Digital footprints and identities
Community attitudinal research

NOVEMBER 2013
# Contents

## Executive summary
- About the research: 1
- Why digital identities and information are important: 1
- Key findings: 2
- Personal information online: 2
- Identity management: 3
- What it means for citizens and providers: 4

## Overview of the research
- Overall project objectives: 5
- Methodology: 5
- The qualitative methodology: 5
- The quantitative methodology: 6
- Statistical reliability: 6

## Personal information online
- Factors influencing whether information is provided: 7
- The context in which the information is being requested: 7
- Elements of the provider requesting the information: 8
- The information being requested: 14
- Alternative strategies: 15
- Withholding information: 15
- Providing inaccurate responses: 16
- Digital footprints: 21
- Anonymity and pseudonymity: 21
- Breaches of trust: 22

## Identity mechanisms
- Online identifiers: 27
- Number of unique identifiers: 27
- Challenges in managing identifiers: 29
- Potential solutions: 32
- Third-party login services: 32
- Awareness and use: 32
- Attractiveness: 33
- Reservations about using third-party logins: 34
- Biometric identification: 35
- Identity certification services: 39
- Essential elements of an identity certification service: 39
- Barriers to using an identity certification service: 41
## Contents (Continued)

**Protecting users** 42
- Shared responsibilities 42
- Government role 42
- Responsibility for protecting users 43
- Where to complain 44

**Conclusions** 46

**Appendix 1**— The qualitative discussion script 47

**Appendix 2**— The online questionnaire 62

**Appendix 3**—Quantitative sample 74
Executive summary

About the research
In late 2012, the Australian Communications and Media Authority (the ACMA) commissioned Taverner Research to conduct qualitative and quantitative research about Australian internet users’ understanding and management of their digital footprints and online identities, and associated issues.

Digital identity and digital footprints are evolving concepts. A ‘digital identity’ is a collection of digital information that contains a set of identifying attributes, which may or may not reflect the attributes of a real person.

The term ‘digital footprints’ refers to the trail, traces or ‘footprints’ that people leave behind online. This is information transmitted online, such as registration details, emails, uploaded videos or digital images, and any other form of transmission of information—all of which leave personal information about individuals available to others online.

The qualitative research was conducted using nine stratified online discussion groups, each over seven days. In total, 98 participants completed all sections of the discussions.

The quantitative stage was completed online in March 2013, with a representative sample of N=2,509 online Australian adults aged 18 and over.

The research was designed to help inform the consideration and development of regulatory and non-regulatory approaches to assisting citizens in managing their digital identities and online information.

Why digital identities and information are important
An increasing focus in digital communications for businesses, individuals and governments worldwide is the management of digital information and identity. In an environment of rapid technological change, consumer online activity is also evolving rapidly.

The aim of this research was to understand behaviour and attitudes to the creation, use and management of an individual’s digital identity and the management of digital information online. It also aimed to identify what triggers an individual’s willingness to provide personal information online.
The management of digital identities and digital footprints is widely recognised as a substantial challenge for both internet users and providers of online sites, services and applications. Government and business in several countries have expressed concern about the complexity faced by internet users when asked to identify themselves online, and the barriers to commerce created by the challenges of ensuring reliable identification of users.\(^1\)

In this context, the concept of ‘trusted identities’ has emerged as a means to encourage greater online economic and social participation, and to mitigate negative activities, such as fraud and unauthorised data collection.

To help internet users manage and keep track of the identification requirements of a range of sites, services and applications, some providers are already offering services that simplify the task by having a single point of entry to multiple sites and applications, or provide a single source to verify their identity. Those who took part in this research were asked to consider different identity-related products and services, with a view to identifying what would encourage take-up and what barriers exist.

**Key findings**

**Personal information online**

Participants in the qualitative research did not see themselves as managing digital identities but rather as performing tasks such as:

- identifying themselves
- minimising and controlling the personal information they provide
- protecting themselves from unwanted intrusions, embarrassment and financial loss.

Qualitative research participants and quantitative research respondents were generally aware that they risked having personal information that they provided when registering for sites, services and applications used in ways they did not want. Trust in assurances about privacy and in privacy settings was low, with many quite sceptical about current industry practices. Many also saw little point in checking assurances in terms and conditions of use. Participants in the qualitative research explained that, if you wanted to use a site, you had to agree. Reading terms and conditions was often made difficult by their length, complex language and the use of small font sizes. However, only a minority of those involved said this was a barrier to engaging in internet activity.

Context was important in determining how participants managed their personal information and what information they were willing to provide. Discussions with them revealed that they had ‘transactional’, ‘social’, and ‘professional’ identities. Their strategies for using these identities differed accordingly. As part of a transactional identity, participants tried to limit the information they provided to only what was necessary for the transaction. With their social identity, they may be more willing to provide personal information, but they were cautious about data that may be used to identify them publicly. They were generally careful about how they constructed their professional identity on sites such as LinkedIn.

---

Participants wanted to maintain control of their online identity, irrespective of the context.

Some who took part in the research were largely unaware of how digital footprint data can be gathered and packaged for commercial use, and found this possibility disturbing. The majority were aware what can be gathered, if not always of the full extent. While many worried about the use that could be made of their digital footprints, others took the view that privacy is limited or does not really exist for internet users. Still, being able to maintain a degree of anonymity and control over personal information remained important to them.

The types of breaches that would annoy them most included:

- having their personal images revealed or their reputation damaged by personal information being spread around
- potential financial loss through credit card details being compromised
- becoming the target of unwanted marketing, especially offline.

For most, the primary concern was online information, such as their physical address, being disclosed, which may pose a risk in the ‘real’ world.

**Identity management**

Respondents reported having a large number of unique logins or passwords—from fewer than five to more than 50. Only a minority considered keeping track of their logins and passwords a serious problem or something that was difficult to manage. Many found it no problem at all. However, taken with other research about how users manage identifiers, it appears that many were not aware that the identity management practices they adopted—such as reusing the same or similar logins and passwords for multiple sites—placed them at risk.

Respondents were divided about the level of protection accorded their personal information when using a password-protected site, service or application. They were more likely to be confident about the safety of information they provided if access relied on biometric identifiers.

In both parts of the research, older users were more likely to say they coped with unwanted requests for personal information by not giving information or not using a supplier. Younger users were more likely to say they would give inaccurate information or supply an email address they did not use or was invalid.

Providing information that was inaccurate, or withholding information not considered necessary, provided a degree of pseudonymity and anonymity, which can be a way to manage online identities. However, this has implications for those who collect or aggregate data based on digital footprints.

A majority of quantitative survey respondents were aware of facilities that enable logging in to third-party services through an existing digital identity, such as a webmail or social media account. Despite this high awareness, less than one in four had used these services. Many had major reservations about the security of the credentials or personal information they provided to a third-party login service. They also had reservations about the potential tracking of their use of other sites and the subsequent use of this information.

Respondents were sceptical about more complex identity tools and certification services. They recognised the convenience of being able to use a single identity certification service to access many sites and services. However, they had reservations about security against hacking and misuse of personal information.
Consequently, most were not willing to consider using these services. Many preferred to continue using multiple logins and passwords, simply to minimise the damage that could result if all their personal data was found in one place. These concerns have implications for data-hosting and storage services, such as cloud services, that promote the benefits of easy access to data through a single storage facility.

**What it means for citizens and providers**

A range of barriers arising from identity management practices currently prevent citizens from engaging confidently with online services aimed at assisting them with the management of their online presence. These barriers are:

- Some users need to be persuaded that their current ways of keeping track of identifiers for multiple sites, services and applications potentially leave them vulnerable to data theft or fraud.
- Many need highly credible assurances that they will have control over the use of their personal information and digital footprints if they are to use such services.

Many require much greater confidence than they currently have that online identity management services are well protected against malicious intrusion.

When implementing changes, providers will need to take account of the strategies that individuals currently employ to manage their online identity and information. Providers need to understand why people want to remain anonymous or create pseudonyms.

**Protective action**

Internet users saw a role for government in educating them about managing their digital information generated by using the internet. They also saw government encouraging providers to promote safe use practices. About half of the online survey respondents believed government should take an active role and control how providers acquired and used personal information. A minority believed government had no role to play, while most recognised that users and service providers shared the primary responsibility for protecting information. Almost 40 per cent of respondents would complain about unwanted use to the service provider they considered responsible. Apart from this group, there was uncertainty about where (if anywhere) internet users could effectively complain about the unwanted use of their personal information.
Overview of the research

Overall project objectives
The ACMA commissioned Taverner Research to undertake a two-stage research project to clarify and quantify Australian internet users’ understanding of:
> issues and concerns about online identity
> the use of personal identifiers
> managing personal information online.

The ACMA commissioned Taverner Research to undertake a two-stage research project to clarify and quantify Australian internet users’ understanding of:
> issues and concerns about online identity
> the use of personal identifiers
> managing personal information online.

researchACMA
The management of digital information and identity is becoming an increasing focus in digital communications for business, individuals and governments worldwide. This current research is part of the ACMA’s research program and is aimed at understanding behaviours and attitudes to the:
> creation, use and management of an individual’s digital identity
> management of digital information online
> identification of what triggers an individual’s willingness to provide personal information online.

researchACMA is the ACMA’s research program that has five broad areas of interest:
> market developments
> media content and culture
> digital society
> citizen and consumer safeguards
> regulatory best practice and development.

This research contributes to the ACMA’s digital society research theme.

Methodology
This report covers both qualitative discussions and the quantitative survey. The qualitative stage explored the research objectives and clarified what could be asked in a quantitative survey and how best to ask it. The quantitative survey tested the extent of the opinions expressed in the qualitative stage and clarified which segments of the internet-using population held these opinions.

The target audience for this research was Australians aged 18 years and over who use the internet for personal reasons.

The qualitative methodology
Nine, seven-day online group discussions were conducted with participants recruited from an Australia-wide database of internet users. In total, 143 participants commenced the discussion and 98 fully completed all sections. Ages ranged from 18 to over 65 years, with a mix of males and females in each group.
Table 1 Stratification of online discussion groups

<table>
<thead>
<tr>
<th>Age group (years)</th>
<th>Pattern of use</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Heavy</td>
</tr>
<tr>
<td>Young, 18–29</td>
<td>Group 1. Social and transactional both high or both moderate (18 started, 8 completed)</td>
</tr>
<tr>
<td></td>
<td>Group 2. More social than transactional (18 started, 14 completed)</td>
</tr>
<tr>
<td>Middle aged, 30–49</td>
<td>Group 3. Social and transactional both high (18 started, 11 completed)</td>
</tr>
<tr>
<td></td>
<td>Group 4. More transactional than social (14 started, 11 completed)</td>
</tr>
<tr>
<td>Older, 50–59</td>
<td>Group 6. High transactional and some high social (18 started, 14 completed)</td>
</tr>
<tr>
<td></td>
<td>Group 7. Mainly Transactional (14 started, 6 completed)</td>
</tr>
<tr>
<td>Seniors, 65+</td>
<td>Group 9. Some high for both social and transactions (9 started, 8 completed)</td>
</tr>
<tr>
<td></td>
<td>Group 8. Light transactions, little social (17 started, 13 completed)</td>
</tr>
</tbody>
</table>

The qualitative questions and prompt material are in Appendix 1.

The quantitative methodology
The quantitative survey was conducted online with a sample of 2,509 respondents drawn from a large ISO-accredited research panel. The sample sought to closely match the population of adult (aged 18 and over) internet users throughout Australia. The online questionnaire was in the field in March 2013.

The full text of the quantitative questionnaire is in Appendix 2 and the sample breakdown is summarised in Appendix 3.

In this report ‘participants’ refers to those who were part of the qualitative study, while ‘respondents’ refers to those who took part in the online survey.

Statistical reliability
The sample was large enough to detect statistically significant differences that were relatively small in magnitude. Where differences are commented on in the text, these are statistically significant unless stated otherwise. A few differences involving small segments were substantial enough to merit comment, but did not reach conventional levels of statistical significance. Where this has occurred it is explicitly identified in the text.
Personal information online

To gain access to a range of services and information online, users are often asked to provide personal information to verify their identity. Trust and familiarity with the provider was one of the most important factors identified in the research, as was the type of information they were requesting. Qualitative participants also mentioned a range of features of websites, online services and applications they used to judge whether a site could or could not be trusted with personal information. The quantitative survey then tested how widely users rely on the main features that were mentioned.

The qualitative discussions also revealed a number of methods that some users adopt to gain access to online services while protecting themselves, including withholding information, and/or giving inaccurate or misleading information.

Factors influencing whether information is provided

The context in which the information is being requested

Participants put thought and care into their digital identity, revealing or concealing personal information they deemed appropriate for a specific interaction.

Participants were willing to reveal or to conceal personal information, depending on the context of the identity information offered by others and the nature of their relationship with them. The ‘other’ party can be another individual but, increasingly, online transactions involve government and commercial entities.

The styles of digital identity can be grouped into the following categories:

> transactional
> social
> professional.

Transactional identity

A transactional identity was kept within the narrowest possible parameters, with users withholding all information except what was necessary for success.

Despite the reference to limiting the personal information provided, information disclosed in creating the identity might include highly sensitive items, where this was required to make use of what is offered online by the other party.

Social identity

For the majority of participants, social identities such as a Facebook page, enabled the reconstruction of their everyday personal and family life in a digital context. The sharing of images was a major part of this process. This information was strictly controlled, with users attempting to limit access to their personal information. This included photos and identifying information, such as address and phone numbers. Their main concern was that they did not want this data to be reassembled on the internet; they wanted to be reassured that only those they selected as ‘friends’ had access. The exception was some older users who felt that people revealed far too much about themselves through their social use of the internet. As one older participant said:

I never use Facebook etc. I could never see the purpose other than trying to promote a public image of one’s self. Sort of brand management. Trying to control others’ image of one’s self. All a bit fake, self-centred and corporate for my tastes.

Group 6: 50–64s, higher users
**Professional identity**
Participants recognised that with a professional identity, such as a LinkedIn presence, users want to be locatable online to provide people they do not already know with a positive image of their skills, experience or business offering. In effect, this identity is part of the complex of social identities created on the internet when use goes beyond conducting transactions.

If it is for leisure, I try not to give a lot of personal information. On the contrary, if I am in a professional context, I will tend to share more personal information.

*Group 2: 18–29s, social more than transactional*

**Elements of the provider requesting the information**

**Trust and familiarity**
Evidence about the types of suppliers of sites, services and applications that would be more or less trusted emerged from direct probing about:

- the sites that participants had decided to withhold requested information from, or to give incorrect information, and what made them comfortable to give information
- the organisations they would trust online to only gather and pass on information with the user’s permission
- the organisations they would trust more and which they would trust less to manage a trusted-identity service.

When asked which sites they trust and what is different about these sites, participants mentioned government sites, banks, PayPal or eBay. They pointed to the size and established reputation of these organisations.

They are big organisations with a reputable history. They know if they break a customer’s trust by sharing information it could cost them a lot.

*Group 1: 18–29s, high transactional and social*

[Be from] secure, reputable companies (e.g., banks where I have an account) or government departments. I will also provide accurate information to shopping sites that I have researched and approached.

*Group 5: 30–49s, social more than transactional*

It comes down to what I consider to be reputable companies and organisations. For example, I feel comfortable on eBay as they take all precautions with strong security and try to eliminate scamming.

*Group 6: 50–64s, higher users*

There was considerable trust that well-established banks and government organisations would ensure the security of transactions. Many believed (although some expressed strong dissent) that the information would be used for legitimate purposes and protected from access by unauthorised third parties.

Others believed that no site could be completely secure from attack by skilled and determined hackers. The following examples point to an underlying sense of insecurity. This is based on publicity about hackers having spectacular success in breaching the security of large reputable organisations.

Thankfully, me becoming an unwilling accomplice to credit card fraud has yet to occur, but I suppose it’s just a matter of time as hackers become more adept at breaking into ‘supposed’ secure sites.

*Group 4: 30–49s, more transactional*

The only problem is the software needs to be one step ahead of the hackers, if only that could be so.

*Group 8: 50–64s, less active*
We are always being told that whenever new [online security] ideas are introduced the hackers have them sorted within 48 hours or less on some occasions.

*Group 8: 50–64s, less active*

For social media sites, in particular, knowing and trusting other users was mentioned as a source of reassurance:

… have trusted friends/members to that new social network other than Facebook.

*Group 1: 18–29s, high transactional and social*

When dealing with other organisations, businesses in particular, they relied on a range of indicators to decide whether a provider could be trusted. These included:

> whether they had a relationship with the organisation or business offline
> its size and reputation
> whether it offered a privacy and/or security policy
> whether trusted friends had used the site without difficulty
> whether the site appeared fully professional.

**Information entrusted to government organisations**

Qualitative research participants (apart from a few who volunteered that they strongly mistrusted government) felt safer giving personal information to government organisations than to commercial or non-government organisations. The qualitative discussions indicated that many would be thinking of organisations like the Australian Taxation Office (ATO), Centrelink and Medicare as ‘typical’ government organisations. These organisations both pay considerable attention to data security and obtain extensive information about individuals from other organisations, and share some of this with each other.

Some mentioned that the government was able to cross-link databases and find this information without the user having to give it, so giving it directly did not increase what the government can find out.

Given the relatively high level of trust in government expressed in the qualitative discussions, respondents were asked in the quantitative survey what information they would give to a government site or service. The types of information listed were based on those that qualitative participants had indicated they would be more or less willing to give to a government organisation site. Their replies are summarised in Figure 1.
The information that would be given to gain access to a government online service fell into groups:

- full name, gender and date of birth appear to be the least sensitive, with three in four willing to provide this information
- home address, phone number(s) and place of birth would be provided by around half
- about one in four would provide their current location
- around one in five would identify their employer
- just under one in 10 would not share any of this information with a government organisation.

As in the qualitative research, there was a relatively small minority (under 10 per cent) who would not trust a government organisation with any of the types of information listed. They were very likely to come from those with no formal educational qualification (21.8 per cent).

**Information entrusted to non-government organisations**

Willingness to share as much information with businesses or other non-government organisations sites, services or applications as with government organisations varied with the characteristics of the site and familiarity with the provider (see Figure 2).

The options shown to respondents were based on characteristics mentioned by qualitative research participants as indicating that an organisation could or would be
trusted or not. The qualitative discussion groups suggested that each of these options would be a ‘trigger for trust’ for at least some internet users.

Figure 2 Organisations respondents would give the same personal information as government organisation

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business or organisation you already know and trust offline</td>
<td>46.8%</td>
</tr>
<tr>
<td>A well known reputable business you have not previously dealt with</td>
<td>28.1%</td>
</tr>
<tr>
<td>An unfamiliar business or organisation with a reasonable quality site</td>
<td>8.6%</td>
</tr>
<tr>
<td>An unfamiliar business or organisation that a friend has told you is</td>
<td>8.3%</td>
</tr>
<tr>
<td>An unfamiliar business or organisation that has a high quality,</td>
<td>7.9%</td>
</tr>
<tr>
<td>professional site</td>
<td></td>
</tr>
<tr>
<td>None of these</td>
<td>44.9%</td>
</tr>
</tbody>
</table>

Base: Total sample, N=2,509
Q4INTa

Almost half the sample would not give any type of organisation as much information as they would give a government organisation (see Figure 2). Only one option—being known and trusted offline—won as much trust as a government organisation from almost half the sample (46.8 per cent). Being a well-known and reputable business that the respondent had not previously dealt with would lead about one in four giving the business or organisation as much information as they would give a government organisation.

The use of commercial sites and services that require personal information from users is widespread. Consequently, it appears likely that many more than half of all internet users do give similar information to commercial and government organisations in the circumstances described. However, the results show widespread caution, at least in principle, and indicate where caution would be more common.

Additional analysis of relationships between the items and other measures suggested that there was a general ‘willingness to trust’. This ran through reactions to what people are willing to give government organisations and what will make them more willing to share the same information with other organisations. Some people were consistently more cautious and some consistently more trusting.

Being known and trusted offline, and being a well-known, reputable organisation, were the keys to being trusted by more respondents.
**Terms and conditions given little attention**

In the qualitative discussion groups, considerable scepticism was expressed about how much attention users give to privacy assurances. Privacy assurances are usually outlined in a set of terms and conditions that users who register for a site or service, or download an application, are asked to accept. They may also be in a statement of the privacy (protection) policy followed by a provider.

The majority of participants did not pay a great deal of attention to a provider’s terms and conditions when making their decision about whether to provide personal information. Thorough reading of terms of use, or even skimming though them to check privacy assurances, was not widespread. The reasons participants gave for not paying more attention included:

- difficulty reading the sheer volume of such material
- the use of small font sizes
- the use of complex legalistic language
- terms of use have to be accepted to gain access to the benefits offered by a site, service or application.

  I for one have a bad habit of skipping terms and conditions, simply because they are too long, tell you things you really don’t need to know which makes you skip past the parts you really should read. Why can’t they keep them simple and use normal words rather than spread it out over 18 pages to say this and that?

*Group 1: 18–29s, high transactional and social*

To test aspects of these qualitative findings, quantitative respondents were asked what they usually do about statements of terms and conditions. Responses varied widely (see Figure 3):

- just over one in 10 reported that they always click through and read terms and conditions statements
- three in 10 reported that they usually skim through terms and conditions looking for key points
- around one in 10 said they usually check for the assurances given about protection of personal information
Features of the website

In considering whether to provide personal details online, some participants mentioned, without any prompting, looking for visual cues. These cues included the site using a secure connection (https://), having a padlock symbol or being identified as ‘safe’ by a trusted browser.

Because they (have) https login rather than http so I can be sure that is it is secure.

*Group 1: 18–29s, high transactional and social*

The obvious things apart from reputation that I look for are the security features such as a padlock symbol or https in the web address.

*Group 5: 30–49s, social more than transactional*

I always check there is a padlock in the address bar if I am buying anything online, or make sure they use PayPal. Also unless there is a privacy statement check box I won’t usually sign up.

*Group 1: 18–29s, high transactional and social*

To be comfortable about sharing personal details, a website needs to look:

… real—not too many ads on the page, if any… If the site looks dodgy, asks too many questions, has pop up ads, or is simply not my style then yes I keep my guard up. Even wording of questions can make all the difference.

*Group 1: 18–29s, high transactional and social*
The quality of the content and the level of professionalism of the website were also important to some participants:

I look for spelling mistakes and poor grammar as signs that the website may have integrity issues.

*Group 6: 50–64s, higher users*

If I get a lot of ads on a website, if I see a lot of spelling mistakes or the whole functionality of a website is wacky, I tend to stay away.

*Group 2: 18–29s, social more than transactional*

I avoid giving any factual personal information to sites that have poor English (any obvious spelling errors or poor grammar).

*Group 4: 30–49s, more transactional*

Most participants were familiar with privacy setting options for sites like Facebook or Google. Many had used these settings as part of their social media activities. However, there were mixed feelings about how confident they were that the settings could achieve the control they wanted over their personal information.

Survey respondents were asked to think about how devices, applications, browsers and sites allow users to choose privacy settings. They were also asked how confident they were that they could achieve the level of privacy they wanted by choosing a preferred privacy setting (see Figure 4).

**Figure 4 Confidence in privacy settings**

![Confidence in privacy settings chart](chart)

*Base: Total sample, N=2,509*

Q3INTc

Nearly 40 per cent were completely confident or confident enough. Almost as many endorsed ‘I hope they work’ (37.9 per cent) or indicated that they were doubtful or sure such settings did not work (14.2 per cent). Men were more likely than women, and younger people more likely than older people, to be confident that privacy settings would work.

**The information being requested**

In addition to the cues already reported that would generate trust or mistrust, some qualitative participants mentioned the nature and quantity of the information sought. There were marked variations in how willing participants were to share different
categories of personal information. The order from most to least sensitive appeared to be:

> information that, if misused, could result in financial loss, such as credit card and banking details
> information that could lead to becoming accessible offline, such as home address and work address and telephone numbers
> information needed to communicate with the user, such as an email address
> identification data that would not make the individual easily accessible to online or offline marketing efforts, such as name and date of birth, appeared less sensitive.

If the information was necessary for carrying out the service (for example, delivering goods to the user’s home requires their home address) then there was much greater willingness to give that information than if the information did not appear to be essential.

Many participants objected to providing any information unless they could see a need for it, given the nature of the use they were making of the site, service or application. Participants felt that providers simply did not have the right to access some information and that users should have control over how their personal information was used.

I assess whether or not they need that actual sensitive information. Why is Random News Website.com asking for my age and gender? Nope, get lost RNW.com.

Group 5a: 30–49s, social more than transactional

Explaining reasonably why they require my information and what they are going to use it for.

Group 1: 18–29s, high transactional and social

Alternative strategies

Withholding information

The qualitative discussions revealed that the majority of participants would withhold personal information to an online provider, if they were not comfortable with the request—either for security or privacy reasons, or because they simply could not see why the information was being requested.

Quantitative respondents were asked in what circumstances they would withhold personal information online. As Figure 5 indicates, sites that lack a padlock symbol prompted most respondents to say they would withhold personal information (83.0 per cent). Over half would withhold personal information if the site did not appear professional, the information they are asking for was not relevant to the offering, or the site was unknown to them. The site not being based in Australia would be a barrier for one in three.

Appearing unprofessional, and asking for information that appeared not to be needed for the service offered, would not be a barrier for one-third or more of the sample. Being unknown to the user would not be a barrier for almost half.

Many sites and services do not have a padlock or other indicator of site security, but are still used. Consequently, the proportion may have been overstated, with more than 80 per cent saying they would withhold information if such certifiers are lacking. However, the percentage endorsing each indicator as grounds for withholding information is a valid basis for estimating the ranking of these cues for caution, in terms of how many users believe they should pay attention to a particular cue.
Figure 5 Circumstances in which personal information would be withheld

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The site does not have a padlock or other sign that it has met a security standard</td>
<td>83.0%</td>
</tr>
<tr>
<td>The site does not appear professional - poor graphics, bad spelling and grammar, poor layout</td>
<td>63.6%</td>
</tr>
<tr>
<td>You cannot see how the information is needed by the site to provide what it offers, even if you are keen to get access</td>
<td>61.5%</td>
</tr>
<tr>
<td>You have not heard of the site</td>
<td>52.0%</td>
</tr>
<tr>
<td>The site is not based in Australia</td>
<td>35.7%</td>
</tr>
<tr>
<td>For some other reasons</td>
<td>0.3%</td>
</tr>
<tr>
<td>None would stop me if I really wanted what the site offers</td>
<td>8.3%</td>
</tr>
</tbody>
</table>

Base: Total sample, N=2,509
Q2PRIV

Indicating that they would withhold information from a site not based in Australia, or a site the respondent had not heard of previously, both increased sharply with age group.

Providing inaccurate responses

Giving inaccurate personal information was also a strategy reported by the qualitative participants. This approach was adopted if they wanted to access a particular site, service or application but found the information required to register to be excessive. Participants reported that they would resist demands to provide too much information by deliberately providing incorrect information; pretending to surrender their anonymity without actually doing so. Users, especially younger users, appeared willing to replace anonymity with what might be termed ‘pseudonymity’. They would do this by withholding or misstating one or more of their real name, their actual age or date of birth, their email address or their physical address.

Younger participants (in their 30s or younger) were more prepared to give incorrect information, especially when asked to provide their age or date of birth:

I’ve entered incorrect personal details to allow me to access information on a website e.g. date of birth. This is only if that information is a ‘required’ field and I felt the end result was something worthwhile.

Group 5: 30–49s, social more than transactional
Often very wary [about giving age] as I don't believe age is significant/necessary in many situations, especially online.

**Group 1: 18–29s, high transactional and social**

I don't [give my age]. I'll use a landline if it's important or if the site insists I'll use my alter ego's age and date of birth.

**Group 3: 30–49s, high transactional and social**

Not happy about it at all. I don't mind age brackets, but I don't see the need on many of the sites that ask for it.

Some participants suggested they had an obligation to give incorrect information to protect online friends who might be vulnerable, in the case of a third party accessing the user's social network account.

I indeed [have] given information online that is not accurate and I will gladly explain why I have done so:

1. to protect my identity, location, and friends, family.
2. when people start asking me all the wrong questions and can't explain why
3. when I think I am talking to some village's lost idiot
4. if I think I am putting myself or anyone I know at risk in anyway
5. when my security program tells me that the site is suspicious
6. sometimes I just have feeling that things are not quite right.

I think these are all valid reasons for being less than honest online.

**Group 3: 30–49s, high transactional and social**

As another in the same group explained:

It is not just about me, it is also about protecting other people, such as friends and family. I do not just add every Tom, Dick and Harry who sends me Facebook requests to become one of my friends, this is because I am concerned about my contact's security, as I have family members, and close friends and school friends in my friends list, and I try to do my best to protect them as well, from fraudsters and scammers, as it is very easy for people to make up fake IDs and join such websites, and they then try to con and scam people.

**Group 3: 30–49s, high transactional and social**

Allowing users to control what they reveal and to whom was a further theme that emerged from the discussions:

The only real site that gives me any pause is Facebook. Not out of fear of what data miners might find, but because when [my] internet illiterate mother throws something up on my Wall, I want to be able to take it down.

The only thing that springs to mind is possibly emphasising certain points of my career history when applying for jobs and downplaying those [that are] not so important, depending on what is asked for in the ad or through the recruitment agency website.

**Group 4: 30–49s, more transactional**

Survey respondents were asked about the circumstances in which they would give incorrect information about themselves. These are listed in Figure 6, which shows the percentage of respondents endorsing each justification for giving inaccurate information.
Internet users appeared to be sharply divided on this issue:

> just under half the respondents (47.4 per cent) were willing to acknowledge giving inaccurate information in at least one situation
> about one in three (36.1 per cent) reported they would rather not use a site than give inaccurate information
> one in six (16.5 per cent) responded that they had never felt the need to give inaccurate information.

**Figure 6 Giving inaccurate personal information**

There were sharp differences between age groups in their willingness to give inaccurate information (see Figure 7). Those aged 18 to 24 years were most willing to give inaccurate information (63.6 per cent). Approximately half or more of those aged 25 to 44 would give inaccurate information. The oldest age groups (55 and over) consistently were the least likely to acknowledge giving inaccurate information and the most likely to say they never did so.

The main reasons that would lead respondents to provide inaccurate information included seeing the information as unnecessary, or not being sure that the site asking for the information could be trusted (see Figure 6). Lack of a clear and accessible policy about security and privacy was a less powerful trigger. However, it would still lead significant minorities of those aged under 35 to give inaccurate information.
Respondents were also asked whether they give different answers to questions asked when registering for different sites. The responses are in Figure 8. Just under half endorsed the reply that they would keep identifying information as similar as they could.
A follow-up question asked those (n=705) who endorsed ‘None of these’ to describe their reasons for giving different answers. As Figure 9 shows, most of the respondents who had not endorsed one of the prompted replies mentioned the desire to avoid one or other type of adverse consequence of a site being hacked, or of information being passed on to third parties the respondent had not approved. This suggested respondents saw grounds for mistrusting the site, even if the word ‘trust’ was not explicitly mentioned.

Many of these reasons could also be taken more generally to support either one of the two prompted reasons listed in the question—either to protect themselves or others from intrusions, or because they considered the service provider did not need the information to provide the service.
The survey results strongly confirmed the qualitative findings that many people—and a large majority of those aged under 35—will preserve their effective anonymity by providing incorrect personal information when required to give information to gain access to a site, service or application. Consequently, instead of using the internet with complete anonymity, many users seek to manage how anonymous they are.

**Digital footprints**

**Anonymity and pseudonymity**

Many participants in this research viewed the internet as an information-sharing medium. However, they wanted control over how that information is shared and with whom. This even included users who doubted that such control is possible.

One of the core concerns expressed by participants related to the misuse by providers of the information entrusted to them and the need for control over the use of personal information revealed online. This was true whether the participant sought to reveal or to conceal their identity.
Give me the right to create, edit, modify and remove what I put online. If you want to associate something to myself, I want that same right over that too.

*Group 5: 30–49s, social more than transactional*

Confidentiality and anonymity were most strongly valued when it comes to information that identifies and locates the user offline being extracted from personal information provided online. The coupling of a social identity with location-based identifiers, such as an address, was a particular concern for some participants. They expressed the view that disclosure of a physical address would attract even stronger reactions than disclosure of telephone numbers or email addresses. There was also real concern expressed about location information being captured from use of a smartphone without the user being aware that the data had been captured, linked to their online identity, packaged and sold.

Being anonymous is the highest degree of control you can have. Beyond that is a level of trust placed in a site's privacy settings.

*Group 5: 30–49s, social more than transactional*

For some qualitative participants, anonymity plays an important role in the way they engage in a range of online activities, such as commentating on online content (for example, blogs, news stories, and forums). It is a key benefit they seek from this medium.

On Reddit I try to avoid giving out any identifiable information, the anonymity allows me to say what I feel.

*Group 2: 18–29s, social more than transactional*

**Breaches of trust**

Qualitative participants were shown a short information video, produced by an overseas regulator, that described how digital information about a person’s everyday transactions can be collected and used. In the subsequent discussions, there was a sense of acceptance among the participants that internet use leaves a trail of data. Some qualitative participants were resigned to data being used without permission to enable online and even offline marketing.

Realistically, if you don't want any of your personal information 'out there' then don't use the internet. We leave a trail everywhere we go, so we each have to accept responsibility that the information may be sold to others or used for whatever reason.

*Group 7: 50–64s, transactional*

For some participants this meant abandoning the concept of privacy altogether.

As I've said … total privacy is a thing of the past.

*Group 3: 30–49s, high transactional and social*

Others were simply not concerned about maintaining privacy.

I'm not too worried about who has my information. I'm not a conspiracy theorist.

*Group 5: 30–49s, social more than transactional*

Responses by qualitative research participants to the potential for digital footprint information to be shared without their permission ranged from resignation (as illustrated above) to surprise and anger. Older participants tended to be more aware of the possibilities and calmer in their reactions. Some in the youngest groups were explicit about how upsetting they found these possibilities.
... I was shocked to hear that the info we provide is sold. That surprised me but now makes me realise how I get those scam emails maybe they bought my email address!!

**Group 1: 18–29s, high transactional and social**

Oh my goodness ... I’m freaking out to be honest! Every day someone gathers info on me. That’s scary. The whole video was a surprise. That’s really scary.

**Group 2: 18–29s, social more than transactional**

I WAS, however, surprised, angry and to be honest, kinda creeped out by the fact that they sell info on medical history.

**Group 2: 18–29s, social more than transactional**

While some younger respondents were not surprised, one of them recalled intense initial reactions to learning of the possibility:

Overall, I wasn’t surprised by the topic/theme of this video. I was gobsmacked when I first found out about this happening only 2–3 years ago, but watching this now was somewhat old hat.

**Group 2: 18–29s, social more than transactional**

Even for those participants who were more aware of the possibility and had accepted that such use (or misuse) was to be expected, they were firm in their desire for this sort of data to be managed ethically.

The quantitative research confirmed the range of reactions found among qualitative participants. As Figure 10 shows, the majority of respondents indicated they were aware of the possible vulnerability of digital footprint data and how it could then be used (65.2 per cent). Just over half of those who had been aware (18.8 per cent out of 33.8 per cent) said they were a bit worried about it.

---

2 In the quantitative survey, they were asked: When we use the internet we leave information behind about ourselves and what we have done. Even some information about offline actions can be found by internet searches. Some organisations gather this information together and supply it for commercial use without permission from those the information is about. This might include information that identifies us individually, or be anonymous. How do you feel about the idea that personal information you have given and data about your activities can be gathered up and passed on for other organisations to use without your knowledge or permission?
One in three (33.8 per cent) said they had not previously been aware of this vulnerability. Of these, just under half (15.1 per cent) indicated they were really shocked or upset that this can happen.

The quantitative survey asked which (if any) of a set of privacy breaches, identified from the qualitative discussions, would so annoy a user that they would stop using the site or service. This was designed to measure the relative sensitivity of the different categories of information listed. Figure 11 lists these in order, from the one that would prompt the most people to stop using the site or service, to the one that would trigger the fewest.

---

Note that this total differs from the sum of the values shown in the graph (33.9%) due to rounding. Where similar differences occur throughout this report, this is due to rounding of the more detailed numbers.
Almost all respondents found something in the list to be sufficiently annoying to prompt them to stop using a site. The greatest concern was a security breach that could directly result in financial loss through credit card details being stolen. Becoming vulnerable to unwanted telemarketing calls would upset almost as many respondents, slightly ahead of being vulnerable to unwanted email marketing material. Concern about other users making personal images available, where this was not intended, and loss of their reputation through sharing of private details, were similarly widespread.

The results indicate that learning about a security breach through media reports would annoy more users (over seven in 10), prompting them to stop using a site. Fewer users would be annoyed if they learnt about the security breach through the provider asking them to reset their login or password (72.2 per cent compared to 48.2 per cent).

The results largely confirmed the findings of the qualitative research about the types of breaches that most annoy users. In particular, having personal images revealed or reputation damaged by personal information being spread, potential financial loss, and becoming the target of unwanted marketing (especially offline) were the events most widely considered annoying.

Protection against these breaches requires secure sites, control over who has access to personal images and sensitive personal information, as well as influence over how they use such information. Assurances are also required from providers to the effect that personal information, including contact details such as email addresses and...
phone numbers, will not be passed on to third parties without the user's knowledge and permission.
Identity mechanisms

To create an account or register to use a website, users will usually nominate a username or login and create a password that fits any requirements the site has. Personal identifying information, such as name and address, are often also required to create an account.

The login and password will then be used for subsequent access to the site. This is the case for most transactional and many social websites.

Many sites offer password and username recovery features, but some users will simply create a new account if their attempts to access the site again are unsuccessful.

One purpose of logins and passwords is to reassure providers that they are dealing with the same individual user. Another is to protect users from any unauthorised person or organisation pretending to be them and using this information to access private information given to a supplier, or undertake transactions using the user’s identity.

For this to work for users, they not only need to have genuinely secure identity authenticators—currently mostly passwords—but they also need to be confident that a supplier will observe assurances given about the security and privacy of their personal information.

As user accounts are usually unique to each website, users will have multiple identities—usernames or logins and passwords.

Online identifiers

Number of unique identifiers

The number of distinct identifiers respondents reported using varied considerably. Figure 12 shows that over 64 per cent reported having fewer than 10 identifiers and only 13.5 per cent reported having 20 or more. Consequently, keeping track of identifiers may not be too onerous for many people, especially if (as reported in the qualitative discussions) many used variations of one or two basic patterns.

The qualitative finding about use of a limited range of passwords is consistent with other studies, such as the 2011 survey for PayPal Australia. That study concluded many users were vulnerable to attack because they use the same identifiers for multiple activities. Respondents taking this approach are likely to be concentrated among those with fewer than 10 different logins and passwords.

---

There were significant differences in the estimated number of unique identifiers depending on whether respondents had logins and passwords for transactional and/or social activities (see Figure 13):

- those with logins for both had a larger number of unique identifiers (10.9)
- those with logins only for transactional use (8.4) and those with logins only for social use (7.7) had fewer unique identifiers.

These differences were to be expected because those engaged in a more limited range of online activities that required identifiers would be expected to have fewer unique identifiers on average.
Challenges in managing identifiers

The research investigated the extent to which internet users found managing logins and passwords a challenge, and the types of strategies they were using to overcome this.

Participants were asked what problems they have had in managing their logins and passwords, and how they kept track of them. Online survey respondents were asked how many unique logins and passwords they had. They were also asked to rate how easy or difficult it was to keep track of them, and whether it was getting easier or harder to keep track.

Qualitative participants reported a wide range of problems and strategies.

Some people keep track of their passwords via an online application or word document. I think this is silly as you can be hacked or your computer die. I keep all mine hand written down and in a safe place in my house, but I rarely need them as I can generally remember each password for each site.

Some troubles I've run into are the length, combinations, capitals, and certain prefixes within a password. This can make it difficult if you can't remember/find your password or depending on the device you are using, to log on. Other than that no other [problems] I can think of.

Group 1: 18–29s, high transactional and social

It's hard to remember them because the different rules mean you have slight variations in each one. I don't [keep track of them], I spend a lot of time clicking 'Forgot your password?'.

(Group 2: 18–29s, social more than transactional)

This drives me crazy! Sometimes I can't even browse a site unless I create an account (Cudo etc..), so depending on my mood I'll sometimes create an account & other times I'll look elsewhere where I don't need to register.

(Group 4: 30–49s, more transactional)

Relatively few seemed to find keeping track of logins and passwords a problem that could not be overcome. Some kept systematic lists in a document on their computer, while others kept lists offline. Those who have no trouble remembering their logins and passwords might achieve this by varying them slightly to meet requirements for:

> the number of characters
> a mix of numbers and letters
> a mix of upper and lower-case letters.

Participants relied on their browser remembering the password they use for a particular site or service.

I write them down or allow my web browser (Chrome) to remember them.

Group 1: 18–29s, high transactional and social

A few expressed frustration about losing track of a password, then having to ask for a new one, and perhaps having to answer security questions to have it sent to them.

It's very difficult as I am registered with a lot of different sites that require logins and passwords.

Group 1: 18–29s, high transactional and social
Several had found ways to make it easier to keep track.

I've never had a problem with this. As far as I'm concerned, I can safely use the same password with slight variations for most websites. If some rogue element from one site uses my password to log onto another site with which I'm a member, and all they can possibly do as a result is find the same information I've posted on their own site or download golden age comic books for free, then I'm no worse off. In contrast, my eBay password is different from my Amazon password because I wouldn't want people working at one site using my credit card info on another, or making alterations to my account.

Group 5: 30–49s, social more than transactional

So, while keeping track of logins and passwords can be challenging, most users reported having found ways of doing this that they were comfortable with. While some expressed frustration, most did not find it to be a major challenge.

Survey respondents were asked how easy or difficult they found keeping track of their logins and passwords. As Figure 14 shows, the bulk of the quantitative sample did not find this task more than ‘sometimes difficult’. A total of 48.8 per cent said it is either no problem or a minor nuisance, 33 per cent that it is sometimes difficult, and 18.2 per cent that it is often difficult or a major difficulty.

Figure 14 Managing passwords and logins: level of difficulty

![Figure 14](image)

*Base: Total sample, N=2,509
Q3INTa*

Respondents were also asked whether keeping track of their different user names, logins and passwords was getting easier, harder or was unchanged. Over half reported that it had not changed (see Figure 15).
Base: Total sample, N=2,509  
Q3INTb

Breaking down the answer by how easy or difficult respondents found keeping track of their logins and passwords clarifies responses to this question (see Figure 16).

There was a significant association between how difficult respondents found keeping track of their logins and passwords, and reporting that this was becoming harder.
The overall low incidence of feeling seriously challenged by password management might be because:

> the task, done properly, is easy
> many users are not doing the task very well, and do not realise that they are vulnerable.

Given the results of the qualitative discussions and the other research cited previously, it appears likely that users did not recognise that the strategies they have adopted to simplify the task leave them vulnerable. Alternatively, they are not sufficiently concerned to give up the convenience of simple coping strategies, such as repeated use of the same password. In addition, the sites they are using lack the security features, such as requiring hard passwords and regular password changes, to force them to do so.

**Potential solutions**

A number of mechanisms have been set up or suggested to help users manage their multiple logins and passwords. These include:

> using the login and password from a more ubiquitous service, such as webmail or a social network, to access another party’s site (third-party login service)
> improving security by using a unique biometric identifier, such as a fingerprint, iris scan or voice ‘print’, to identify a user
> using a service where credentials registered with a certifying authority are used to access another site (identity certification services).

Attitudes towards third-party login services, biometric identifiers, and certification services were all examined.

Considerable effort was made in the qualitative research to communicate concepts, such as the use of physical identification devices, visual identity certification through smartphone applications, and the use of online identity verification services (see Appendix 1).

In the online survey, the explanation of the relevant concepts was abbreviated as much as possible (see Appendix 2).

**Third-party login services**

**Awareness and use**

A growing number of websites offer a user the ability to log on to the site using existing credentials, for example, their login and password from Facebook, Google+, PayPal and Microsoft.

As Figure 17 shows, most respondents (80.5 per cent) were aware of such services and almost a quarter (22.9 per cent) had used them.
Between age groups, there were significant differences in awareness of such sites and in having used them, with awareness and use declining with age.

**Attractiveness**

Respondents were presented with a list of potential advantages that might attract them to use a third-party login service. Figure 18 summarises the replies.

The most common response, given by half the sample, was that such a service had nothing attractive to offer.

The obvious advantages were endorsed by between 18.1 per cent and 28.9 per cent of the sample. These were:

> reducing the number of logins and passwords to keep track of
> saving time registering for a new site
> having more trust in the site offering the login service.
Figure 18 Attractions of using third-party logins

Base: Total sample, N=2,509

Reservations about using third-party logins
The most often endorsed (45.2 per cent) of the prompted reservations was the preference to keep different sites separate and avoid having data held by these sites potentially gathered together in one place (see Figure 19). The concern that the login site might pass on information without the user’s knowledge or permission was next most often endorsed (36.3 per cent). Again, this aligns closely with the qualitative findings.

Other reservations were:
> lack of control over what was passed on (35.1 per cent)
> concern that the sign-in site would gather information about the user’s online activities (30.9 per cent)
> doubts about how secure it would be (29.5 per cent)
> concern that the user might then not have an individualised login to the other sites accessed through the service (10.8 per cent).
Biometric identification

The qualitative participants were shown a document that outlined different ways of ‘establishing who you are’. It included a list of personal information that might be sought and a range of biometric identifiers, such as a fingerprint, iris scan or voice.

Reactions to the options outlined varied. There were some quite detailed and knowledgeable responses. For example, one (from Group 5: 30–49s, social more than transactional) provided a detailed review of the perceived advantages and disadvantages of each type of biometric identifier, and compared these to the use of personal information to verify a user’s identity.

While many felt considerable confidence in the effectiveness of some biometric identifiers, others saw these as intrusive:

- I feel comfortable using any of these and find the use of biometric indicators useful as they are unique to the individual person e.g., iris scan.
  
  *Group 4: 30–49s, more transactional*

- I would love to use either my fingerprints or an iris scan rather than having to remember my PINs for my credit and debit cards. I would feel safe using these as they’re not easily hacked. The informational identifiers can easily be found by someone looking for that information or easy to come by, for example, if you lost your wallet or had a home break in, so on the whole not a safe bet.
  
  *Group 4: 30–49s, more transactional*
I think fingerprint or iris scan are good ways of identifying people... Signature is OK, but can be copied and in an online world it's impractical.

*Group 5: 30–49s, social more than transactional*

Some of the so-called biometrics are just plain spooky: DNA, voice print, iris scan etc. I just want to buy some wine on the internet, not work for MI-5.

*Group 5: 30–49s, social more than transactional*

Some found the idea of a biometric identifier hard to grasp:

I am not exactly sure how something like this is supposed to work.

*Group 4: 30–49s, more transactional*

I probably wouldn't use any of these. It's too complex.

*Group 2: 18–29s, social more than transactional*

One raised the issue of trust in the organisations that would have to store the information so the user could be verified:

Who’s going to collect and store biometric identifiers? How are they going to prove themselves to people? It seems, to me, that everything is coming back to trust.

*Group 8: 50–64s, less active*

The survey asked how vulnerable or safe respondents would feel when logging into a reputable site using a password or a biometric identifier. The qualification of the sites as ‘reputable’ was included to reduce any variation in the interpretation of the scenarios.

Most respondents (65.4 per cent) felt reasonably safe (59.7 per cent) or very safe (5.7 per cent) when using a reputable password-protected site. Only 17.2 per cent felt vulnerable (14.2 per cent) or very vulnerable (3.0 per cent) to unauthorised access to and use of their personal information. However, 17.4 per cent were unsure how safe they felt (see Figure 20).

Substantially more respondents felt very safe when using a biometric identifier rather than password (34.4 per cent compared to 5.7 per cent). More would feel at least reasonably safe (72.5 per cent compared to 65.5 per cent).
Some users saw biometric identifiers as a better guarantee of access security than passwords. However, even with biometric identifiers, the most common reply was still that the user would feel only reasonably safe from unauthorised access to and use of their information. Just under one in five were unsure how safe such a site would be, whether logging in with a password or using a biometric identifier.

Analysis of the relationship between the two items found a consistent shift towards feeling safer using a biometric identifier than using a password-protected site (see Figure 21).
Figure 21 Safety when using a biometric access, by safety when using a password

Specifically:

> those who felt safe or very safe from unauthorised access when using a password-protected site were the most likely to feel the same way when using a biometric identifier

> only about one in seven of those who felt vulnerable, very vulnerable, or were unsure how safe they would be using a password-protected site, would feel very safe using a biometric identifier

> over one in three of those who feel very vulnerable using a password-protected site would feel very vulnerable using a biometric identifier

> very few (under five per cent) who gave other replies about their safety when using a password-protected site would feel very vulnerable using a biometric identifier
rating themselves as vulnerable—but not very vulnerable—using a biometric identifier was rare except among those who gave the same rating for safety when using a password-protected site

over half of those who were unsure how safe they would be when using a password-protected site were also unsure how safe they would be using a biometric identifier

the rest of those who were unsure about their safety using a password-protected site would mostly feel reasonably or very safe when using a biometric identifier.

Identity certification services

The qualitative discussions explored some specific approaches to providing users help to manage their online identity, such as:

a physical ‘key chain device’ that can be plugged into a tablet or laptop to confirm identity

a smartphone app that displays to a cashier, for example, a photo of the user to verify that they are the owner of the credit card or other payment medium being used

using an ‘identity certification’ (or verification) service.

The idea of these applications, devices or services was more attractive to those who had difficulty in keeping track of all of their logins and passwords.

Qualitative participants were told that an identity certification service could ask them each time they used it to access another site or service, what information, if any, held by the trusted service would be passed on. Some felt that being asked about this each time a third site was reached would be complicated or annoying. There was an ongoing tension between wanting access and wanting control, and users having to reconcile this every time they transact online.

Essential elements of an identity certification service

The online survey tested understanding and potential use of identity certification services, after providing a brief explanation of the concept.

The first question asked which (if any) of a list of undertakings about protection of personal information would users consider essential before they would use such a service. Respondents were also given the option of saying that none was essential. A later question asked whether they would be interested in using such a service if it provided all the guarantees they considered essential.

The question was designed to communicate the potential safeguards that could and should be offered by such a service. These safeguards emerged in the qualitative research. As a result, the undertakings described were designed to reassure users about:

the existence of security to deal with fears that a device might be lost or stolen and misused, or that a site might be hacked

the risk of consequent financial loss

concern about loss of personal control over the sharing of information between the certifying site and sites that were to be used.

The majority of respondents indicated that it would be essential for an identity certification service to let the user choose what personal information was passed on (58.9 per cent). They also indicated that it would be essential to reimburse any financial loss, if the identity certification site was hacked or personal details were captured and misused (55.9 per cent).
More than four in ten respondents also identified other undertakings:

> letting the user decide whether information passed on by the identity certifying site to the site being accessed is a one-off or not (46.5 per cent)
> the identity certification service letting the user know if the site to be accessed will pass on personal information to any other party (45.3 per cent)
> the identity certification service guaranteeing that no personal information will be transmitted to another site without the user’s permission (44.5 per cent)
> the identity certification service letting the user decide what information it can pass on to other sites (43.4 per cent).

A third (34.3 per cent) also indicated that it was essential for a certification service to remember the user’s preferences. Only 16.5 per cent said none of these undertakings was essential.

The major implication is that users would want a wide range of assurances about indemnity from loss. They would also want detailed control over the use made of their personal information when using an identity certification service—much more control than most users have with sites they currently use.

The next question asked whether, if the identity certification service undertook to do all the things the respondent considered essential, the respondent would; might; or definitely would not be willing to use the service. The responses are summarised in Figure 22.

**Figure 22 Willingness to consider using an identity certification service**

If all essential undertakings are given...
- **Would be willing to consider using**
  - 28.9%
- **Might be willing to consider using**
  - 55.4%
- **Would definitely NOT be willing to use**
  - 15.7%

*Base: Total sample, N=2,509*  
Q2CONb

If all the undertakings a respondent identified as essential were given, most respondents might be willing or would be willing to consider using an identity certification site. However, 15.7 per cent would not be willing to consider doing so, even if those undertakings were given. Just over one in four (28.9 percent) would be (rather than might be) willing to consider using the service.
Barriers to using an identity certification service

The strongest reservations expressed in the qualitative discussions were:

> fear of a site being hacked and then becoming vulnerable to abuse, including theft using credit card details

> concern that a central login service might use information gathered from activity across multiple sites as a commercial opportunity, resulting in spam online and possibly being targeted with marketing calls and mail offline.

Of particular concern was the potential for hackers to gain access to credit card details and to offline location information, such as street address and phone numbers, if these were held by a third party.

All respondents were asked ‘What, if anything, would stop you from being willing to use an identification service ... if it had all the features you believe are essential?’

Although over one in four (28.9 percent) had explicitly rejected even trying out such a site, only 6.8 per cent firmly maintained this rejection. This suggests that many respondents read the question as asking what would stop them using an identity certification service, once they had started doing so, while others read it as asking what would stop them from even trying such a service.

Security of the site, or lack of confidence that undertakings about privacy standards would be met, were the key themes behind many replies.

An underlying mistrust of any assurances given by suppliers of sites, services and applications again emerges. Nevertheless, most of these users were using multiple sites and services, despite such underlying mistrust.

These answers were consistent with the perceived drawbacks of third-party login services and their twin barriers:

> concern about the security from hackers of information given to the site

> lack of confidence that such a service would set and observe acceptable privacy settings and policies.

Two other barriers mentioned by a few respondents were:

> whether there were charges associated with using the service

> finding that signing up was inefficient or took too much effort.
Protecting users

Shared responsibilities
Previous research by the ACMA\(^5\) found that community participants saw distinct roles for themselves, industry and government in protecting their personal information online:

- individuals regard themselves as having primary responsibility for protecting their personal information online
- service providers and industry players were seen as mainly responsible for enabling a secure environment
- government has a role in providing general education and raising awareness.

Several themes emerged from discussion of what personal information would be provided to government or other organisations, and which types of organisations could be trusted to provide identity certification systems. The views expressed revealed some sharp divisions about what government should take responsibility for. Some recognised that the nature of the internet, with many providers being based in other countries, sharply limited the potential effectiveness of a legislative or regulatory approach. A few felt government was not the most appropriate custodian of personal online information. Others wanted support through government legislation and enforcement.

Given the range of different views expressed in the qualitative research, an item was included in the online survey to examine the role respondents believed that government should take in protecting internet users from misuse of their personal information.

The quantitative results are in Figure 23, which briefly summarises the response options. The full text of the question is in Appendix 2.

Government role
A majority of this sample of adult Australian internet users wanted government to take an active role. Half (50.7 per cent) wanted the government to enact and actively enforce legislation. Another 22.8 per cent wanted the government to be active in both educating and warning users, and encouraging providers to follow government-prescribed standards.

There was minority support for government limiting itself to educating the public about the risks, and publicising sites and services that violate standards.

A small group saw the government as having a minor role (4.4 per cent) or rejected government involvement outright (2.9 per cent).

Responsibility for protecting users

Respondents were asked who they thought should take responsibility. The replies to this question (shown in Figure 24) provide additional context for the previous item about the role of government.

The most common response by nearly half the sample (45.0 per cent) was ‘all of them equally’.

Figure 24 Locus of responsibility for protecting user information

Base: Total sample, N=2,509
Q7PRIVb

Note: ‘…’ indicates the option has been abbreviated—for the full text see Appendix 2
Responses indicated a hierarchy. The Australian Government was the least likely to be nominated as individually responsible for protecting user information. Endorsement of users and providers was about equally common. About 20 per cent of respondents gave more than one reply. While endorsement of ‘no-one can give real protection’ was fairly low (8.7 per cent), it was more likely to be endorsed by those aged 65 or more (17.2 per cent) compared to 5.8 per cent to 9.6 per cent for younger age groups.

Where to complain

Consumer protections relating to personal information are shared among a range of Commonwealth and state regulatory bodies, including the Office of the Australian Information Commissioner and the ACMA. Although a proportion of users believed they were informed about channels for complaint resolution, comments like the following were common:

- There must be a government authority that take such complaints and could provide support, but how you would go about it is a mystery to me.  
  *Group 9, 65+, mixed use*

- I’m sure there is an ombudsman out there somewhere  
  *Group 5: 30–49s, social more than transactional*

- This is a problem. As I have said before there seems to (be) no regulatory organisation for the Internet. I do not know of one.  
  *Group 9, 65+, mixed use*

One participant mentioned the difficulty for Australian authorities in controlling the activities of sites based in other countries. Consequently, for the majority of participants, there was uncertainty about where users could go to complain if they believed their personal information had been misused:

- I don't think there is anyone who provides support for a complaint about the internet. I am not sure how you would go about complaining about the internet and what happens on it.  
  *Group 9, 65+, mixed use*

Issues participants had sought to complain about in the past included:

- unwanted phone calls, which might result from information given online or might have nothing to do with internet use
- internet scams
- general complaints about online government services.

This uncertainty was further demonstrated by replies to a survey question about where respondents would go to complain about misuse of personal information online (see Figure 25). These replies were all verbatim and coded into the categories shown. The responses showed that:

- the most common response was contacting the supplier, but only 37.6 per cent said they would do this
- the next most common response was that they would not know (27.1 per cent); adding those who would do nothing brings the total to 30.2 per cent
- this was followed by simply unsubscribing from, or ceasing to use, the site or service (11.1 per cent).
Overall, the replies indicated that there was no clear channel for making complaints beyond complaining to the provider. The next most volunteered response was unsubscribing and stopping use of the service.

There was a general doubt that, even if users knew where to complain and did so, there would be effective follow through. Few satisfactory outcomes were reported by the small subset of participants who had attempted to lodge complaints.
Conclusions

Individuals have a nuanced view about their online identities. They have developed different identities, such as 'transactional' and 'social' and 'professional' identities, for different purposes. These identities are managed differently, based on the risks they see attached to them. Individuals also adopt strategies for managing the information they disclose about themselves in establishing their identity, and the information they disclose during the course of interactions. These strategies have implications for the reliance placed on particular categories of identity information, as well as the reliance on the data collected about individuals during transactions.

The findings point to a need for industry, government and citizens to find more targeted approaches to the challenges arising from the management of identifying data in a fully networked world.

Governments and industry have already been exploring ways to provide simpler, single channels to give internet users secure ways to establish who they are online. However, at this stage, most users do not find keeping track of their multiple online identifiers sufficiently difficult to accept the risks that they see inherent in single login services or a single identity certifier. Nor are many users sufficiently conscious of the risks resulting from many current strategies for coping with the task, such as reusing the same or very similar passwords, to necessarily look for a solution.

For citizens to overcome the barriers that arise from identity management practices and currently inhibit greater online engagement:

> Some will need to be persuaded that their current ways of keeping track of identifiers for multiple sites, services and applications leave them vulnerable.

> Many would need highly credible assurances that they will have control over how their personal information and digital footprints are used.

> Many would require much greater confidence than they currently have that such services are well protected against malicious intrusion.

Providers need to recognise users desire to keep certain online information private, and the strategies they are currently employing to achieve this, including withholding information or creating pseudonyms.
Appendix 1—
The qualitative discussion script

SECTION 1. DAY 1 OPENING STATEMENT
Welcome to the online discussion. The Australian Communications and Media Authority (ACMA) is conducting an online discussion about how people (and organisations) identify themselves to each other online. This research is being conducted to help ACMA and the Australian government understand how consumers find current practices and what you think about some new ideas for improving the process. Your participation in this online discussion is valuable and discussion outcomes will help the ACMA with future policy and regulatory decisions.

We recognise that this is a substantial commitment so we are offering an $80 ‘thank you’ to everyone who contributes to each set of questions.

OUR GUIDELINES
1. Log in at least once a day (twice if you can) and post your comments or material in response to activities you are asked to carry out.
2. People will have different reactions, feel differently about issues and have different experiences. We encourage you to comment on where your reactions and experiences are similar to those reported by others taking part, and where your reactions or experience are different.
3. Discussion will be moderated where necessary. Comments that contain offensive language or other content or that ridicule other participants or their ideas are likely to be removed.
4. We want you to spend up to 30 minutes each day on:
   - activities we suggest and sharing your reactions to those activities
   - responding to issues or questions we post
   - commenting on what other participants post.
We are aiming to have about 10 to 12 people actively contributing.
5. Even if you have no relevant experience of a particular area, please tell us about this and give us any thoughts you have on what others have to say.
6. If you appear to have not made a contribution we will send you a private email reminder. You will also receive emails to let you know that a new activity or new questions have been opened for you to look at.

Q1.1 Agreement to follow guidelines.
I agree to observe these guidelines and make an active contribution to the discussion.
1) Yes, I accept these guidelines and will contribute
If you do not agree please sign out with our thanks for considering taking part.

Respondents identified by first name and an initial.

For this project we do not ask participants to reveal details like gender and age, but focus on their pattern of internet use. However, we had details of participant demographics, which were accessible when conducting data analysis.

Set up as a poll question.
SECTION 2—WARM UP
To get started, please tell us all a bit about your internet use. That includes what you do online from a PC, tablet or mobile phone.

Q2.1 What do you do online with organisations (businesses, government organisations, providers of information or services) to get your personal business done?

Q2.2 And what do you do online that is social?
Q2.3 Some people only think of interacting on social network sites as social use of the internet. Others include anything from email correspondence with friends to sharing information, pictures or videos. Some people even treat interaction with business sites as a form of social exchange. How about you—do you draw a line between these? Where do you draw it?

Warm up and orient participants to each other

Was useful to see what sorts of things people mention as ‘doing business’ as against ‘being social’.

DAY 1 (CONTINUED) SECTION 3.
We all present different sides of ourselves to different audiences online (and offline as well). For example, on the phone, we often have a quite different tone of voice and style when answering at work from when we answer at home.

Have a look at the attached pdf. It shows the different information that Alice shares online with different types of organisation and individuals.

(To look at the pdf AND keep your discussion window open, try right clicking on the link then select ‘open in new window’ or similar from the options that come up. You should then be able to swap between this discussion window and the pdf while answering questions about it.)

You will need to have a pdf reader like Adobe Reader installed.

‘ALICE’ GRAPHIC EMBEDDED AS A PDF TO BE CLICKED OPEN.

Q3.1 How is this diagram similar or different to what you do about giving personal information online? In particular, what does Alice do that is different to what you do? Is there anything missing from the graphic?

Q3.2 What different ‘you’s’ do you present online?

Some people upload a photo, some use nicknames or pseudonyms.

How do you identify yourself in different contexts?

Q3.3 When do you prefer to be anonymous? When are you comfortable sharing information or images (name, photos that show what you look like or some things you do, or other information) that people you meet face to face would have access to? What makes the difference between when you share and when you do not?

This was expected to reveal more about the distinctions people make about what they will give out and how they classify organisations and individuals that they will share more or share less with.

(See ‘Alice’ graphic)
DAY 1 SECTION 3A. SHARING REACTIONS

Q3.4 Now we would like you to look back at what others had to say about Q3.1 to Q3.3. To do that quickly, click on the ‘Navigation’ button at the top left hand corner of this page, look down the drop down list and click on Q3.1.
If you are one of the early contributors there might not be contributions from more than a few others as yet. If less than six or seven others have answered so far, please take a break here and come back later today when more people have had time to post their contributions.
When you look over the answers, please look out for things that are different to the views you expressed.
Then just click Next Question until you reach this question again, and
1) Tell us below what you think about the different viewpoints you have noticed.
2) What (if anything) has prompted you to reconsider your own views?
3) Tell us all how you would explain the basis of your opinions so everyone can understand what is behind the positions you took.

Q3.5 1) Taking your reactions to what others have said into consideration, what are the main things that make you comfortable to provide more sensitive information online?
2) Is there anything you actively look for on a site that helps you feel more secure in giving information about yourself?
DAY 1 SECTION 4.

Q4.1 What types of information about yourself have services asked you to give online? ‘Services’ here includes websites and software or application downloads.

Q4.2 Tell us about some sites that have asked you for information about you that you decided not to give. The sorts of things we would like to know are:
  1) What sort of information was sought and what organisation wanted that information?
  2) What do you think they wanted it for?
  3) What made you decide not to provide that information?

Q4.2a If you can, please copy a link to one or more of these sites and paste it in here. If you cannot copy and paste any links, what can you tell us that will help us to find the site(s) you were thinking of?

Q4.3 Sometimes people give information about themselves which is not accurate.
  1) What (if anything) has prompted you to give information about yourself online that is not exactly true? That includes using a name that is different to yours, or describing yourself in ways that are not accurate.
  2) What makes you comfortable to share?
  3) What makes you cautious about sharing?

Q4.4 What difference (if any) does the device you are using make—whether you are going online from your desktop computer, a tablet or your mobile phone? What is different about how secure you feel going online from these different devices?

Q4.4a That is all for today. We hope you have enjoyed the discussion so far. Please log in again tomorrow for the next set of questions.

DAY 2 SECTION 4a SHARING REACTIONS AFTER ENOUGH HAVE POSTED THEIR RESPONSES.

Q4.5
  1) Now go back and see what other people have written for Q4.1 to Q4.4. Just like the last time we asked you to look back of less than five or six others have posted replies, please take a break and come back to this later when more people have had a chance to post their answers. Again, look for what is different to your own answers.
  2) Taking this into consideration, what do you think are the main things that influence your willingness to give personal information online?

Aimed at revealing any distinction participants make between different categories of personal information, and between different categories of online ‘others’ as well as prompting discussion of how they decide what to share or not share and with whom. At this stage have not introduced ‘trust’ as an issue—want to see if they bring this up.

Intended to reveal more about what generates mistrust—and whether people are sometimes just ‘having fun’
<table>
<thead>
<tr>
<th>DAY 2—SECTION 5</th>
</tr>
</thead>
</table>
| **Q5.1** Have a look at the attached video (http://bcove.me/hef5co8y) for a discussion about all the information we leave behind us and how companies use it to make money. This is sometimes called our ‘digital footprint’. (Don’t forget to turn on your sound).
| 1) What are your reactions to this video?
| 2) What (if anything) was a surprise?
| **PROBES TO PROMPT FURTHER DISCUSSION:**
| Q5.2 Now go back and see what other people have written for Q5.1. Again, please take a break if you find there are less than six or seven other contributions to look at?
| In the views expressed, what is different to what you said?
| Q5.3 Taking all that you have read into account,
| 1) which organisations do you trust online to only gather and/or pass on information about you with your permission?
| 2) how are the organisations you feel are more trustworthy different from those you don’t trust so much?
| Q5.4 People often accept terms and conditions without reading them carefully to see how information about them will be collected and used.
| 1) What (if anything) stops you from reading through such conditions?
| 2) Tell us about times when you have been annoyed or upset by the ways information about you has been used.
| 3) What (if anything) did you do about it? |
DAY 2 SECTION 6.
MANAGING PASSWORDS AND LOGINS

Q6.1 Many organisations want you to have a password to log in to their services and they can have a lot of different rules about the format of your log in and password.
1) What problems have you had managing your logins and passwords?
2) How do you keep track of them all?

Q6.2 Have a look at these examples of passwords that are easy to guess. (If you right click the link, you should be able to open it and keep this window open as well.)
http://soc.li/omTYCgB
What do YOU do to make it harder for others to guess or find your passwords?

Q6.3 How do you keep track of the different passwords you have?
Q6.4 Do you use any software program to help you manage your passwords (i.e. one where you enter a master password)? If you have, how well has this worked for you?

Q6.5 Please respond to each point below.
Have a look at the attached pdf that describes some ways of establishing who you are then tell us how you feel about using any of these.
1) What would be the advantages?
2) What worries would you have?

SHARE REACTIONS TO OTHERS:
Q6.7 Now go back and see what other people have written for Q6.1 to Q6.6. Again, if only a few have commented so far, please take a break and come back and look again later when more people have had time to post their thoughts.
In what people are saying, look for anything that seems to be different to what you said.
How would you explain your views to others who think differently to you so they can understand how you get to your position?

Q6.8 Taking everything into consideration, what concerns do you have about what you have to do to identify yourself online?

Trigger exploration of the care taken to use passwords that are not easily 'broken' or guessed
Specific probe for how people 'keep track'
See if people have used other forms of credential or are even aware of them—and explore perceived pros and cons of some prompted possibilities

(follows ‘Alice’ graphic at the end of this appendix)
DAY 3—SECTION 7 ACCESS SCENARIOS

Q7.1 Consider two different scenarios for how you would access a range of different services offered by different sites on the internet.

SCENARIO ONE—SEPARATE INDIVIDUAL REGISTRATIONS.
In one, every site is independent and requires you to establish an identity, pretty much as mostly happens now. Here is a typical sign-up page.
Tell us what, if anything, about signing up like this bother you?

Q7.2 SCENARIO 2: WORKING THROUGH A GATEWAY SITE
There are sites that are set up so you can have a single login and password (or even just one login without needing a password) to then deal with a lot of other organisations. You register once only and have a single login and password. After you log in, the gateway site then asks you:
1) which other sites you want to use,
2) for each one you use on that visit, what information you want passed on to that site, and
3) whether this is for this occasion only or if that site can keep a record of the information.
The first link goes to a service that gives access to several different Australian government departments.
http://australia.gov.au/service/register-for-online-services
The next two links offer services where you deal with a lot of different organisations.

View the next example as a video with sound turned on:
http://player.vimeo.com/video/43375136

View the next example as a web page:
http://openid.net/get-an-openid/start-using-your-openid/

Now share your reactions to them and how they compare with registering and logging in for each individual site.
Q7.3 What do you like about these different approaches to proving who you are?
Q7.4 What (if anything) do you dislike?
What (if anything) would worry you about using sites like these?
Q7.5 What questions would you want answered before you would be willing to use any of these different approaches to establishing your identity?

Introduce and gain initial reactions to the concept of a trusted identity manager compared to continued dealing with sites in isolation from each other.
<table>
<thead>
<tr>
<th>Question</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q7.6 Overall which approach do you prefer—individual sites operating independently, or a group of sites you access through a common gateway site? And what leads you to your preference?</td>
<td></td>
</tr>
<tr>
<td>PROBES TO PROMPT FURTHER DISCUSSION:</td>
<td></td>
</tr>
<tr>
<td>Q7.7 Now go back and see what other people have written about Q7.1 to Q7.6. (As before, take a break if there are less than six or seven other contributions and come back later when more have had a chance to post their contributions.) In the views that have been expressed, what differences can you see from what you have said? How would you explain your views to others so they would understand the basis for your position?</td>
<td></td>
</tr>
<tr>
<td>Q7.8 Taking the material you have viewed and other people’s answers into consideration, how do you now feel about trusting a single gateway site to look after securing your links to a lot of other sites?</td>
<td></td>
</tr>
<tr>
<td>Q7.9 How much would you trust a gateway site that was set up by a particular organisation (or government)? What would make you feel secure to use that single gateway site?</td>
<td></td>
</tr>
<tr>
<td>Q7.10 What would help you feel confident that YOU are the only one who can decide how your information is shared and used?</td>
<td></td>
</tr>
</tbody>
</table>
**DAY 4—SECTION 8**

**Q8.1 TRUSTED IDENTITY SERVICES**

Please read the two different scenarios below, then answer the questions about them.

**SCENARIO 1: MARIAN**

Marian uses her iPad to do most of her online transactions. She has a key chain from an ID provider which she plugs into her device when she wants to confirm her identity. The keychain itself contains no usable information and only works on Marian’s device. Used with a single, short PIN or password, the keychain allows her to permit sharing of different information about her depending on the type and sensitivity of the transaction or activity. For instance, she can simply confirm her age with supporting authentication from the government issuer of birth certificates or she can allow sensitive transactions like sharing her medical records with a specialist. All this without remembering complex passwords whenever and wherever it is convenient for her.

**SCENARIO 2: ALAIN**

As long as he has his smartphone, Alain often doesn’t need to use a plastic card to purchase goods. At many outlets, he ‘checks in’ using an identity application on his smartphone which allows the cashier to see his photo on the point-of-sale terminal to prove he is the same Alain who has sufficient funds in his account to pay for the goods. The application can also store other preferences such as body size, food preferences and whether he is happy for a staff member to approach him with special offers.

**Q8.2 How would you feel about using either of these?**

**Q8.3 Overall, which one would you prefer (or object to less)?**

1) SCENARIO 1—MARIAN

2) SCENARIO 2—ALAIN

**Q8.4 What makes it more appealing?**

**Q8.5 These services will pass on different information about you to different third parties.**

1) When would you want to give permission for this each time?

2) When would you be happy for the third party site to hold that information until it is updated or changed?

3) What would make the difference here?

---

**Further probe how people react to a ‘trusted identity’ manager and how this should be provided.**

**Q8.3 set up as a ‘poll’ question as in a survey.**
Q8.6 Services like Scenarios 1 and 2 could be managed in different ways. Among the options, think about the following:
1) Provided by an Australian government agency
2) Provided by a dedicated, not for profit organisation independent of the government
3) Provided by commercial organisations that would aim to make a profit from providing the service, and would compete with each other to provide the best service at the lowest price
4) The government regulating and auditing a not for profit or commercial supplier to ensure everything was being properly done.

What do you like or dislike about each of these options? On balance, which would you prefer and what leads you to say that?

PROBES TO PROMPT FURTHER DISCUSSION:
Q8.7 Now go back and see what other people have written about Q8.1 to Q8.6.
(As before when looking back, if less than six or seven others have posted their contributions, take a break and look back again later today when more have had a chance to contribute).
In the views others expressed, what were the differences from what you said?
What has given you food for thought about how well these options might work to make identifying yourself and controlling personal information both easier and more secure?
Q8.8 You could agree to a service like these giving a third party information about you once only, that the other party would then keep until you update it.

Or you could decide that you want to be asked for permission every time your information is passed on to that third party.

How do you now feel about when you would trust a third party to hold information you had given once, and when you would want to be asked each time?
DAY 4 SECTION 9
Q9.1 BEST PRACTICE
Have you come across any services online that you feel you can really trust to do three things—
1) to be sure you and only you can get into and use the service in your name
2) to allow you to keep private those things that you choose to be private,
3) do 1) and 2) without being too difficult to manage?
If you can name such a site or types of site, please describe that service and what makes it work well for you.
What, if anything, do you look for on such sites or about them that helps you feel more confident?
Q9.2 If you can, please copy in below a link that goes to that service—or to more than one if you have come across more that you feel ‘set the standard’ for others. (Or give us some other information that might help us find a site or sites you feel do these things well.)
### DAY 5—SECTION 10
### TRADE OFFS AND REDRESS
Information about you is being collected by services and applications you are using.

#### Q10.1
1) When would you believe you would know or be told that the information was being collected? When would you think you would not be told?
2) And how important is it for you to be sure you will be warned and given a chance to opt out before such information was collected?

Please respond to both points above.

#### Q10.2
How would you feel if you discovered such information was being collected without your permission?

Or that you had given permission when you accepted the ‘conditions of use’ for an app without reading all the detail?

#### Q10.3
Some people say they accept information being used without their explicit permission if they get enough value from using a site, like making it easier and more convenient to use, more tailored to their own interests, or even that it will get them marketing offers that they are really interested in.

When (if ever) have you been willing to make trade offs like this, and accept that personal information will be passed on even when you were not asked about it?

#### Q10.4
If you wanted to complain about information being passed on without your permission, or stop your information being collected and used,
1) What would you do?
2) Where could you make a complaint?
3) Who should provide support when you have a complaint about information that has been collected about you and how it is being used?
DAY 5—SECTION 11 BLUE SKY IDEAS—UK DIGITAL BY DEFAULT
Q11.1 Recently the UK government released its national digital strategy. Under the strategy, UK government services are now ‘digital by default’. The UK government now assumes that most people will do their business with government online, and provides other options only as backups for those who cannot or do not want to deal with the government online.

What effect do you think this would have on the way people living in the UK will have to manage their identity online?
Q11.2 What would be your concerns if this happened in Australia in the future?

Day 5—SECTION 12 WRAP UP
Q12.1 Reflecting on those five past days, do you think your views have changed? If so in what ways?

SIGNING OFF
This is the end of this online discussion. A big thank you! We greatly appreciate your contribution. We will send you each an email asking you to give us the details we need to forward you the $80 token of our appreciation for your time and contribution.

Possible areas of concerns expected to be Assisted access, Security issues, Losing data in the cloud, Possible skills needs, Trust of government, Balance of power and democracy

Pick up issues that might not have been covered.

Probe for concern about knowing who the other party is online

Pick up any other issues affecting trust in use of personal information given online.
Figure A1.1 Digital identities graphic (‘Alice’)
Figure A1.2 Informational and biometric identifiers graphic

Inside the figure are examples of informational identifiers—parts of our life history and other things private to us. Outside the figure are biometrics which identify us by characteristics or traits.
Appendix 2—
The online questionnaire

NOTES:
1) Code numbers of response options were not displayed on screen
2) Question numbers and titles were not displayed on screen
3) Responses preceded by a box allowed multiple responses; those preceded by a circle were exclusive
4) Text in block capitals preceded by ** was instructions to the programmer and was not displayed on screen.

Digital identities online questionnaire
Preamble
On behalf of the ACMA (Australian Communications and Media Authority), Taverner Research says ‘Thank you’ for taking part in this online survey.
The survey is about your experiences on the internet in managing your identity, identifying yourself to other users, and identifying other users.
It should take around 15 minutes for you to complete. This survey is best viewed in full screen.
Please read each question and follow the instructions to record your replies. Some questions may also ask you to type in a comment.
Please read the instructions and our privacy policy below before continuing.
Instructions
For each question you will be required to click one or more boxes or type in your answer in the box provided.
Please do not use the browser’s FORWARD and BACK buttons at any stage. Only use the NEXT button within the survey to move through.
If you would like to pause the survey to return to it later, simply click the SUSPEND button and then click on your original link to return.
Who are we/Privacy Policy
Taverner Research, an independent market research company abides by the Code of Professional Behaviour of the Australian Market & Social Research Society (AMSRS).
If you have any questions, please email survey@taverner.com.au.
If you want to check that Taverner is an accredited research company, please call the Australian Market and Social Research Society on 1300 36 4830.
Thank you in advance for taking part.
Please click 'Next' at the bottom of the screen to continue.
Demographics
SECTION 1: ABOUT YOU
To make sure we will get a good cross section of the community please answer the following questions about you
Q1DEM GENDER
I am ...
  o Male
  o Female
Q2DEM AGE GROUP
I am aged ...
  o Under 18—THANK AND TERMINATE
  o 18-19
  o 20-24
  o 25-29
  o 30-34
  o 35-39
  o 40-44
  o 45-49
  o 40-54
  o 55-59
  o 60-64
  o 65-69
  o 70 OR OVER
Q3DEM. I live in ...
  o 1. Sydney
  o 2. Elsewhere in NSW
  o 4. Melbourne
  o 4. Elsewhere in Victoria
  o 5. Brisbane
  o 6. Elsewhere in Queensland
  o 7. Adelaide
  o 8. Elsewhere in South Australia
  o 9. Perth
  o 10. Elsewhere in Western Australia
  o 11. Hobart or Launceston
  o 12. Elsewhere in Tasmania
  o 13. Darwin
  o 14. Elsewhere in the Northern Territory
  o 15. The ACT
  o 16. Not in Australia
IF 16 IN Q3DEM THANK & TERMINATE
Q1INT
Now some questions about the ways you use the internet—the things you do online for your own personal use (not for work).
Do you have logins and a password for:
> Carrying out tasks online like looking for information, ordering goods and services, paying bills, using government services and the like
  o 2. Engaging in social activities with other individual internet users like discussions, social networking, sharing photos and images, and making voice or video calls over the internet
  o 3. Manage logins, usernames and passwords for a child
  o 4. Manage logins, usernames and passwords for another adult
Q2INT
Do you use a mobile device (smartphone or tablet) to access the internet?
  o 1. Yes
  o 2. No
Q3INT. The number of different usernames and passwords I use is …
(PLEASE PICK THE FIRST ANSWER THAT YOU ARE SURE IS CORRECT)
  o 50 or more
  o At least 20
  o 3 At least 10
  o At least five
  o More than one
  o Only one
  o None
Q3INTa. Keeping track of my different user names, logins and passwords is …
**RANDOMISE DISPLAY IN ORDER 1-5 OR REVERSE
  o No problem
  o A minor nuisance
  o 3.Sometimes difficult
  o Often difficult
  o A major difficulty
Q3INTb. Keeping track of my different user names, logins and passwords is …
**RANDOMISE DISPLAY OF 1-5 OR REVERSE
  o 1. Getting much harder
  o 2. Getting harder
  o 3. Not getting either harder or easier
  o 4. Getting easier
  o 5. Getting much easier
Q3INTc Many devices, applications, browsers and sites let you choose the privacy settings that suit you.
In general, how confident are you that you can achieve the level of privacy you want by choosing your preferred privacy setting.
I am ...
**RANDOMISE DISPLAY OF 1-6 OR REVERSE**
- 1. Completely confident
- 2. Confident enough
- 3. Hope they work
- 4. Doubt whether they work
- 5. Sure they won’t work
- 6. Found them too hard and confusing to use

--------------
- 7. Never had the chance to choose my privacy settings

Q4INT Which (if any) of the following information are you willing to give to obtain access to an online service or offer that you want from GOVERNMENT organisations?
How about …
☐ Your full name
☐ Your date of birth
☐ Your gender
☐ The place where you were born
☐ Your home address
☐ Your phone number/s
☐ Your employer
☐ Your current location
> None of these

Q4INTa The BUSINESSES and NON GOVERNMENT organisations described in the list below vary in what you know about them.
Would you give AS MUCH personal information as you would give online to a GOVERNMENT organisation if the site, service or application came from …
CLICK ON ALL THAT APPLY.
☐ 1. An unfamiliar business or organisation that a friend has told you is safe to use
☐ 2. An unfamiliar business or organisation that has a high quality, professional site
☐ 3. An unfamiliar business or organisation with a reasonable quality site that offers something you really want to use
☐ 4. A business or organisation you already know and trust offline
> 5. A well known reputable business you have not previously dealt with
☐ 6. I would not give ANY of these as much personal information as I would give a government organisation
Q4INTb Which of the following would upset or annoy you so much you would stop using that site or service?
- 1. Private photos you post online being used in public ways
- 2. Reputation being damaged or compromised by private information being used in public ways
- 3. Your credit card details being stolen from a website where you used a credit card
- 4. Learning through media reports of a security breach that let hackers get to other user’s personal information
- 5. Your health information (such as medical conditions you have) being passed on without your permission
- 6. Being asked by a site or service to reset your login and password because of a security breach
- 7. Your email address being passed on without your permission so you get targeted marketing material online
- 8. Your home or mobile phone number that you gave when registering being passed on without your permission and used by telemarketers
- 9. Being told when you login that terms and conditions for how your information is used have been changed
- 10. None of these would upset or annoy me enough to stop using a site or service

Q1SEC Using a login and password to access reputable online services or an online device leaves me
**RANDOMISE DISPLAY OF 1-4 OR REVERSE**
- 1. Very vulnerable to unauthorised access to and use of information I have given
- 2. Vulnerable to unauthorised access to and use of information I have given
- 3. Reasonably safe from unauthorised access to and use of information I have given
- 4. Very safe from unauthorised access to and use of information I have given
- 5. Unsure how safe or vulnerable I would be

Q2SEC Using biometric data (fingerprint, iris scan, or voice) to access your device or reputable online services would mean you were ...
**KEEP IN SAME ORDER AS Q1SEC**
- Very vulnerable to unauthorised access to and use of information I have given
- Vulnerable to unauthorised access to and use of information I have given
- Reasonably safe from unauthorised access to and use of information I have given
- Very safe from unauthorised access to and use of information I have given
- Unsure how safe or vulnerable I would be
Q1PRIV When a site asks you for other personal information like your name, age, gender, date of birth, phone number, address, email address or where you work, when have you given incorrect information?
  ○ 1. When I want access but feel unsure how trustworthy the site is
  ○ 2. When the site gives no clear and easily found policy about assuring the security and privacy of information given
  ○ 3. When I simply do not see why the information is needed for me to use the site
  ○ 4. Never—I would rather not use the site than give inaccurate information
  ○ 5. Never—I have never felt the need to give inaccurate information

Q2PRIV Do you decide to not give information like your active email address or other personal information when asked to register to use a site if ….
  ○ 1. You cannot see how the information is needed by the site to provide what it offers, even if you are keen to get access
  ○ 2. The site does not appear professional—poor graphics, bad spelling and grammar, poor layout
  ○ 3. The site is not based in Australia
  ○ 4. You have not heard of the site
  ○ 5. The site does not have a padlock or other sign that it has met a security standard
  ○ 6. For some other reason (PLEASE SPECIFY)
  ○ 7. None of these will stop me using a site if I really want what it offers

Q3PRIV When registering or signing in for the first time to access or use different online sites and services, I am most likely to …
**RANDOMISE ORDER OF 1-4; KEEP 5 LAST**
  ○ 2. give different emails addresses, but otherwise keep identifying information similar as above
  ○ 3. give different answers to the same questions to protect myself and others from intrusion
  ○ 4. give different answers to the same questions because I dislike being asked for information that is not relevant or needed
  ○ 1. keep identifying information I give as similar as I can—I just reveal more to some sites or services than to others GO TO Q5PRIV
  ○ 5. None of these apply for me GO TO Q5PRIV

Q4PRIV What are your reasons for giving different answers to the same questions when registering for different sites? PLEASE TYPE IN YOUR ANSWER BELOW.
Q5PRIV When there are terms and conditions of use for a site, do you …
PLEASE GIVE ONLY ONE ANSWER.
  ○ 1. Always click through and read
  ○ 2. Usually click through and at least skim through looking for key points
  ○ 3. Usually at least check what assurances are given about protection of personal information
  ○ 4. Usually do not look unless it is in an easy to read font, clear and simple
  ○ 5. Usually tick and continue without reading it—what matters is how much I want access to that site
  ○ 6. It depends on what information I am asked to give
When we use the internet we leave information behind about ourselves and what we have done. Even some information about offline actions can be found by internet searches.

Some organisations gather this information together and supply it for commercial use without permission from those the information is about. This might include information that identifies us individually, or be anonymous.

How do you feel about the idea that personal information you have given and data about your activities can be gathered up and passed on for other organisations to use without your knowledge or permission?

Which of the following comes closest to you reaction?

**RANDOMISE DISPLAY OF 1-4 OR REVERSE, KEEP 5 LAST**

1. Really shocked or upset that this can happen
2. Surprised and a bit worried that this can happen
3. Aware of this is possible and a bit worried about it
4. Aware this is possible and simply accept that privacy does not really exist if you use the internet
5. Some other reaction (PLEASE DESCRIBE)

What role if any should government have in protecting you from misuse of personal information you have given online?

I think government should …

1. Take an active role: pass laws and regulations, set standards and enforce these with penalties for violations as well as actively educating the public about the risks and publicising sites and services that commit breaches
2. Set out standards and encourage providers to follow them as well as educating the public, but not waste time trying to police the issues as so many providers are not based in Australia and not subject to Australian law
3. Limit itself to active education of the public about the risks to their private information, and publicising sites and services that violate standards
4. Leave the main responsibility with individual users, as we are the ones who can make a difference by being careful and boycotting sites and services that offend
5. Stay out of the issue and leave it up to the individual users
6. None of these

Who is primarily responsible for protecting individual users from misuse of personal information they have given online?

☐ 1. Australian government
☐ 2. Providers of online sites and services
☐ 3. Users
☐ 4. All of them equally
☐ 5. No-one can give real protection
Q1CONa Some organisations offer you the option of logging onto their sites through your existing Facebook, Google, Microsoft, LinkedIn or similar site login and password. That way you do not have to register and create a new login, password or profile. Have you noticed invitations to do this?
  O 1. No
  O 2. Yes, but I have not used any
  O 3. Yes and I have used them

Q1CONb What reservations, if any, do you have about such offers?
**RANDOMISE THE ORDER OF 1-6; KEEP 7 AND 8 LAST**
  O 1. I don't have logins to the other sites
  O 2. I prefer to keep what I do on different sites separate—I don't want what I do being gathered together
  O 3. I don't think this will be secure enough
  O 4. I don't have enough control over what information about me is passed on or how it is then used
  O 5. I am worried that the site or service I use to identify myself will pass on information about me without my knowledge or permission
  O 6. I suspect the site I use to identify myself will collect and use information about how I use the other sites or services

O 7. I have other reservations [PLEASE DESCRIBE]
  O 8. I don't have any reservations

Q1CONc Which, if any, of the following advantages attract you to taking up such an offer?
**RANDOMISE ORDER OF 1-3; KEEP 4 & 5 LAST**
  O 1. It reduces the number of logins and passwords I have to keep track of
  O 2. It saves me from spending time registering for the new site
  O 3. I have more trust in the site I am already registered with
  O 4. It has other advantages (PLEASE DESCRIBE THESE)
  O 5. I don't find anything attractive about such offers
Let's say that you use a site—let's call it Site A—to verify your identity to other sites like Site B that you want to use. As a consequence, Site A might have quite a lot of information about you.

It would work like this:

Listed below are things that Site A could do to put you in control of how your personal information is used when accessing other sites and services like Site B.

Please read all the options below THEN pick ALL those undertakings by Site A that you would consider essential if you were to use the service.

> Site A lets you choose what personal information will be passed on to another site or service like Site B
> Site A remembers your preferences from the last time you used Site B, and asks you if you want to change them
> Site A lets you decide whether information about you will be passed on for this occasion only or permanently available to Site B
> Site A tells you whether Site B would pass on your information in any way to other organisations
> Site A asks you to decide what information Site B can pass on about you to other organisations
> Site A gives guarantees to reimburse any financial loss you incurred if Site A is hacked and your details captured and misused
> Site A guarantees that none of your information will be transmitted to any other site without your permission
> Site A operates under a code of practice which gives you options to resolve any problems or issues that may arise
> None of these are essential

If Site A undertook to do ALL the things I considered essential, I …

RANDOMISE DISPLAY ORDER 1-3 AND REVERSE

- 1. Would be willing to consider using Site A
- 2. Might be willing to consider using Site A
- 3. Would definitely NOT be willing to use Site A regardless of the assurances it offered
Q3CONc What, if anything, would stop you from being willing to use an identification service like Site A if it had all the features you believe are essential? PLEASE TYPE IN YOUR ANSWERS BELOW.

Q1COMP If you wanted to complain about a site or online service passing on personal information without your permission, or wanted to stop your information being misused, what would you do? PLEASE TYPE IN YOUR ANSWERS BELOW.

Q5DEM
To finish, a few other questions about you. Your answers will only be used to group together replies from people who give similar answers. Remember, we cannot identify you or report any of your answers in a way that can be linked to your name, your email address or anything else that might identify you or allow anyone to communicate with you. We do not have any of that information.

In my household, there are one or more children or young people who use the internet aged ....
- 1. Under 6
- 2. 6 to 11
- 3. 12-16
- 4. 16-17
- 5. 18-20
- 6. No children or young people in the household use the internet

**NO Q6DEM

Q7DEM EMPLOMENT STATUS
Are you now in paid employment or self-employed ...
- 1. Full time (35 hours a week or more)
- 2. Part-time (less than 35 hours per week)
- 3. No—not in paid work

IF 1 OR 2 IN Q7DEM GO TO Q9DEM

Q8DEM
Are you ...
- 1. Looking for paid work
- 2 Retired
- 3. Student
- 4. Home duties
- 5. Not working for other reasons
Q9DEM HIGHEST EDUCATION
Which of the following is the highest level of education you have completed?

- 1. Postgraduate degree
- 2. Undergraduate degree
- 3. Tertiary diploma, not from university
- 4. Finished the equivalent of MATRIC, HSC, VCE or Year 12 now
- 5. Finished technical, trade or commercial TAFE or college certificate
- 6. Finished intermediate, School Certificate or equivalent of Year 10 now
- 7. Some secondary school or technical or commercial education
- 8. Less than the above
- 9. Something else (PLEASE DESCRIBE)

Q10DEM HOUSEHOLD INCOME
We also need your answer to a question about your current financial situation. Your answers will help ACMA assess whether income level makes a difference to the ways that people answer other questions in this survey. Remember, we cannot link this information to you as an individual in any way, as we do not have any information that can identify you.

Roughly speaking, would your household’s total income from all sources before tax be …

- 1. Under $15,000 (about $288 per week or less)
- 2. At least $15,000 but less than $20,000 ($288 to $345 per week)
- 3. At least $20,000 but under $30,000 ($385 to $576 per week)
- 4. At least $30,000 but under $39,999 ($577 to $769 per week)
- 5. At least $40,000 but under $50,000 ($770 to $961 per week)
- 6. At least $50,000 but under $60,000 ($962 to $1,153 per week)
- 7. At least $60,000 but under $70,000 ($1,154 to $1,346 per week)
- 8. At least $70,000 but under $80,000 ($1,347 to $1,538 per week)
- 9. At least $80,000 but under $100,000 ($1,539 to $1,923 per week)
- 10. At least $100,000 but under $130,000 ($1,540 to $2,500 per week)
- 11. $130,000 or more (Over $2,500 per week)
- 12. Not sure
- 13. Prefer not to say

IF 1-11 IN Q10DEM GO TO Q12DEM

Q11DEM
Could you say whether your annual household income would be …

- 1. Under $50,000 per year ($962 per week)
- 2. $50,000 per year or more ($963 per week)
- 3. Not sure
- 4. Prefer not to say
Q12DEM LOTE
Do you speak a language other than English at home?
> 1. No
> 2. Yes

Q13DEM DISABILITY
Do you consider yourself to be a person with a disability?
That means any condition that has lasted or is likely to last six months of more AND restricts your life in some way. We will not ask anything further about the disability.
  o 1. Yes
  o 2. No
  o 3. Prefer not to say

Q99END. Thank you. That is the end of the survey. The survey was carried out by Taverner Research on behalf of the Australian Communications and Media Authority (ACMA). They thank you for your time.
Appendix 3—Quantitative sample

The target and achieved breakdown by location and gender is shown in Table 3. A more detailed breakdown by age and gender is shown in Table 2.

Targets were based on 2011 National Census by Capital City vs Rest of State with rows split as nearly as possible to be 50 per cent in each gender.

As the breakdowns show, the sample achieved a reasonably good match within the major States to the Capital City versus Rest of State population split so that weighting by these demographics was not required.

Table A3.1 Sample targets and sample obtained by location within major state

<table>
<thead>
<tr>
<th>Location</th>
<th>TARGET Male</th>
<th>Female</th>
<th>ACHIEVED Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sydney</td>
<td>258</td>
<td>258</td>
<td>259</td>
<td>261</td>
</tr>
<tr>
<td>Other NSW</td>
<td>157</td>
<td>157</td>
<td>160</td>
<td>158</td>
</tr>
<tr>
<td>Total NSW</td>
<td>413</td>
<td>415</td>
<td>419</td>
<td>419</td>
</tr>
<tr>
<td>Melbourne</td>
<td>224</td>
<td>226</td>
<td>241</td>
<td>232</td>
</tr>
<tr>
<td>Other Victoria</td>
<td>88</td>
<td>88</td>
<td>74</td>
<td>82</td>
</tr>
<tr>
<td>Total Victoria</td>
<td>313</td>
<td>313</td>
<td>315</td>
<td>314</td>
</tr>
<tr>
<td>Brisbane</td>
<td>121</td>
<td>121</td>
<td>102</td>
<td>103</td>
</tr>
<tr>
<td>Other Queensland</td>
<td>116</td>
<td>116</td>
<td>136</td>
<td>136</td>
</tr>
<tr>
<td>Total Queensland</td>
<td>237</td>
<td>237</td>
<td>238</td>
<td>239</td>
</tr>
<tr>
<td>Adelaide</td>
<td>73</td>
<td>73</td>
<td>73</td>
<td>69</td>
</tr>
<tr>
<td>Other South Australia</td>
<td>27</td>
<td>27</td>
<td>26</td>
<td>32</td>
</tr>
<tr>
<td>Total South Australia</td>
<td>100</td>
<td>100</td>
<td>99</td>
<td>101</td>
</tr>
<tr>
<td>Perth</td>
<td>68</td>
<td>68</td>
<td>94</td>
<td>81</td>
</tr>
<tr>
<td>Other West Australia</td>
<td>57</td>
<td>57</td>
<td>23</td>
<td>45</td>
</tr>
<tr>
<td>Total West Australia</td>
<td>125</td>
<td>125</td>
<td>117</td>
<td>126</td>
</tr>
<tr>
<td>Total Tasmania</td>
<td>29</td>
<td>29</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>Total ACT</td>
<td>20</td>
<td>20</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>Total NT</td>
<td>12</td>
<td>12</td>
<td>11</td>
<td>18</td>
</tr>
<tr>
<td>TOTALS</td>
<td>1,249</td>
<td>1,251</td>
<td>1,249</td>
<td>1,260</td>
</tr>
</tbody>
</table>
### Table A3.2 Target and obtained sample by age group and gender within state or territory

<table>
<thead>
<tr>
<th>Segment</th>
<th>TARGET</th>
<th>Female</th>
<th>ACHIEVED</th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSW 18-24</td>
<td>63</td>
<td>63</td>
<td>64</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>NSW 25-34</td>
<td>93</td>
<td>92</td>
<td>93</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>NSW 35-44</td>
<td>87</td>
<td>87</td>
<td>90</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>NSW 45-54</td>
<td>80</td>
<td>79</td>
<td>80</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td>NSW 55-64</td>
<td>56</td>
<td>57</td>
<td>57</td>
<td>58</td>
<td></td>
</tr>
<tr>
<td>NSW 65 or more</td>
<td>34</td>
<td>36</td>
<td>38</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>VIC 18-24</td>
<td>48</td>
<td>48</td>
<td>48</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>VIC 25-34</td>
<td>71</td>
<td>70</td>
<td>72</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>VIC 35-44</td>
<td>66</td>
<td>66</td>
<td>66</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>VIC 45-54</td>
<td>60</td>
<td>60</td>
<td>60</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>VIC 55-64</td>
<td>43</td>
<td>43</td>
<td>44</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>VIC 65 or more</td>
<td>25</td>
<td>26</td>
<td>26</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>QLD 18-24</td>
<td>36</td>
<td>37</td>
<td>36</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>QLD 25-34</td>
<td>53</td>
<td>54</td>
<td>54</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>QLD 35-44</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>QLD 45-54</td>
<td>46</td>
<td>45</td>
<td>46</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>QLD 55-64</td>
<td>33</td>
<td>32</td>
<td>33</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>QLD 65 or more</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>SA 18-24</td>
<td>15</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>SA 25-34</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>SA 35-44</td>
<td>21</td>
<td>21</td>
<td>2</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>SA 45-54</td>
<td>19</td>
<td>19</td>
<td>18</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>SA 55-64</td>
<td>14</td>
<td>13</td>
<td>14</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>SA 65 or more</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>WA 18-24</td>
<td>20</td>
<td>19</td>
<td>20</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>WA 25-34</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>WA 35-44</td>
<td>26</td>
<td>27</td>
<td>18</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>WA 45-54</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>WA 55-64</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>WA 65 or more</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>TAS 18-24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>TAS 25-34</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>TAS 35-44</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>TAS 45-54</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>TAS 55-64</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>TAS 65 or more</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ACT 18-24</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>ACT 25-34</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>ACT 35-44</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>ACT 45-54</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>ACT 55-64</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>ACT 65 or more</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NT 18-24</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>NT 25-34</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>NT 35-44</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>NT 45-54</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>NT 55-64</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>NT 65 or more</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>TOTALS</td>
<td>1,249</td>
<td>1,251</td>
<td>1,249</td>
<td>1,260</td>
<td></td>
</tr>
</tbody>
</table>
Targets were based on ABS data on adult internet users in Australia, 2011 with a notional split by gender as close as possible to 50 per cent within each row.

As is usually the case with survey samples, and particularly online panel samples, the sample had a higher percentage of respondents with a university degree (33 per cent) than would be expected in the adult population (22 per cent for Australians aged 15 and over, and 27 per cent for Australians aged 15 and over who have used the internet). It appears that the sample over-represents those with higher levels of education. However, it is difficult to identify reliable targets for the education distribution of those who use the internet, so no weighting has been applied.

A summary of the highest level of education reported by the sample is given in Table A3.3.

<table>
<thead>
<tr>
<th>Table A3.3 Highest completed educational qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postgraduate degree</td>
</tr>
<tr>
<td>Undergraduate degree</td>
</tr>
<tr>
<td>Tertiary diploma, not from a university</td>
</tr>
<tr>
<td>Finished the equivalent of Year 12 now</td>
</tr>
<tr>
<td>Finished technical, trade of commercial TAFE or college certificate</td>
</tr>
<tr>
<td>Finished or equivalent to Year 10 now</td>
</tr>
<tr>
<td>Some secondary school or technical or commercial education</td>
</tr>
<tr>
<td>Less than the above</td>
</tr>
<tr>
<td>Something else</td>
</tr>
</tbody>
</table>

Almost half the sample reported working full time and almost two in three worked full time or part time (see Table A3.4).

<table>
<thead>
<tr>
<th>Table A3.4 Employment status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work full time</td>
</tr>
<tr>
<td>Work part time</td>
</tr>
<tr>
<td>Not in paid work</td>
</tr>
<tr>
<td>Retired</td>
</tr>
<tr>
<td>Home duties</td>
</tr>
<tr>
<td>Unemployed seeking paid work</td>
</tr>
<tr>
<td>Studying</td>
</tr>
<tr>
<td>Not working for another reason</td>
</tr>
</tbody>
</table>

Those not working were mostly retired or caring for their household, with just under 6 per cent of the sample unemployed, about 5 per cent studying and 4 per cent not working for other reasons.

---

Table A3.5 Household income

After additional probe

<table>
<thead>
<tr>
<th>Income Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under $50,000 pa</td>
<td>31.1 per cent</td>
</tr>
<tr>
<td>$50,000 of more</td>
<td>52.7 per cent</td>
</tr>
<tr>
<td>Not sure</td>
<td>3.2 per cent</td>
</tr>
<tr>
<td>Refused to say</td>
<td>12.9 per cent</td>
</tr>
</tbody>
</table>

Before additional probe

<table>
<thead>
<tr>
<th>Income Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under $15,000 pa</td>
<td>3.9 per cent</td>
</tr>
<tr>
<td>$15,000 to &lt;$20,000 pa</td>
<td>4.0 per cent</td>
</tr>
<tr>
<td>$20,000 to &lt;$30,000 pa</td>
<td>5.8 per cent</td>
</tr>
<tr>
<td>$30,000 to &lt;$40,000 pa</td>
<td>8.4 per cent</td>
</tr>
<tr>
<td>$40,000 to &lt;$50,000 pa</td>
<td>7.7 per cent</td>
</tr>
<tr>
<td>$50,000 to &lt;$60,000 pa</td>
<td>7.8 per cent</td>
</tr>
<tr>
<td>$60,000 to &lt;$70,000 pa</td>
<td>6.0 per cent</td>
</tr>
<tr>
<td>$70,000 to &lt;$80,000 pa</td>
<td>6.5 per cent</td>
</tr>
<tr>
<td>$80,000 to &lt;$100,000 pa</td>
<td>9.8 per cent</td>
</tr>
<tr>
<td>$100,000 to &lt;$130,000 pa</td>
<td>10.5 per cent</td>
</tr>
<tr>
<td>$130,000 or more pa</td>
<td>9.0 per cent</td>
</tr>
<tr>
<td>Not sure</td>
<td>4.3 per cent</td>
</tr>
<tr>
<td>Refused</td>
<td>16.1 per cent</td>
</tr>
</tbody>
</table>

There was a wide range of income levels (see Table ), but a substantial number either preferred to not report the household income (16 per cent) or said they did not know what it was (4 per cent). An additional 4 per cent were willing and able to indicate whether the annual household income was below $50,000 pa or was $50,000 or more.

Almost one in five (19.4 per cent) reported they spoke a language other than English at home (somewhat above the total population level of about 16 per cent reported by the ABS), and 14.5 per cent reported they had a disability that had lasted at least six months and interfered with their daily activities, well below the 33 per cent reported by the most recent national Health Survey. Four in 10 (39.7 per cent) lived in a large city (over one million population) closely matching the adult population.