identity theft and financial fraud.

**Figure 44: Harms Australians perceive could result from a data breach**



P13. Which of the following do you think could result from a data breach of an organisation? Select all that apply. Base: Australians who haven't had personal information involved in a data breach (n=866)

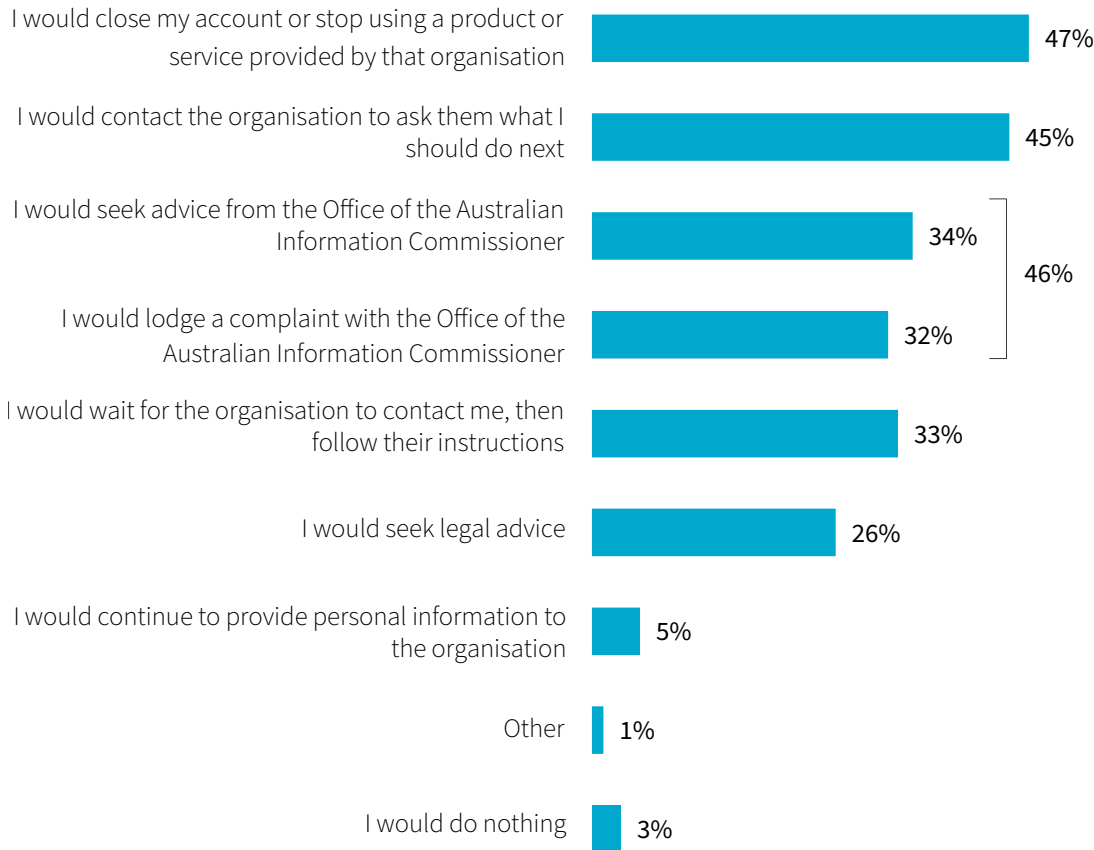
## Reactions to data breaches

Nearly half (47%) of Australians would close their account or stop using a product or service provided by an organisation that experienced a data breach, 45% would contact the organisation to ask them what to do next and a third (33%) would wait for the organisation to contact them, then follow their instructions.

Almost half (46%) of Australians say they would either seek advice from or lodge a complaint with the OAIC in the event of a data breach. This is driven by those aged 65 and over (55% 65+ years, cf. 44% 18–64 years).

However, this measure should be viewed in the context of completing the online survey, which had earlier probed awareness of the OAIC as an organisation that 'exists to uphold privacy laws and to investigate complaints about the misuse of personal information'. This creates a situation where respondents have been educated while completing the survey, highlighted within the group of respondents who were previously unaware of the OAIC, of whom 42% now state they would seek advice from or lodge a complaint with the OAIC in the event of a data breach.

**Figure 45: Reactions to a data breach**



P14. How would you react if your personal information was involved in a data breach of an organisation? Select all that apply. Base: Australians 18+ years (n=1,626)

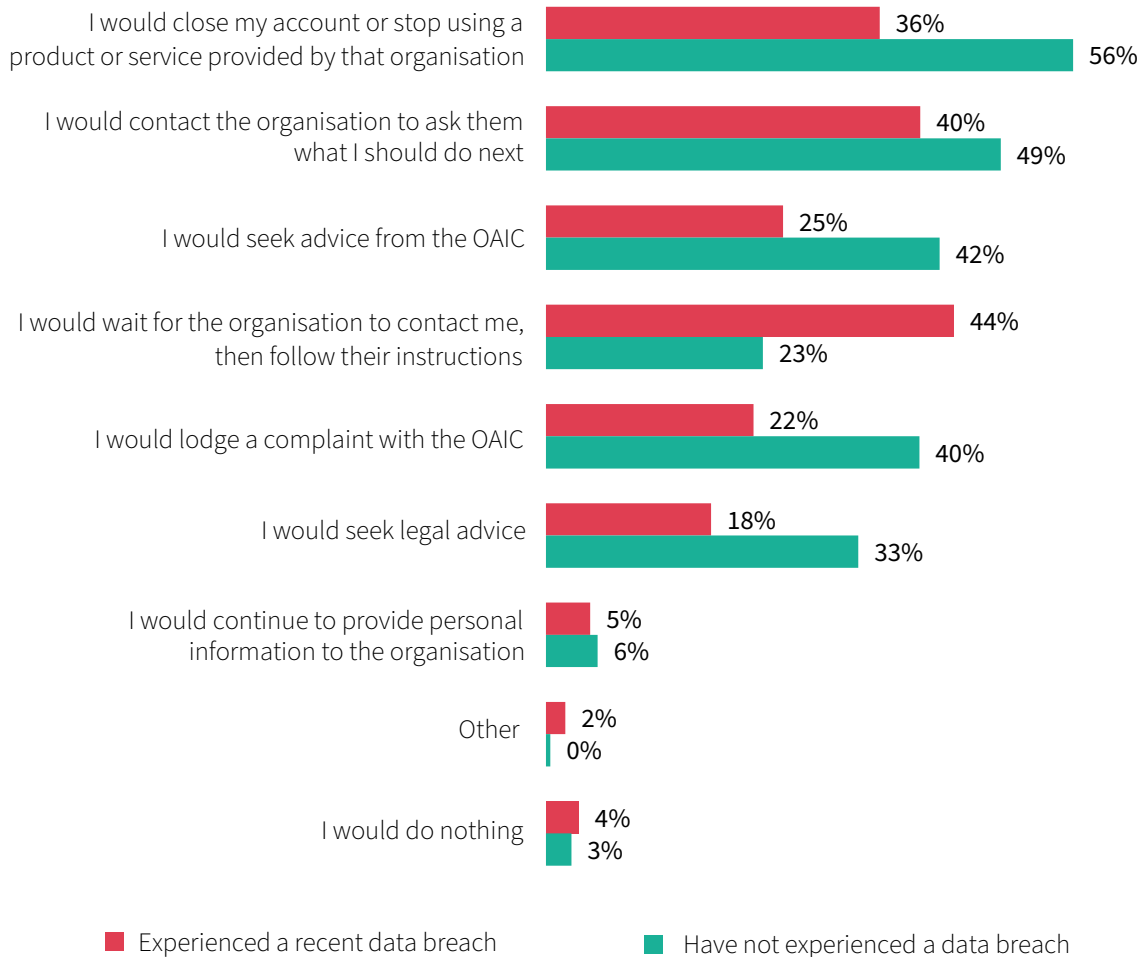
These views vary for people who have experienced a data breach compared to those who have not.

Australians who have experienced a data breach are most likely to say they would wait for the organisation to contact them and follow their instructions (44% experienced a data breach, cf. 23% not experienced a data breach).

People who have not experienced a data breach are most likely to report they would stop using the organisation's product or service (56% not experienced a data breach, cf. 36% experienced a data breach).



**Figure 46: Reactions to a data breach by experience of data breach**



P14. How would you react if your personal information was involved in a data breach of an organisation?

Select all that apply. Base: Australians 18+ years (n=1,626)

P10. In the past 12 months, has an organisation told you that your information was involved in a data breach?

Base: Australians 18+ years, experienced a data breach in the previous 12 month (n=760), did not experience a data breach (n=866)

- Privacy breaches and harm

## Factors that influence Australians to remain with organisations

Most Australians are willing to remain with an organisation that has suffered a data breach, provided the organisation quickly takes action.

From a list of 8 factors that may influence an individual to remain with an organisation, respondents on average picked 4 or 5 options.

The actions most likely to influence an individual to remain with an organisation are the organisation quickly putting steps in place to prevent customers experiencing further harm from the breach (62%) and making improvements to its security practices (61%).

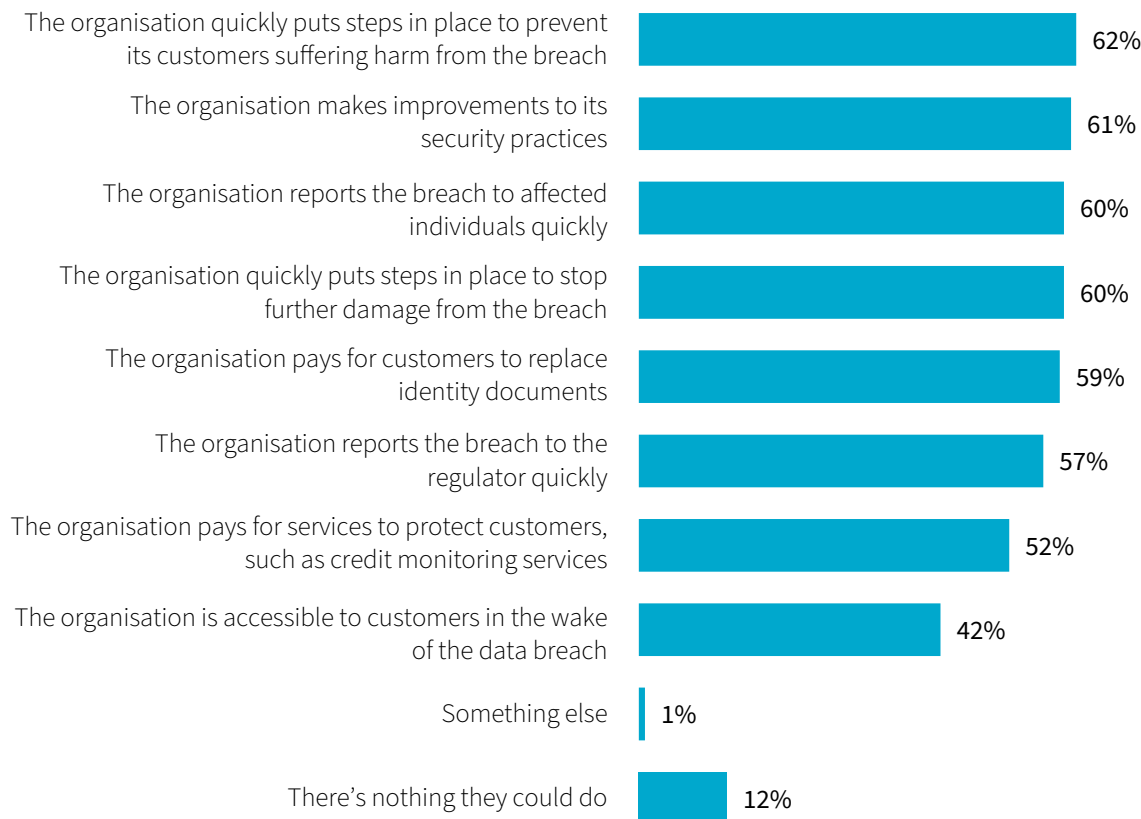
For 12% of Australians, there is nothing an organisation could do that would influence them to stay after a data breach.



### Steps most likely to influence Australians to stay after a data breach

- 1 Steps are quickly put in place to prevent customers suffering harm
- 2 Improvements are made to security practices
- 3 The breach is reported quickly to affected individuals

**Figure 47: Factors that influence people to remain with an organisation after a data breach**



P15. Which of the following factors would influence you to remain with an organisation that suffered a data breach? Select all that apply. Base: Australians 18+ years (n=1,626)

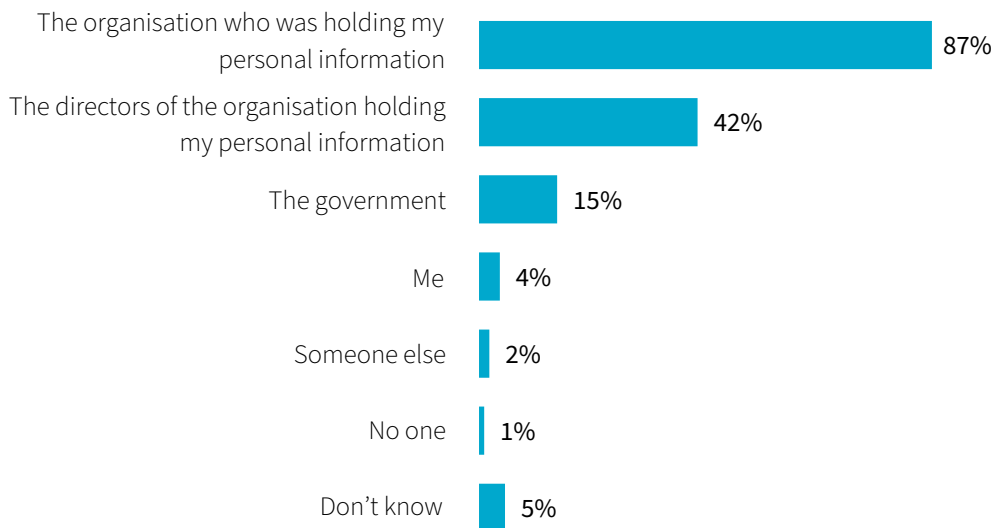
Younger Australians are more open to staying with an organisation that takes steps to address a data breach, with only 8% of those aged 18 to 34 saying there is nothing an organisation can do, compared to 15% of people aged 35 and over.

## Responsibility for data breaches

The majority (87%) of Australians say organisations should be held responsible if they experience a data breach and individuals' information is affected.

Two in five (42%) Australians believe the directors of those organisations should be held accountable – this increases to 47% among males, compared to 37% among females.

**Figure 48: Responsibility for data breaches**



P16. If an organisation that you used was affected by a data breach and your information was affected, who do you think should be held responsible? Select all that apply. Base: Australians 18+ years (n=1,626)

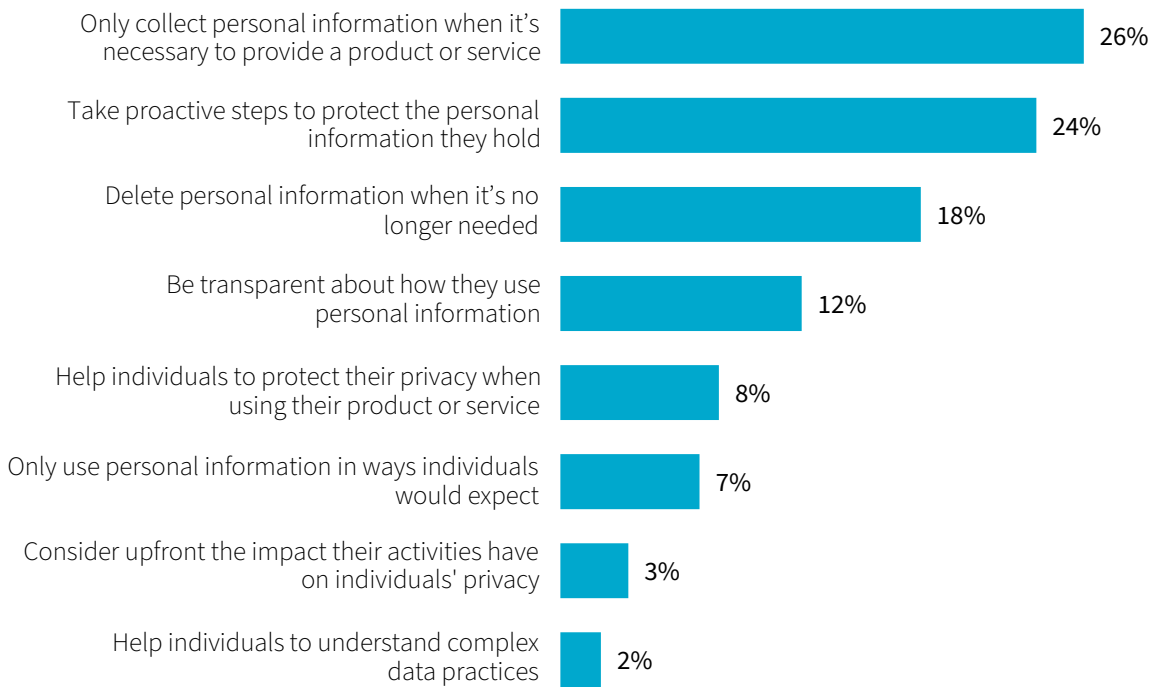
Australians aged 18 to 24 are less likely to hold organisations accountable, with three-quarters (76%) saying the organisation should be held responsible compared to 88% of those aged 25 and over.

The youngest cohort is more likely to think the government should be held accountable (23% 18–24 years, cf. 14% 25+ years), which is in line with their opinion that the [government should be legislating more](#) to protect their privacy.

## Ways for organisations to protect personal information

A quarter (26%) of Australians believe the most important way an organisation can protect their personal information is by only collecting the information necessary to provide the product or service. Australians view the second most important thing organisations can do is take proactive steps to protect the information they hold (24%).

**Figure 49: Most important action organisations should take to protect personal information**



P8. There are many ways an organisation can protect your personal information, which of these do you think is the most important? Select one. Base: Australians 18+ years (n=1,626)



### Top 3 actions organisations can take to protect personal information

- 1 Only **collect** it when it's necessary
- 2 Take proactive steps to **protect** it
- 3 **Delete** it when it's no longer needed



# Part 5

## Digital technologies

## Part 5: Digital technologies

This section of the report covers biometrics, artificial intelligence and targeted advertising.

### Biometric technology

Australians' level of comfort with biometric information being collected and used depends largely on the type of organisation and the context.

Australians are the most comfortable with the collection and use of their biometric information in border security and law enforcement contexts. There is moderate support for its use by the private sector for safety and security reasons.

The main areas of concern for Australians when it comes to uses of their biometric information are targeting and profiling for commercial purposes, or when the information is needed to access non-sensitive services like entertainment.

### Comfort with biometric analysis

The majority of Australians are not comfortable with biometric analysis, which is defined as the use of a wide variety of techniques, such as AI, to make assumptions or predictions about the characteristics of an individual from their biometric data.

Less than half (45%) are 'very' or 'somewhat comfortable' with the use of biometric analysis to determine someone's health or disease status. Australians aged 18 to 34 are the most comfortable with this use of biometric data (56%), compared to 41% for those aged 35 and over.

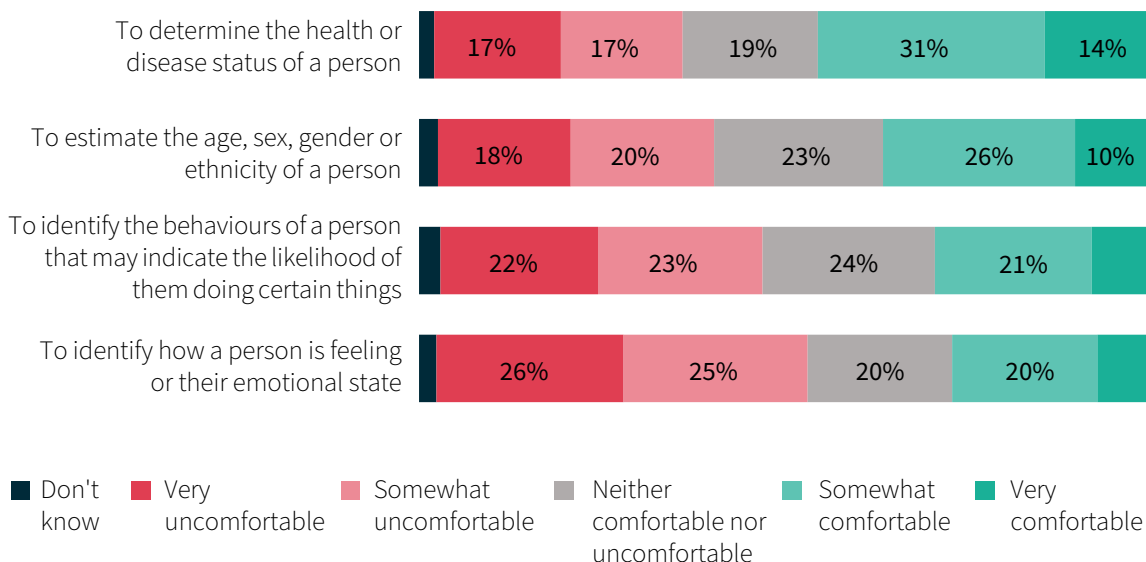
Australians are divided when it comes to using biometric analysis to estimate a person's age, sex, gender or ethnicity (36% 'very' or 'somewhat comfortable', cf. 38% 'very' or 'somewhat uncomfortable').

Three in ten (29%) Australians are comfortable with biometric analysis being used to predict someone's behaviour, while 44% are not comfortable.

The use of biometric analysis to identify how a person is feeling or their emotional state has the highest discomfort score (51% uncomfortable, including 26% 'very uncomfortable').



**Figure 50: Comfort with biometric analysis**



B1. Biometric analysis uses a wide variety of techniques, such as artificial intelligence, to make assumptions or predictions about the characteristics of an individual from their biometric data. How comfortable are you with the use of biometric analysis for the following? Base: Australians 18+ years (n=1,653)

A little more than a third (36%) of Australians aged 18 to 34 are comfortable with biometric analysis being used to predict behaviour, compared to a quarter (26%) of those aged 35 and older.

### Comfort with one-to-one uses of biometric information

A common use of biometric information is to confirm a person is who they say they are by comparing their biometric information to their existing information. Based on an aggregation of the 9 measures tested, half (49%) of Australians are comfortable with this kind of use of their biometric information.

However, comfort levels vary depending on the organisation and reason for verifying their identification.

Two in three (67%) Australians are comfortable with the use of their biometric information in this way to go through passport control at an airport. More than half are comfortable with its use in the contexts of doing their everyday banking (56%), accessing government services (56%), getting on a domestic flight (55%) and using personal devices, such as to unlock a phone or record fitness data (55%).

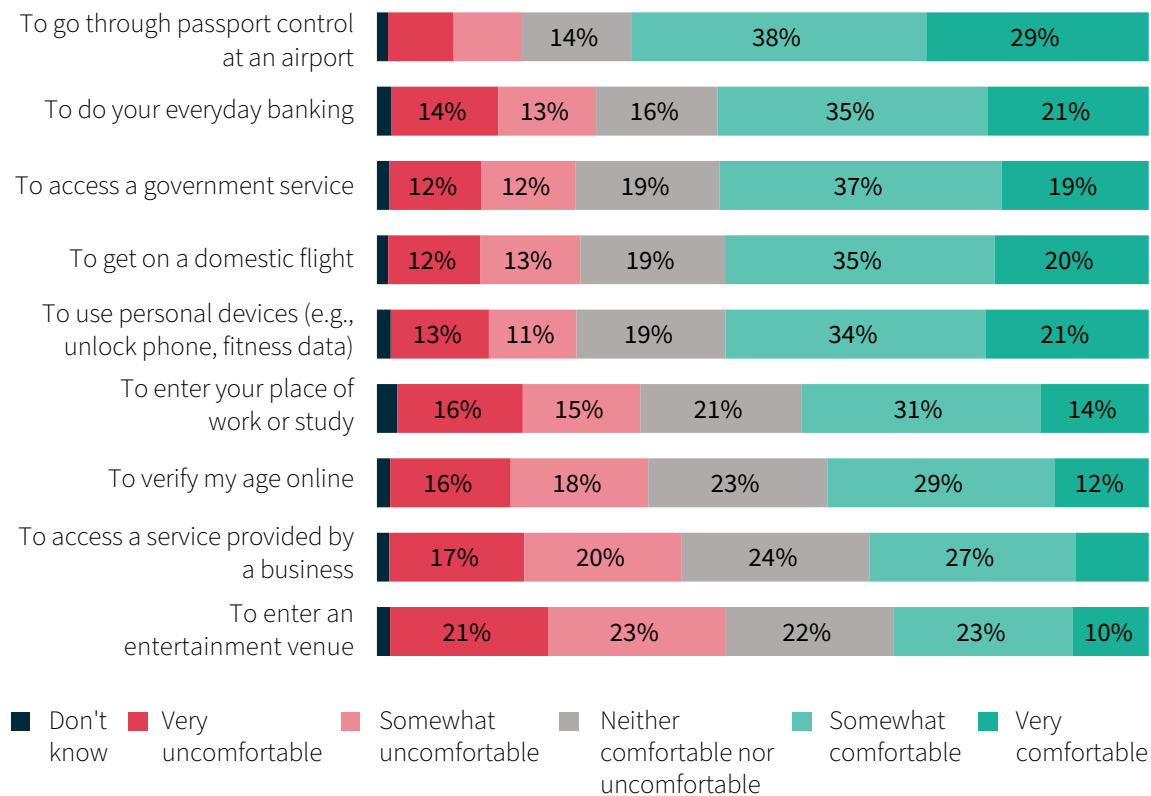


- Digital technologies

Australians are not as comfortable with the use of their biometric information for identity confirmation to access their place of work or study (45%) or verify their age online (42%).

Only a third are comfortable with it being used when they want to access a service provided by a business (36%) or enter an entertainment venue (33%).

**Figure 51: Comfort with one-to-one uses of biometric information**



B2. A common use of biometric information is to confirm you are who you say you are by comparing it to existing information. How comfortable are you with the use of your biometric information to confirm you are who you say you are in the following situations? Base: Australians 18+ years (n=1,653)

- Digital technologies

## Comfort with one-to-many uses of biometric information

Biometric information can also be used to figure out who a person is by comparing their biometric information to large databases containing many people's biometric information. In those circumstances, a person's biometric information may be collected even if they are not the person being identified.

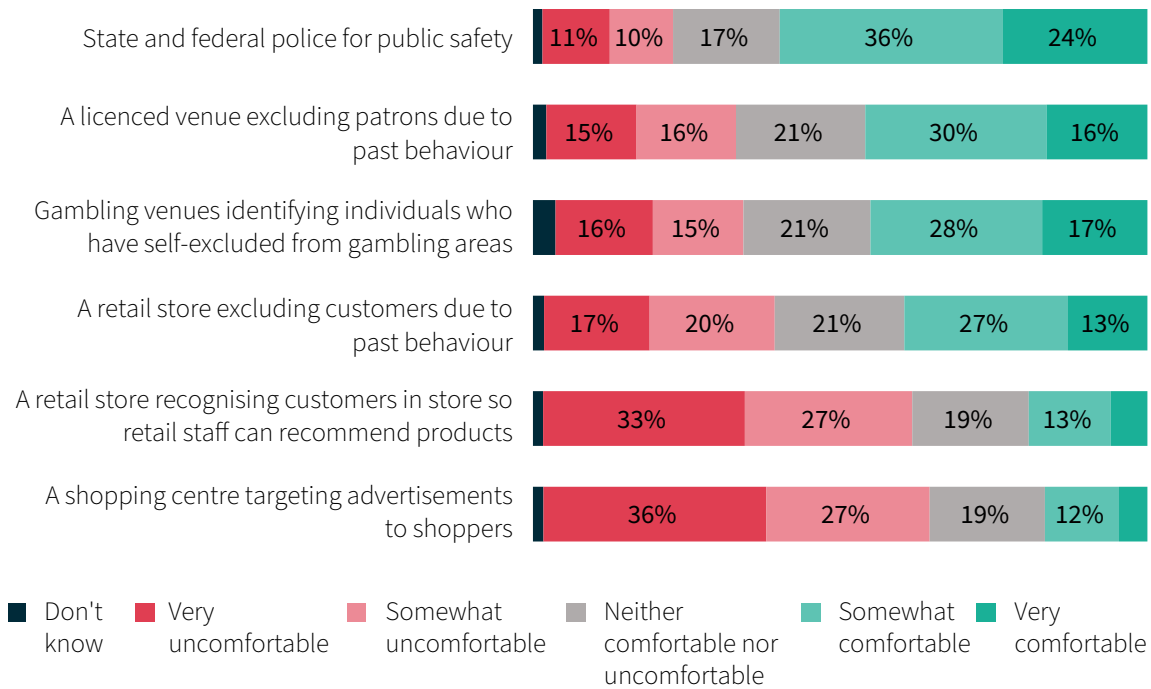
Comfort with this use of biometric information varies significantly depending on the context. There is a reasonable level of comfort with law enforcement using it for public safety, a mixture of opinions around using it to identify people for behavioural-related reasons and discomfort with the commercial use of biometric information in this way.

Australians are most comfortable with their biometric information being used in this way by state and federal police for public safety (60% comfortable, including 24% 'very comfortable'). This has greater support among Australians aged 55 and older than those aged 18 to 54 (66% 55+ years, cf. 56% 18–54 years).

Nearly half of Australians are comfortable with one-to-many uses of their biometric information by a licenced venue to exclude patrons due to past behaviour (46%) and by gambling venues to identify individuals who have self-excluded from gambling areas (45%).

The majority of Australians are uncomfortable with their biometric information being used by shopping centres for targeted advertising (63% uncomfortable, including 36% 'very uncomfortable') and by retail stores to recognise customers in store so staff can recommend products (60% uncomfortable, including 33% 'very uncomfortable').

**Figure 52: Comfort with one-to-many uses of biometric information**



B3. Biometric information can also be used to figure out who a person is by comparing the biometric information to large databases containing many people's biometric information. Often, your biometric information will be collected even if you are not the person being identified. Sometimes this involves collecting the biometric information of everyone who enters a space, such as a venue, and automatically comparing it to the database. How comfortable are you with the use of your biometric information in the following situations? Base: Australians 18+ years (n=1,653)

- Digital technologies

## Trust in organisations' handling of biometric information

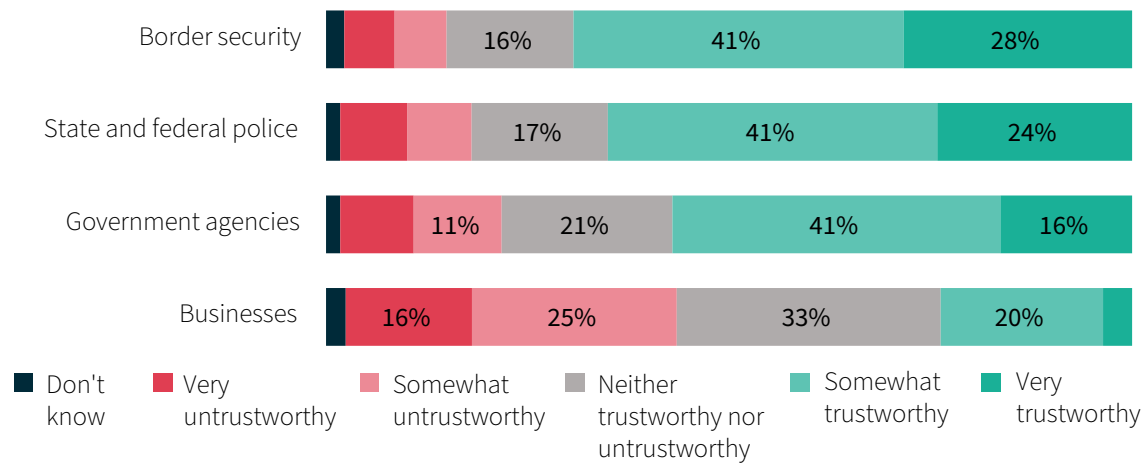
Australians are much more likely to trust the public sector to collect and use biometric information than they are businesses.

Seven in ten (69%) Australians consider border security trustworthy, and two-thirds (65%) consider the state and federal police trustworthy.

More than half (57%) of Australians trust government agencies to collect and use biometric information.

Only a quarter (24%) of Australians say businesses are trustworthy when it comes to the collection and use of biometric information.

**Figure 53: Trust in organisations' handling of biometric information**



B4. In your opinion, how trustworthy are the following to collect and use biometric information? Base: Australians 18+ (n=1,653)

Australians aged 65 and older are more likely to consider border security (80%) and state and federal police (75%) trustworthy than those aged under 65 (67% border security, 63% state and federal police). Females are also more likely to consider border security (72%) and state and federal police (68%) trustworthy than males (67% border security, 62% state and federal police).

Australians aged 65 and older are more likely than those under 65 to say government agencies are trustworthy (66% 65+ years, 55% 18–64 years).

Australians aged 18 to 34 are more likely to consider businesses trustworthy (30%) compared to people aged 35 and over (21%).

## Artificial intelligence

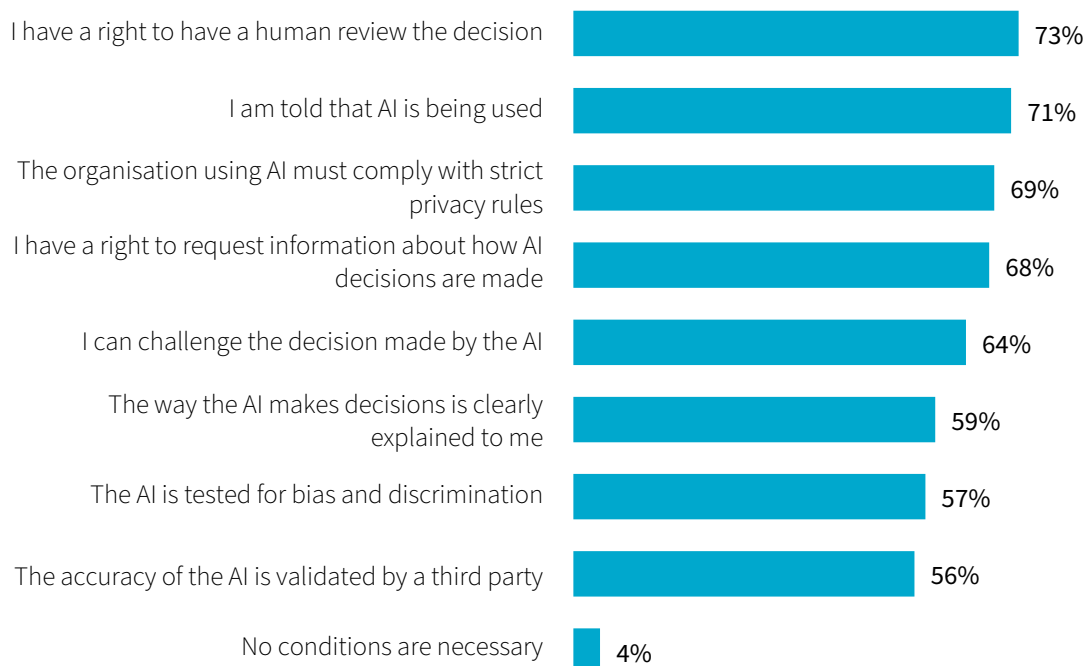
### Conditions for the use of artificial intelligence

Australians are cautious about the use of artificial intelligence (AI) to make decisions that might affect them, with 96% saying there should be some conditions in place before AI is used in this way.

The conditions considered to be most essential before an organisation uses AI are that people have a right to have a human review the decision (73%) and they are told AI is being used (71%).



**Figure 54: Conditions for the use of artificial intelligence**



F11. What conditions do you consider to be essential before an organisation uses artificial intelligence to make a decision that might affect you? Select all that apply. Base: Australians 18+ years (n=1,642)

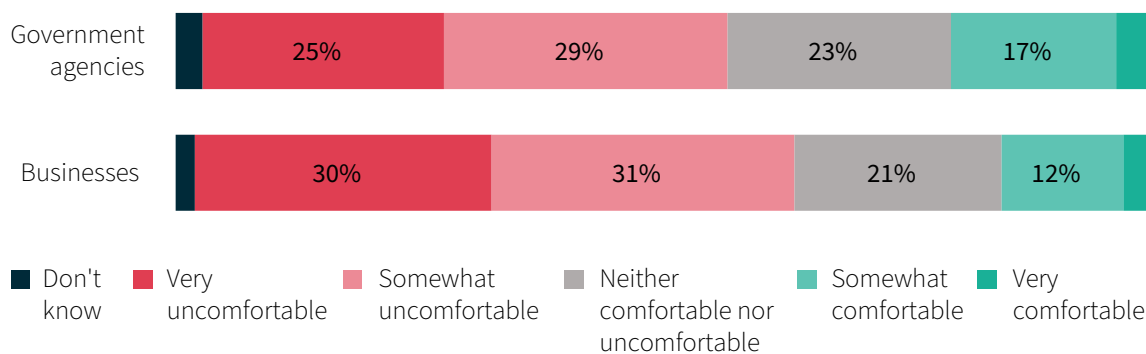
- Digital technologies

Australians aged 55 and over, females and people with annual household incomes under \$40,000 are all more likely to express the need for more conditions to be in place before AI is used in decision-making processes. While there are higher proportions within these demographics that desire a stricter framework, the order of importance of the conditions is in line with the total population.

## Comfort with the use of artificial intelligence

Australians are more comfortable with government agencies using AI that uses their personal information to make decisions about them than they are with businesses. One in five (20%) Australians are ‘very’ or ‘somewhat comfortable’ with government agencies using the technology to make decisions about them compared to 15% for businesses.

**Figure 55: Comfort with the use of artificial intelligence**



F12. How comfortable are you with government agencies using artificial intelligence to make decisions about you, using your personal information?

F13. How comfortable are you with businesses using artificial intelligence to make decisions about you, using your personal information?

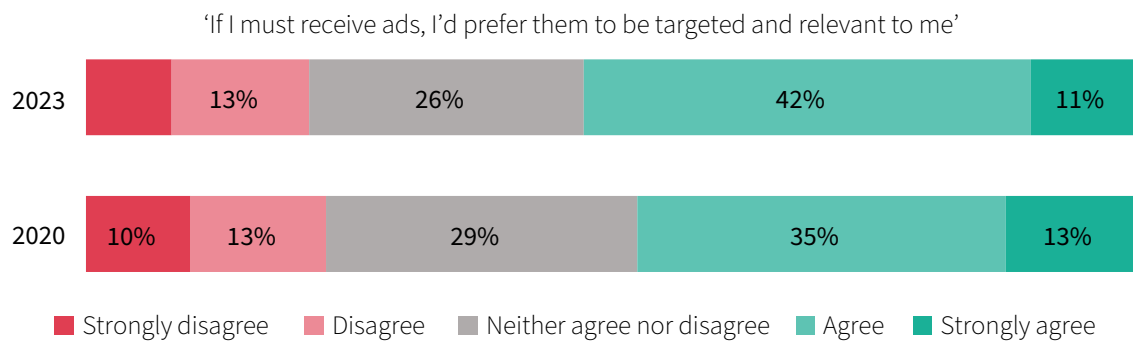
Base: Australians 18+ years (n=1,642)

Similar to the findings around conditions for the use of AI, discomfort with using AI to make decisions based on personal information increases with age and is also more of a concern for females compared to males (‘very’ or ‘somewhat uncomfortable’ with use by government agencies, 48% males, cf. 60% females, 43% 18–34 years, 56% 35–54 years, 62% 55+ years; ‘very’ or ‘somewhat uncomfortable’ with use by businesses, 57% males, cf. 66% females, 49% 18–34 years, 62% 35–54 years, 72% 55+ years).

## Acceptance of targeted advertising

If they must receive ads, just over half (53%) of Australian adults would prefer the ads are targeted and relevant to them. This has increased slightly from 48% in 2020.

**Figure 56: Acceptance of targeted advertising**



G6 (2023) and B6 (2020). Thinking about data privacy, to what extent do you agree or disagree with the following: If I must receive ads, I'd prefer them to be targeted and relevant to me? Base: Australians 18+ years, 2023 (n=1,916), 2020 (n=1,506)

Females are more open to receiving targeted ads than males (56% females, cf. 49% males).



# Part 6

## Children's privacy



## Part 6: Children's privacy

Australian parents and guardians feel strongly about their children's privacy and are very supportive of organisational and technology measures to increase levels of protection. They recognise the importance of privacy for their children, but half do not feel in control of it.

Australian parents' belief that children have the right to grow up without being profiled and targeted has increased since 2020. However, parents' feeling of being in control of their children's data privacy has decreased.

Parents' decisions to provide their children access to connected devices and digital services early in life are affected by privacy concerns. Many are uncomfortable with businesses obtaining, tracking, and using their children's personal information in ways that are not in the best interests of the child.



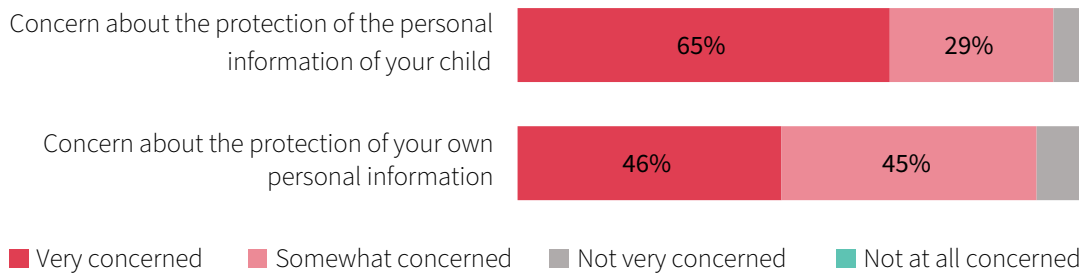
## Concerns for children’s privacy

Parents are slightly more concerned about their children’s privacy (94% concerned) than they are about their own (91%).

However, the strength of their concern is much higher when it comes to their children, with 65% ‘very concerned’ about the protection of their child’s personal information, compared to 46% being ‘very concerned’ about the protection of their own personal information.

The strength of concern has increased since 2020, when 51% of parents said they were ‘very concerned’ about the protection of their child’s personal information and 37% were ‘very concerned’ about the protection of their own personal information.

**Figure 57: Parents’ concerns about the protection of personal information**



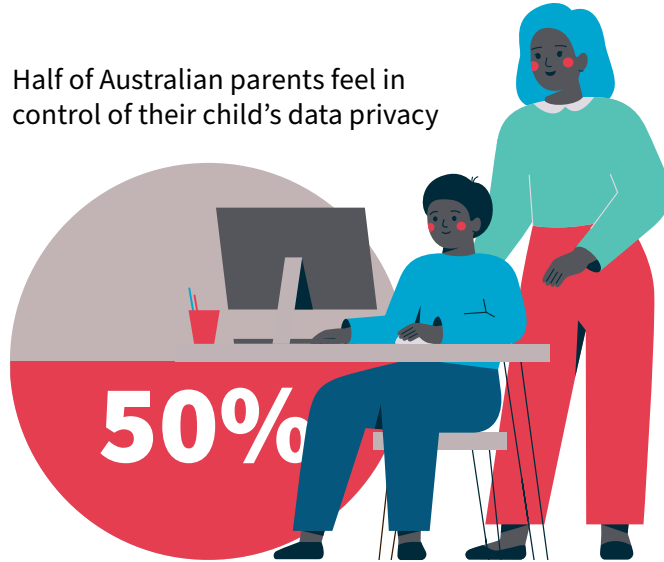
C6. How concerned are you about the protection of the personal information of your child?  
 C5. How concerned are you about the protection of your own personal information?  
 Base: Australian parents and guardians of children aged 2–17 years (n=679)

Female parents are significantly more likely than male parents to be ‘very concerned’ about the privacy of their child (72% females, cf. 59% males), with a smaller difference when it comes to how they view their own protection (49% females, cf. 43% males).

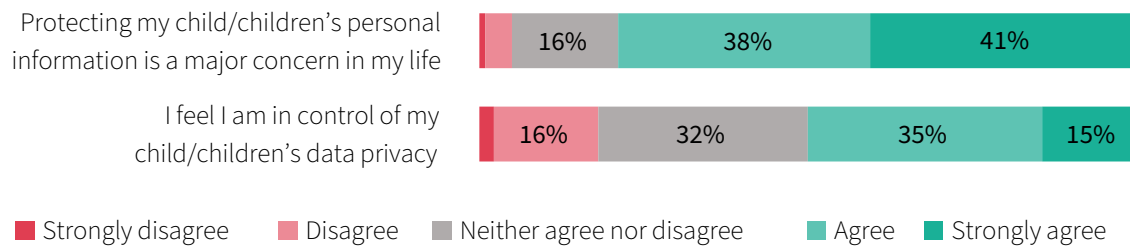
## Concern and control over children’s privacy

Protecting their child’s personal information is a major concern for 4 in 5 (79%) parents. However, only half (50%) feel they are in control of their child’s data privacy and nearly 1 in 5 (18%) do not think they have control. Feelings of control are similar across ages and gender of children and have decreased by 12 percentage points since 2020.

Half of Australian parents feel in control of their child’s data privacy



**Figure 58: Parents’ concern and control over their child’s data privacy**



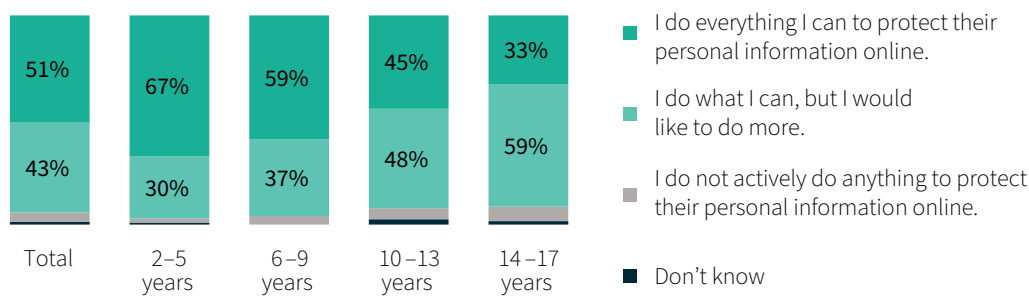
C13. Thinking about children’s data privacy, to what extent do you agree or disagree with each of the following statements? Base: Australian parents and guardians of children aged 2–17 years (n=679)

The older the child, the less likely parents are to feel in control of their child’s privacy. Fifty-nine per cent of parents of children aged 2 to 5 feel in control of their child’s privacy, compared to 58% of parents of children aged 6 to 9, 48% of parents of children aged 10 to 13 and 37% of parents of children aged 14 to 17.

## Parents’ actions to protect their children’s privacy online

Half of parents (51%) believe they are doing everything they can to protect their child’s personal information online, while around 2 in 5 (43%) say they do what they can, but would like to do more.

**Figure 59: Parents’ actions to protect their children’s privacy online, by child’s age**



C7. Thinking about protecting your child’s personal information online, which of the following best applies to you? Select one. Base: Australian parents and guardians of children 2–5 years (n=200), 6–9 years (n=140), 10–13 years (n=149), 14–17 years (n=190)

Only 4% of parents do not actively do anything to protect their child’s personal information online. This is 8 percentage points lower than in 2020 and supports the growing concern about children’s privacy. Driving the increase are parents of children aged 2 to 5 (67%), with a 16 point increase since 2020.

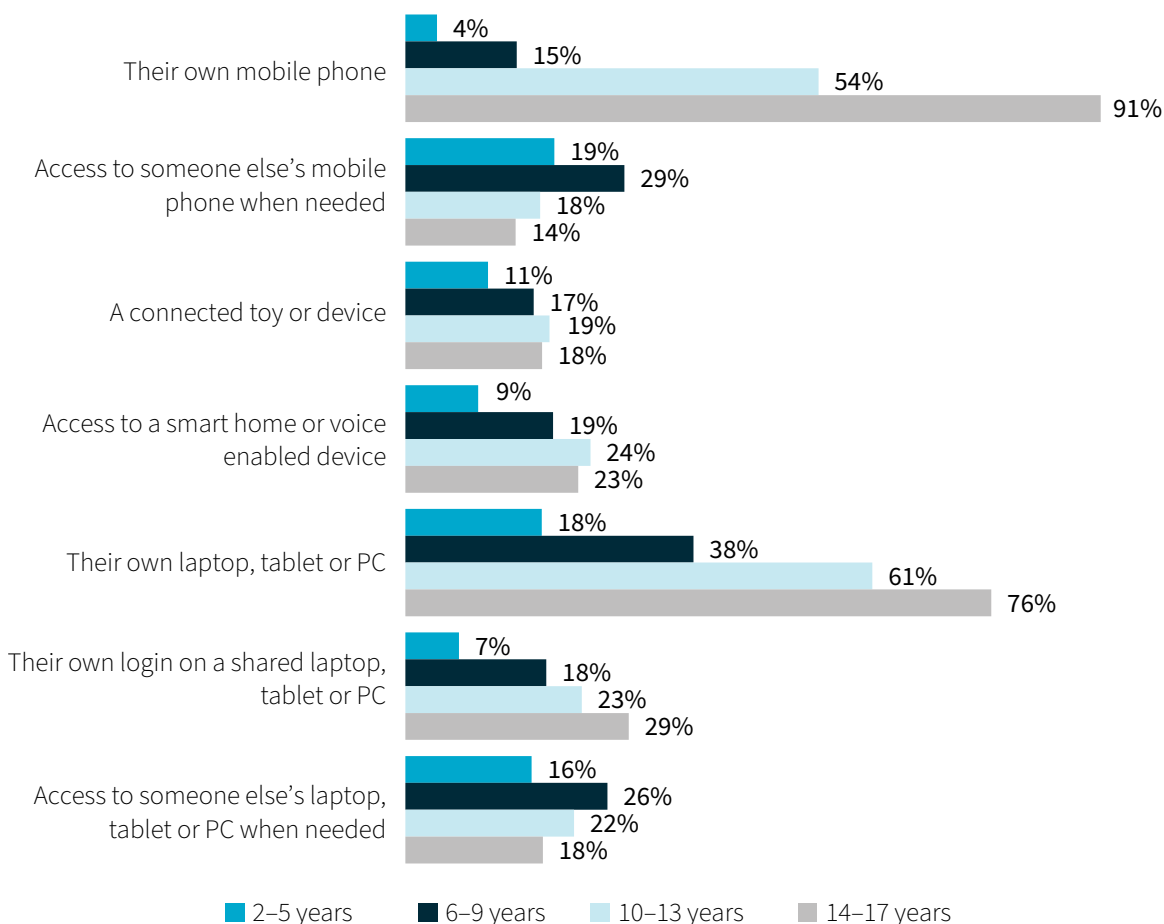
## Children’s access to and ownership of devices

Two-thirds (65%) of children aged 2 to 17 have access to a laptop, tablet or PC whether it be their own device (47%), their own login to a shared device (19%) or access to someone else’s device when needed (20%). More than a third (36%) of children aged 2 to 5 have access to a laptop, tablet or PC.

Access to a mobile phone is less common (55%), however more than half (54%) of children aged 10 to 13 have their own mobile phone. This increases to 91% among children aged 14 to 17, compared to 15% for those aged 6 to 9 and 4% for children aged 2 to 5.

Access to smart home or voice-enabled devices (such as Google Home or Amazon Alexa) and connected toys or devices (such as fitness trackers or robotic toys) is less common again. The percentage of children who have a connected toy or device is down 14 points since 2020 among those aged 6 to 9 and 4 points overall.

**Figure 60: Children’s access to and ownership of devices**



C3. To your knowledge, which of the following do they currently have? Base: Australian parents and guardians of children 2–5 years (n=200), 6–9 years (n=140), 10–13 years (n=149), 14–17 years (n=190)

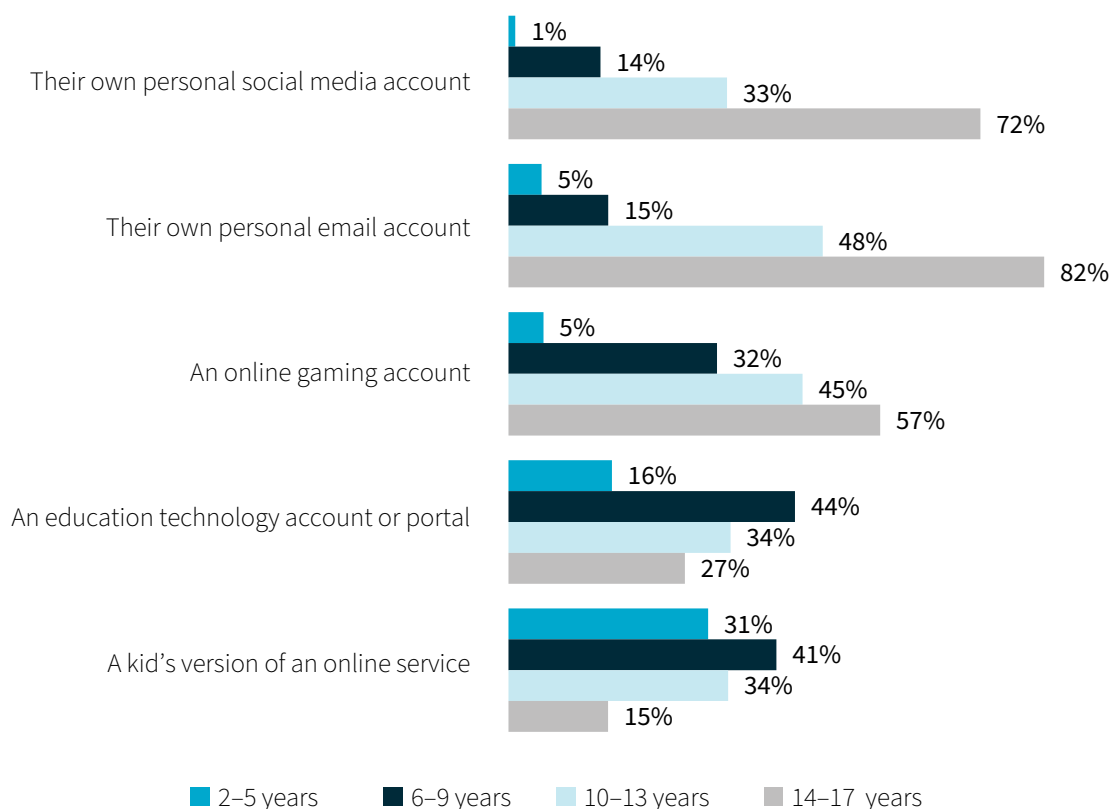
## Children’s use of online accounts and services

A child’s version of an online service and educational technology (edtech) accounts or portals are the most common accounts for children aged 2 to 5 and 6 to 9. At 10 to 13 years, popularity shifts to having their own email and online gaming accounts. By 14 to 17 years, social media accounts, such as Instagram and TikTok, surpass online gaming, while edtech and a kid’s version of an online service continue to decrease.

One in seven (14%) children aged 6 to 9 have their own social media account. This more than doubles among children aged 10 to 13 (33%) and more than doubles again among children aged 14 to 17 (72%).

Among children aged 14 to 17, online gaming accounts have increased by 23 percentage points since 2020. While overall male children (39%) are more likely to have a gaming account than female children (28%), female children have seen a greater increase since 2020 (up 11 points).
















**Figure 61: Children’s use of online accounts and services**



C3. To your knowledge, which of the following do they currently have? Base: Australian parents and guardians of children 2–5 years (n=200), 6–9 years (n=140), 10–13 years (n=149), 14–17 years (n=190)

- Children’s privacy

### Technology adoption by age

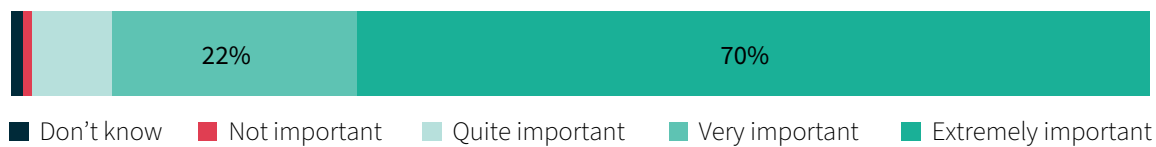
	9 years	10 years	11 years	12 years	13 years	14 years	15 years	16 years
Their own laptop, tablet or PC								
An online gaming account								
Their own personal email account								
Their own mobile phone								
Their own personal social media account								

<25% adoption	>25% adoption	>50% adoption	>75% adoption
---------------	---------------	---------------	---------------

## Importance of children’s privacy when choosing services

The privacy of their child’s personal information is of high importance to 91% (70% ‘extremely important’ and 22% ‘very important’) of parents when deciding to provide their child with access to digital devices and services. This level of importance is consistent across age groups and genders.

**Figure 62: Importance of children’s privacy when choosing services**



C4. How important is the privacy of your child’s personal information when you are deciding what access to digital devices and services you do or do not allow your child? Base: Australian parents and guardians of children aged 2–17 years (n=679)

## Appropriate ages for children to learn about privacy and provide consent

A third (32%) of parents believe children should start learning about data privacy and the protection of their personal information between ages 4 and 6, with 3 in 5 (59%) parents saying learning should begin before the age of 10. Despite the level of concern around privacy, this is a decrease from 2020 when 70% of parents thought children should be learning about privacy before they reach age 10.

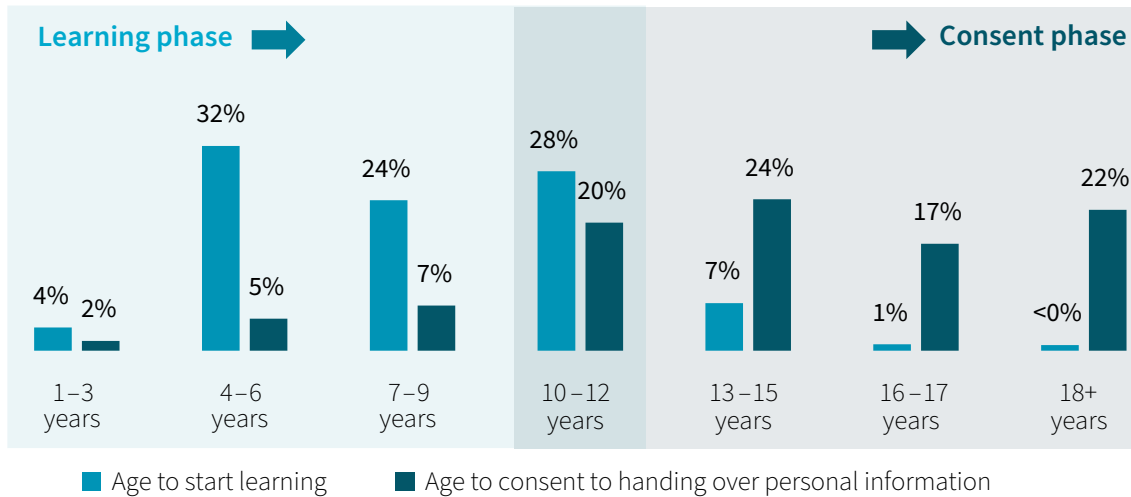
Parents’ views of the most appropriate age for children to start learning about privacy differ depending on the age of their child. On average, parents of children aged under 10 believe children should start to learn about privacy 2 years younger than parents of children aged 10 and older (average 7.3 years for parents of a child <10 years, cf. average 9.1 for 10+ years).

Parents believe the average age for children to start consenting to handing over their personal information to use an online service is 13 years 8 months. More than 1 in 5 (22%) believe children should be 18 or older before it is appropriate for them to consent to this.

Again, the views of parents change depending on the age of their child, with parents of children aged 14 to 17 believing the average age for children to start providing consent is 2 years older than parents of children aged 2 to 5 (average 14.8 for parents of a child 14–17 years, cf. average 12.8 for 2–5 years, average 13.4 for 6–9 years, average 14 for 10–13 years).



**Figure 63: Appropriate ages for children to start learning about data privacy and provide consent**



C10. Thinking about children in general, what age do you think it 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 children to consent to handing over their personal information in exchange for an online service, such as social media or online gaming?

Base: Australian parents and guardians of children aged 2–17 years (n=679)

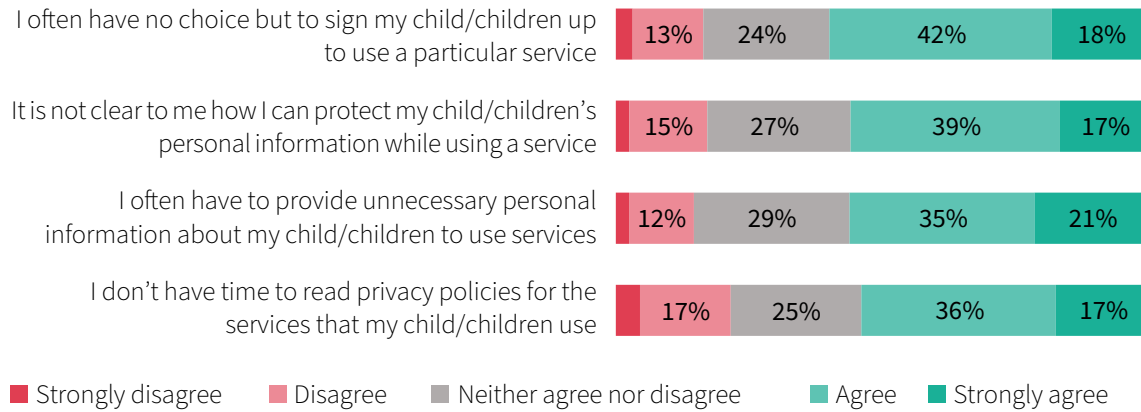
## Beliefs about accessing children’s services

Most parents express helplessness and confusion when it comes to accessing services for their child, with 3 in 5 (60%) saying they often have no choice but to sign their child up to use a particular service. More than half have had to provide unnecessary information about their child to use services (56%) and are not clear how they can protect their child’s information when using a service (56%).

Time is also a factor for parents, with 54% saying they do not have the time to read privacy policies for the services their child uses.

- Children’s privacy

**Figure 64: Parents’ beliefs about accessing children’s services**

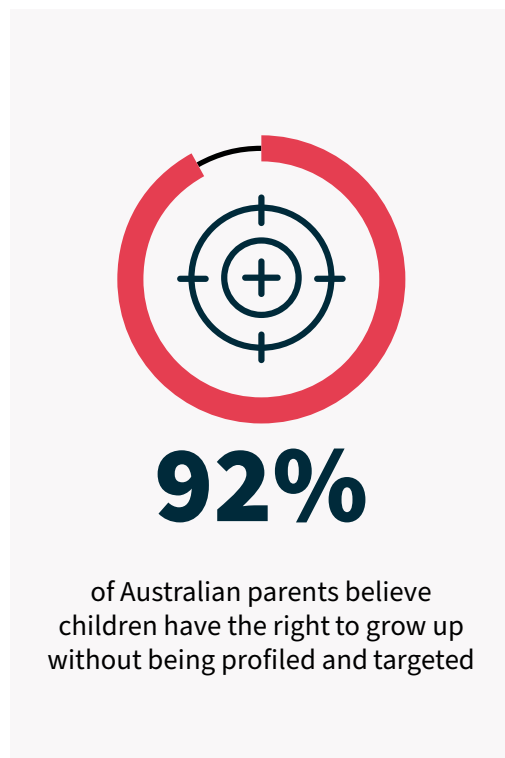


C13. Thinking about children’s data privacy, to what extent do you agree or disagree with each of the following statements? Base: Australian parents and guardians of children aged 2–17 years (n=679)

Beliefs of lacking choice and having to provide unnecessary information about their child to use a service peak among parents of children aged 14 to 17 (66% no choice, 64% provide unnecessary information).

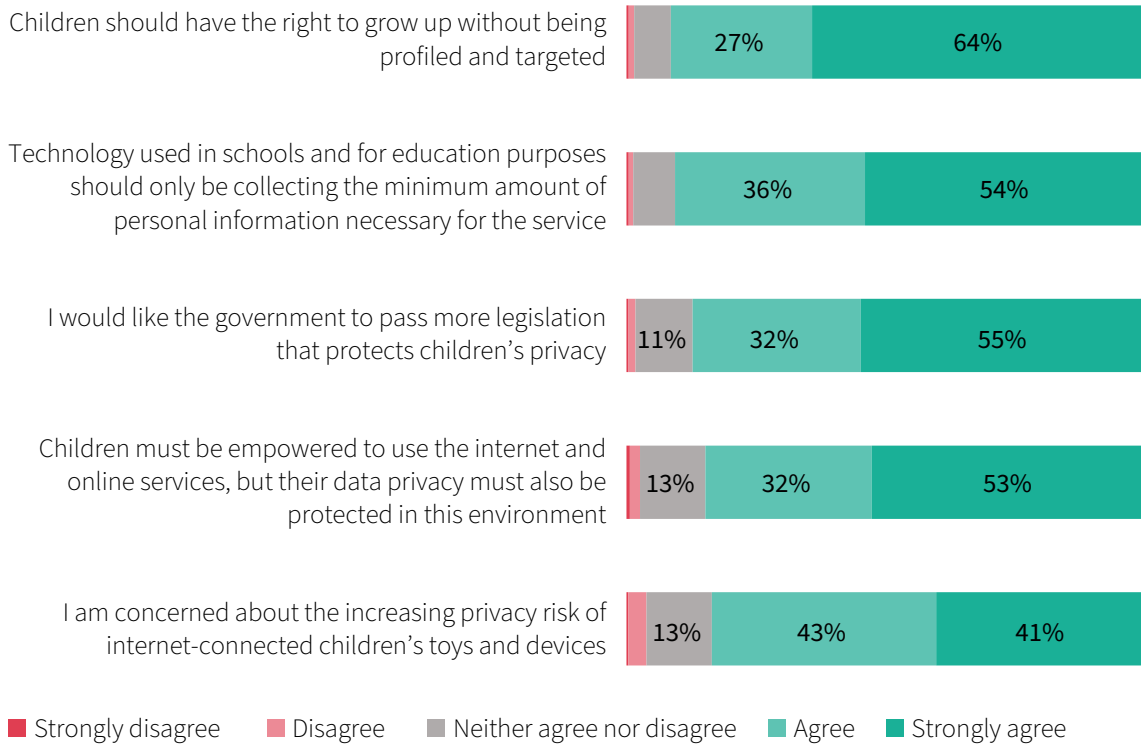
## Beliefs about children’s privacy

Nine in ten (92%) parents believe children should have the right to grow up without being profiled and targeted, which is an increase of 7 percentage points since 2020. This may be a factor in why 87% of parents would like the government to pass more legislation that protects children’s privacy and why 85% of parents say children must be empowered to use the internet and online services, but their data privacy must be protected.



- Children’s privacy

**Figure 65: Parents’ beliefs about 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 and guardians of children aged 2–17 years (n=679)

Most (91%) parents believe technology used in schools and for education purposes should only collect the minimum amount of personal information necessary for the service. This peaks among parents of children aged 14 to 17 (96%), compared to parents of children aged 2 to 5 (87%), aged 6 to 9 (91%) and aged 10 to 13 (88%).

Most (84%) parents are also concerned about the increasing privacy risk of internet-connected children’s toys and devices. This has increased by 12 percentage points since 2020 and may explain the 4 point decrease in [children’s ownership of connected toys or devices](#) over the same period.

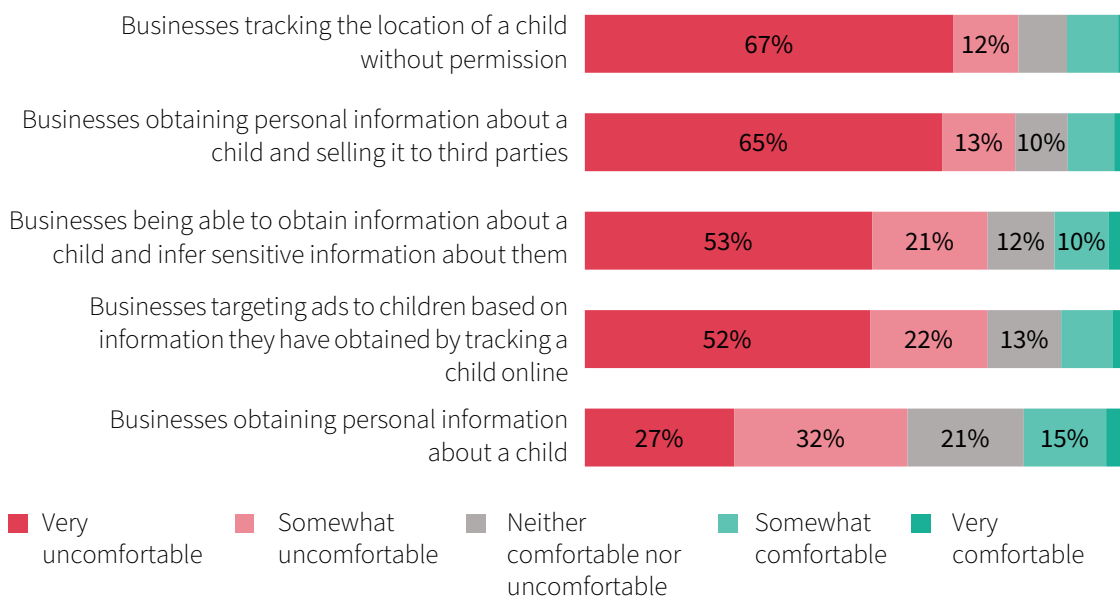
## Comfort with businesses using children’s personal information

Three in five (59%) parents are uncomfortable with businesses obtaining personal information about a child. How the business uses this information has a strong effect on the level of discomfort, with 79% of parents uncomfortable with businesses obtaining personal information about a child and selling it to third parties. A similar proportion (79%) of parents are uncomfortable with businesses tracking the location of a child without permission.

Three-quarters (74%) 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).

Similarly, three-quarters (74%) of parents are uncomfortable with businesses targeting ads to children based on information they have obtained by tracking a child online.

**Figure 66: Parents’ comfort with businesses using children’s personal information**



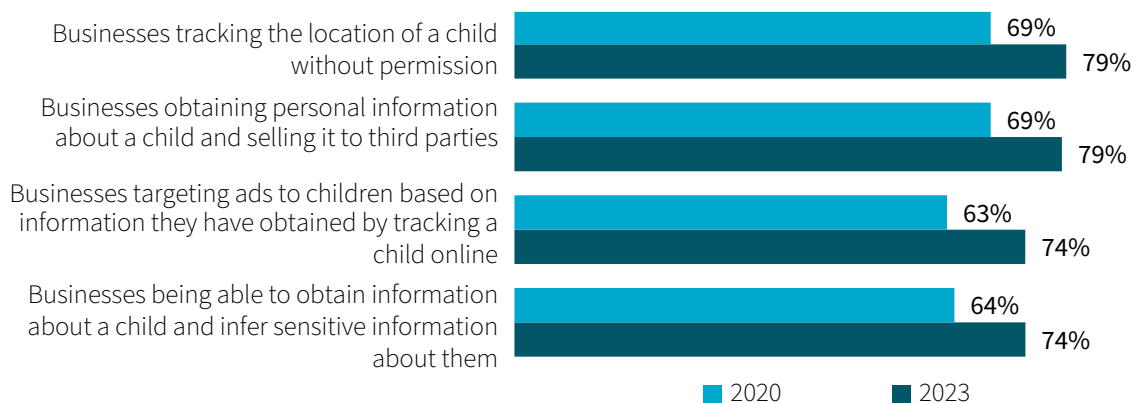
C14. Still thinking of children’s data privacy. How comfortable are you with each of the following? Base: Australian parents and guardians of children aged 2–17 years (n=679)

- Children’s privacy

This is highest among parents of children aged 14 to 17 (78%) and lowest for parents of children aged 6 to 9 (69%), compared to 71% of parents of children aged 2 to 5 and 77% of parents of children aged 10 to 13.

The discomfort around several measures has increased significantly since 2020: discomfort with obtaining information and inferring sensitive information about children (up 11 points); discomfort with location tracking (up 10 points); selling personal information to third parties (up 10 points) and businesses targeting ads to children (up 9 percentage points).

**Figure 67: Change in parents’ discomfort with businesses using children’s personal information**



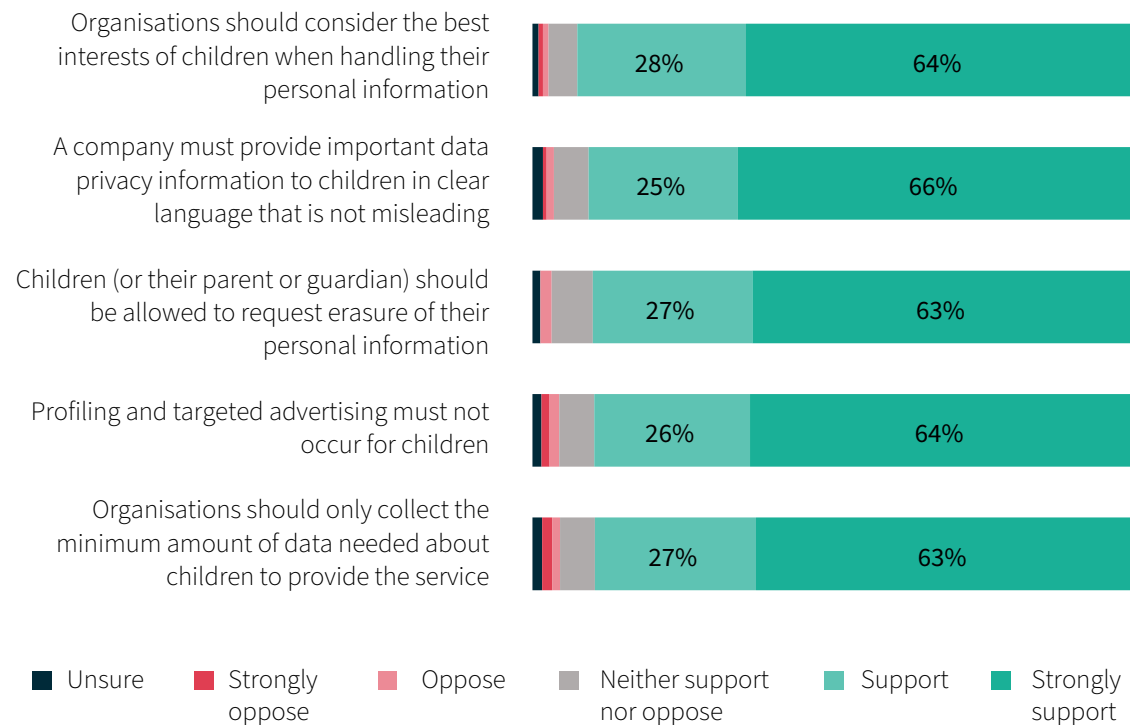
C14. Still thinking of children’s data privacy. How comfortable are you with each of the following? ‘Somewhat uncomfortable’ and ‘very uncomfortable’. Base: Australian parents and guardians of children aged 2–17 years, 2020 (n=789), 2023 (n=679)

## Organisational measures to increase children’s privacy

The majority of parents strongly support organisations adopting a child-centric approach to handling personal information about children.

This includes organisations considering what is in the best interests of children when handling their personal information (93% support, including 64% ‘strongly support’), providing important data privacy information to children in clear language that is not misleading (91% support, including 66% ‘strongly support’) and only collecting the minimum amount of data needed about children to provide the service (90% support, including 63% ‘strongly support’).

**Figure 68: Organisational 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 and guardians of children aged 2–17 years (n=679)

Mirroring parents’ belief that children have the right to grow up without being profiled or targeted, 9 in 10 (90%) parents also support measures to stop profiling and targeted advertising to children. This is supported by more parents of children aged 2 to 5 (92%), compared to parents of children aged 6 to 9 (88%), 10 to 13 (87%) and 14 to 17 (90%), and has increased by 7 percentage points since 2020.

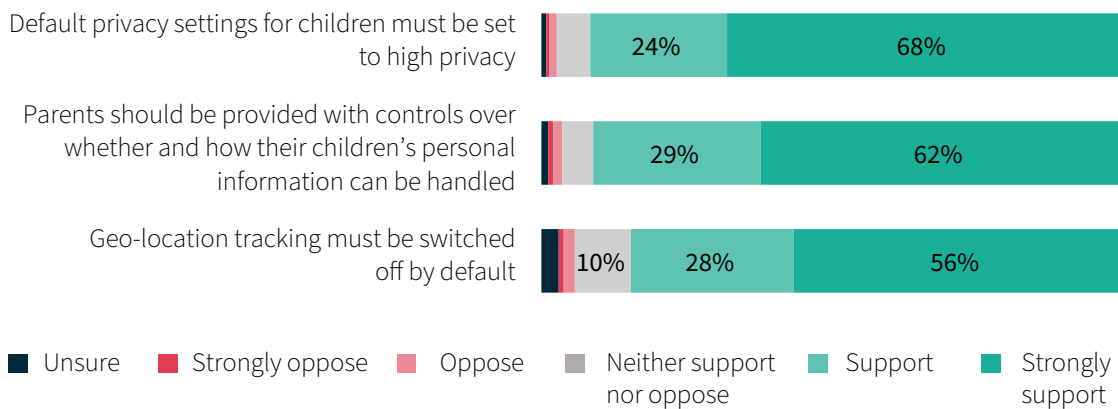
## Technology measures to increase children’s privacy

Parents strongly support technology measures to increase the online privacy of children, with 92% supporting (including 68% who ‘strongly support’) default privacy settings for children being set to high and 85% supporting (including 56% who ‘strongly support’) geo-location tracking being turned off by default for children.

Support for geo-location tracking being switched off peaks in parents of children aged 2 to 5 (87%), compared to parents of children aged 6 to 9 (83%), 10 to 13 (84%) and 14 to 17 (83%), and has increased by 13 percentage points since 2020.

Nine in ten (91%) parents support (including 62% ‘strongly support’) being provided with controls over whether and how their child’s personal information can be handled.

**Figure 69: Technology 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 and guardians of children aged 2–17 years (n=679)

## Responsibility for the protection of children's information

Parents consider responsibility for protecting their child's personal information does not lie with a single entity.

Four out of five (81%) parents say they should be responsible for protecting their child's personal information. This is consistent across all ages, but is slightly stronger among parents of female children (85%) compared to parents of male children (79%).

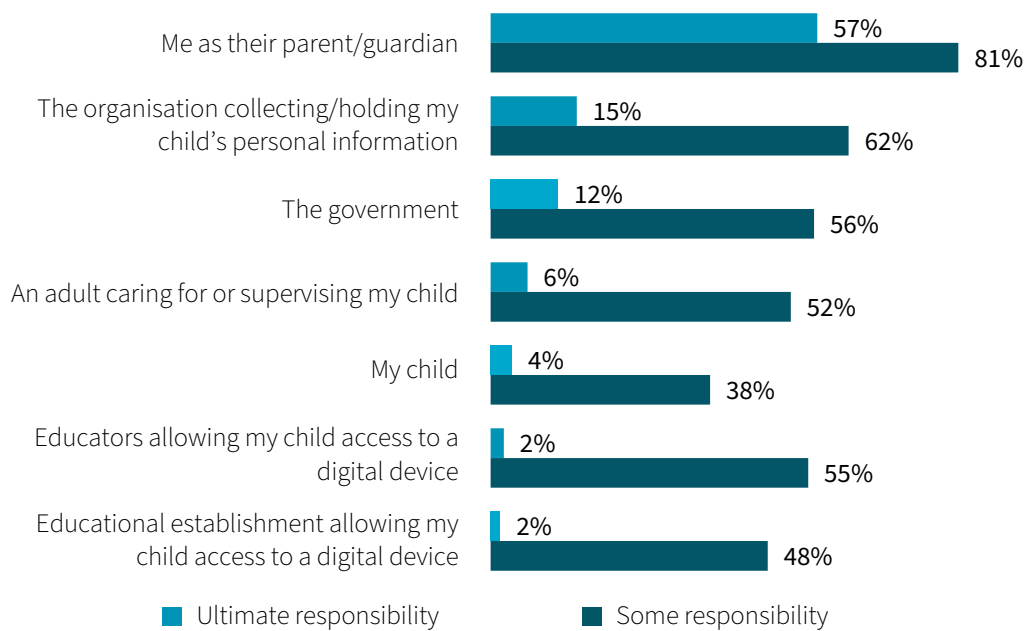
More than half (56%) of parents say the government has some responsibility for the protection of their child's personal information. This is driven by parents of female children (63%) compared to parents of male children (50%).

Two in five (38%) parents say their child has some responsibility for protecting their information. This increases with the age of the child – 20% for parents of children aged 2 to 5, 31% for parents of children aged 6 to 9, 41% for parents of children aged 10 to 13 and 62% for parents of children aged 14 to 17.

More than half (57%) of parents believe they bear ultimate responsibility for protecting their child's personal information.



**Figure 70: Responsibility for the protection of children’s personal information**



C8. Who do you think should be responsible for protecting your child’s personal information? Select all that apply. Base: Australian parents and guardians of children aged 2–17 years (n=679)  
 C9. And of these, who do you think should be ultimately responsible for protecting your child’s personal information? Select one. Base: Australian parents and guardians of children aged 2–17 years, excluding those who responded ‘Don’t know’ in C8 (n=670)

There is no significant difference in where ultimate responsibility is placed as the child grows. The age or gender of the parent also does not have any notable impact.



# Methodology

# Methodology

## Overview

ACAPS 2023 is the sixth survey in a series initiated in 2001. The methodology has evolved over the past 2 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 and CATI methodology, where 800 surveys were conducted via CATI and 1,000 were completed online, with respondents reached via an online research panel. In 2020, all data was collected online, with 39% of respondents recruited via telephone. In 2023, all data was again collected online, with all respondents reached via an online research panel.

## Questionnaire development

The questionnaire was jointly developed by Lonergan Research and the OAIC.

Comprehensive cognitive and pilot testing was undertaken to evaluate the questionnaire from a respondent perspective and ensure the questions were clear, unambiguous and interpreted in the manner intended.

## Questionnaire length, sample size and modularisation

The total length of the 2023 survey was 30 minutes, which is 10 minutes shorter than in 2020. Despite the decrease in total survey time, the number of questions increased from 76 in 2020 to 86 in 2023.

The increased efficiency in the data collection was possibly due to an adaptation of 2020's modular approach, which allowed more respondents to answer all questions, while reducing overall fatigue.

Each respondent was invited to answer an initial round of questions that determined their demographic profile and general awareness of and attitudes to privacy matters. They were also asked to complete a single module from a selection of 4. If the respondent indicated they were a parent with a child aged 2 to 17, they were asked to complete the module on children's privacy. Otherwise, they were randomly assigned to complete 1 of the other 3 modules. The average length of first round interviews was 13 minutes.

Once a respondent had completed a first round of questions, they were then asked to complete the remainder of the modules on a second round. In order to ensure a high response rate on the second round, an additional incentive payment was offered to returning respondents.

This led to a second-round completion rate of 82%, with an average length of interview of 12 minutes. Due to the linking of respondent information between the 2 rounds, the demographic and general awareness information was not required to be asked on the second round.

The goal in 2023 was to replicate the 2020 sample size of n=1,500 per module (with the exception of the children’s privacy module). The initial approach was to achieve n=1,900 completed surveys of Australians aged 18 or older to reach the per module target, based off the recontact rate seen in the pilot launch data. The recontact rate was slightly higher than anticipated, which resulted in a marginally larger sample count at the close of fieldwork.

Quotas were applied on the recruitment of the first round of respondents to be representative of the general population of adults in Australia. The proportion of parents that completed this first round was a natural fall-out from the nationally representative sample and accounted for 36% of respondents.

Module	Total respondents
Demographic information	n=1,916
General awareness	n=1,916
Fair and reasonable	n=1,642
Privacy breaches	n=1,626
Legal considerations	n=1,653
Biometrics	n=1,653
Children’s privacy	n=679

Legal considerations and biometrics were combined for modularisation purposes.

## Weighting

Due to differences in the total number of respondents per module, each module was individually weighted to be representative of the general population of adults in Australia, with the exception of the children’s privacy module, which was left as a natural fall-out of the weighted round one survey.

## Fieldwork

The survey fieldwork started on 18 March 2023 and was completed on 28 March 2023. The recruitment and hosting of the survey were carried out by one of Lonergan Research’s panel provider companies, with all data hosted on Australian servers.



## Glossary and shortened forms

### Glossary

Term	Definition
<b>Artificial intelligence (AI)</b>	<p>Artificial intelligence was explained to respondents as follows:</p> <p>‘Many organisations are now using artificial intelligence or automated decision-making processes, which may rely on your personal information, to make decisions about you. For example, to help with:</p> <ul style="list-style-type: none"> <li>• diagnosing illnesses</li> <li>• generating your credit score</li> <li>• making hiring decisions for employers and recruitment organisations.’</li> </ul>
<b>Biometrics</b>	<p>Biometrics were explained to respondents as follows:</p> <p>‘The next section is about biometrics, which is biological and behavioural information about you. This includes things like:</p> <ul style="list-style-type: none"> <li>• your fingerprints</li> <li>• your facial image</li> <li>• your voiceprint</li> <li>• scans of your iris or retina</li> <li>• your DNA</li> <li>• the way you walk, your keystroke patterns or other physical characteristics that could be used to identify you.’</li> </ul>
<b>Biometric analysis</b>	<p>The use of a wide variety of techniques, such as AI, to make assumptions or predictions about the characteristics of an individual from their biometric data.</p>
<b>Data breach</b>	<p>A data breach was defined to respondents as follows:</p> <p>‘A data breach is when personal information held by an organisation is accessed or disclosed without authorisation, or is lost.</p> <p>Data breaches may result from malicious action (e.g. cyber criminals), human error (e.g. personal information being emailed to the wrong person) or errors in business or technology processes.’</p>

Term	Definition
<b>Organisations</b>	Organisations is used in the survey and report as an umbrella term for private and public entities. The terms ‘businesses’ and ‘government agencies’ are used to distinguish these organisation types.
<b>Parents</b>	Parents is used to refer to both parents and guardians. The children’s privacy module was asked of parents and guardians of children aged 2 to 17.
<b>Personal information</b>	<p>Personal information was defined to respondents as follows:</p> <p>‘In Australia, privacy law relates to the protection of an individual’s ‘personal information’. This is any information about you that identifies you or could reasonably be used to identify you. This includes things like:</p> <ul style="list-style-type: none"> <li>• your name or address</li> <li>• your date of birth</li> <li>• your financial details</li> <li>• photos or videos of you</li> <li>• your opinions and beliefs</li> <li>• your membership of groups and affiliations</li> <li>• your racial or ethnic origin</li> <li>• your health information</li> <li>• your biometrics (e.g. your facial image, DNA, fingerprints)</li> <li>• your sexual preferences</li> <li>• your criminal record.’</li> </ul>
<b>Privacy breach</b>	The term ‘privacy breach’ is used to refer to a wide range of problems experienced with the handling of personal information. It is distinct from ‘data breach’.

## Shortened forms

Shortened form	Expanded term
<b>ACAPS</b>	Australian Community Attitudes to Privacy Survey
<b>AI</b>	Artificial intelligence
<b>cf.</b>	Statistics in this report are regularly compared across demographic groups. Within brackets, 'cf.' is used to introduce the comparison.
<b>e.g.</b>	For example
<b>OAIC</b>	Office of the Australian Information Commissioner
<b>Privacy Act</b>	<i>Privacy Act 1988</i> (Cth)



## List of figures

<a href="#">Figure 1: What privacy means to Australians</a> .....	11
<a href="#">Figure 2: The most important aspects of privacy</a> .....	13
<a href="#">Figure 3: Beliefs about protecting personal information</a> .....	14
<a href="#">Figure 4: Percentage that understand how to protect personal information by gender and age</a> .....	14
<a href="#">Figure 5: Concern about protecting personal information</a> .....	14
<a href="#">Figure 6: Beliefs around control over personal information</a> .....	15
<a href="#">Figure 7: Self-rated knowledge of data protection and privacy rights</a> .....	16
<a href="#">Figure 8: Self-rated and tested knowledge of privacy rights by gender and age</a> .....	17
<a href="#">Figure 9: Actions Australians always or often take out of concern for their data privacy</a> .....	18
<a href="#">Figure 10: Perceived privacy risks</a> .....	19
<a href="#">Figure 11: Importance of privacy when choosing a product or service</a> .....	21
<a href="#">Figure 12: Influences of privacy practices on choosing products and services</a> .....	21
<a href="#">Figure 13: Influences of privacy practices by age group</a> .....	22
<a href="#">Figure 14: Important factors when choosing a product or service</a> .....	23
<a href="#">Figure 15: Awareness of the Privacy Act</a> .....	25
<a href="#">Figure 16: Awareness of the Privacy Commissioner (OAIC)</a> .....	26
<a href="#">Figure 17: Awareness of organisation types covered by the Privacy Act</a> .....	27
<a href="#">Figure 18: Belief that organisation types should be covered by the Privacy Act</a> .....	28
<a href="#">Figure 19: Extent Australians can access and use data</a> .....	29
<a href="#">Figure 20: Access to personal information held by organisations</a> .....	29
<a href="#">Figure 21: Beliefs that Australians should have specific privacy rights</a> .....	30
<a href="#">Figure 22: Impact of privacy certification on trust in organisations</a> .....	31
<a href="#">Figure 23: Desired content in privacy policies</a> .....	32
<a href="#">Figure 24: Beliefs that organisations should do more to protect personal information</a> .....	33



<a href="#">Figure 25: Beliefs about organisations’ personal information handling practices</a> .....	34
<a href="#">Figure 26: Concern about organisations sending personal information overseas</a> .....	35
<a href="#">Figure 27: Concern about organisations sending personal information overseas by age</a> .....	35
<a href="#">Figure 28: Comfort sharing personal information with local and overseas organisations</a> .....	36
<a href="#">Figure 29: Comfort sharing personal information with local and overseas organisations by age</a> .....	36
<a href="#">Figure 30: Trustworthiness by industry sector</a> .....	37
<a href="#">Figure 31: Trust in aspects of personal information handling</a> .....	38
<a href="#">Figure 32 33: Trust in aspects of personal information handling by industry sector</a> .....	39
<a href="#">Figure 34: Information considered fair and reasonable to provide when accessing services by industry sector</a> .....	40
<a href="#">Figure 35: Comfort with the use of personal information for government research and development</a> .....	41
<a href="#">Figure 36: Beliefs about whether certain practices are fair and reasonable</a> .....	42
<a href="#">Figure 37: Problems experienced with the handling of personal information</a> .....	43
<a href="#">Figure 38: Incidence of privacy breaches</a> .....	44
<a href="#">Figure 39: Harms experienced from privacy breaches</a> .....	45
<a href="#">Figure 40: Harms Australians perceive could result from a privacy breach</a> .....	47
<a href="#">Figure 41: Awareness and impact of data breaches</a> .....	48
<a href="#">Figure 42: Awareness and impact of data breaches by age</a> .....	48
<a href="#">Figure 43: Harms experienced from data breaches</a> .....	49
<a href="#">Figure 44: Harms Australians perceive could result from a data breach</a> .....	50
<a href="#">Figure 45: Reactions to a data breach</a> .....	51
<a href="#">Figure 46: Reactions to a data breach by experience of data breach</a> .....	52
<a href="#">Figure 47: Steps organisations can take to influence people to remain with them after a data breach</a> .....	54
<a href="#">Figure 48: Responsibility for data breaches</a> .....	55

• List of figures

<a href="#">Figure 49: Most important action organisations should take to protect personal information</a>	55
<a href="#">Figure 50: Comfort with biometric analysis</a>	58
<a href="#">Figure 51: Comfort with one-to-one uses of biometric information</a>	59
<a href="#">Figure 52: Comfort with one-to-many uses of biometric information</a>	60
<a href="#">Figure 53: Trust in organisations’ handling of biometric information</a>	61
<a href="#">Figure 54: Conditions for the use of artificial intelligence</a>	62
<a href="#">Figure 55: Comfort with the use of artificial intelligence</a>	63
<a href="#">Figure 56: Acceptance of targeted advertising</a>	63
<a href="#">Figure 57: Parents’ concerns about the protection of personal information</a>	65
<a href="#">Figure 58: Parents’ concern and control over their child’s data privacy</a>	66
<a href="#">Figure 59: Parents’ actions to protect their children’s privacy online, by child’s age</a>	66
<a href="#">Figure 60: Children’s access to and ownership of devices</a>	67
<a href="#">Figure 61: Children’s use of online accounts and services</a>	69
<a href="#">Figure 62: Importance of children’s privacy when choosing services</a>	69
<a href="#">Figure 63: Appropriate ages for children to start learning about data privacy and provide consent</a>	70
<a href="#">Figure 64: Parents’ beliefs about accessing children’s services</a>	71
<a href="#">Figure 65: Parents’ beliefs about children’s data privacy</a>	72
<a href="#">Figure 66: Parents’ comfort with businesses using children’s personal information</a>	73
<a href="#">Figure 67: Change in parents’ discomfort with businesses using children’s personal information</a>	73
<a href="#">Figure 68: Organisational measures to increase the data privacy of children online</a>	74
<a href="#">Figure 69: Technology measures to increase the data privacy of children online</a>	75
<a href="#">Figure 70: Responsibility for the protection of children’s personal information</a>	76



**Australian Government**  
**Office of the Australian  
Information Commissioner**



Australian Community Attitudes  
to Privacy Survey 2023



[oaic.gov.au/acaps](https://oaic.gov.au/acaps)  
[corporate@oaic.gov.au](mailto:corporate@oaic.gov.au)

**OAIC**