Australian Government | acma

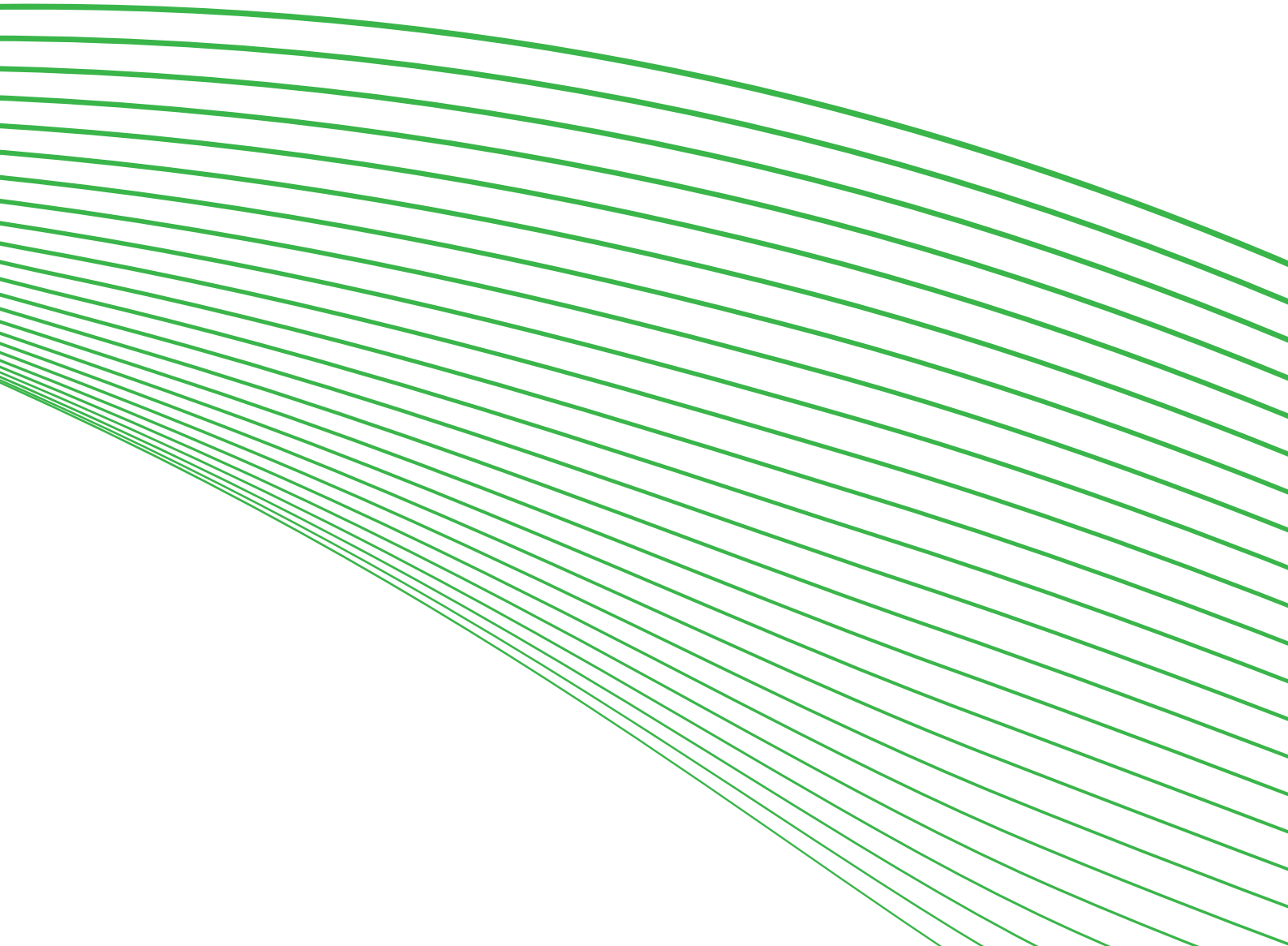
Australian Communications and Media Authority

researchacma

Managing your digital identity

Digital footprints and identities research
Short report 1

NOVEMBER 2013



Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

Contents

Summary

Who are you online?

Most Australians have multiple digital identities, managing between five and 50 login and password combinations to conduct their day-to-day online activities, according to recent ACMA research.

Half the participants in the research said they sometimes find it difficult to manage their online identities and passwords.

While they are generally comfortable with providing details like their date of birth and phone numbers to government agencies, they resist providing personal data to other organisations and services.

Some Australians respond to unwelcome demands for information by going elsewhere. But a significant number (47 per cent)—and an even greater proportion of younger Australians—would provide inaccurate or misleading information about themselves to use a site, application or service.

Australians also have three distinct online 'identities':

- a 'transactional identity'—the minimum information required to make a specific task work with an organisation or service such as a financial institution, insurance company, online retailer or government agency
- a 'social identity'—developed on social networking services and including personal data shared across online communities
- a 'professional identity'—locatable online with a positive image of their skills, experience or business offering.

Most did not recognise the strategies they have adopted to manage their logins and passwords are risky, or they are simply not worried about it.

But there are a number of strategies that can help Australians take control of their online identity management and enhance their security and privacy. These are:

1. **Conduct a personal identity audit to understand:**
   - who the information is shared with
   - what the information will be used for
   - whether the personal data is discarded once it is not required
   - if the personal information has commercial value, is the trade-off worth it?
2. **Use privacy enhancing tools.**
3. **Be informed about how to protect your digital privacy.**

This short report, which looks at how we manage our identities online, is drawn from the qualitative and quantitative findings of the *Digital footprints and identities* research. The research aimed to understand how Australians act and react to the challenges of digital identity when they are online.

Key findings

Logins and passwords—taking the easy and risky options

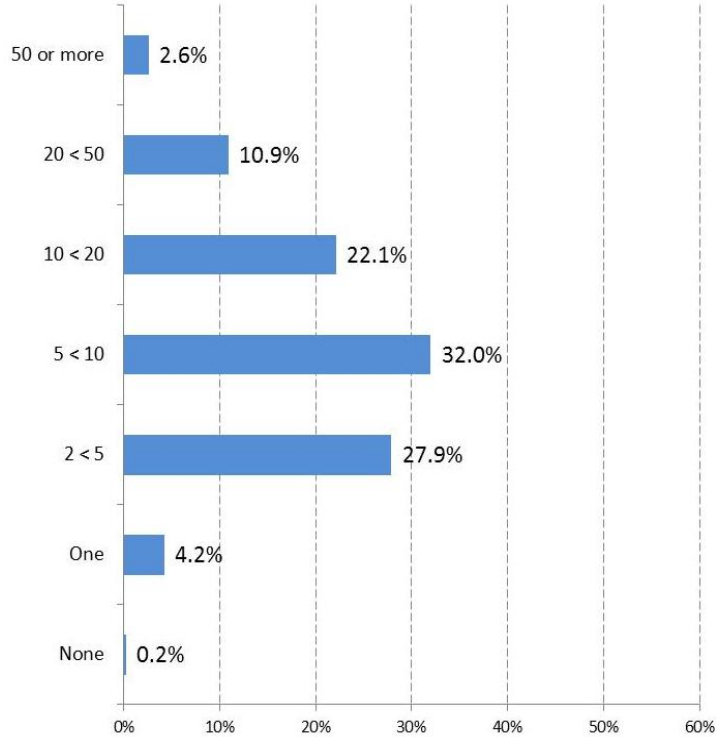
The research asked a nationally representative sample of Australians:

> how many unique logins and passwords they had

> what demands managing the identifiers imposed on their online experience.

The results show seven in ten managing more than five identifiers and 13 per cent managing 20 or more (see Figure 1).

Figure 1 Reported number of unique identifiers

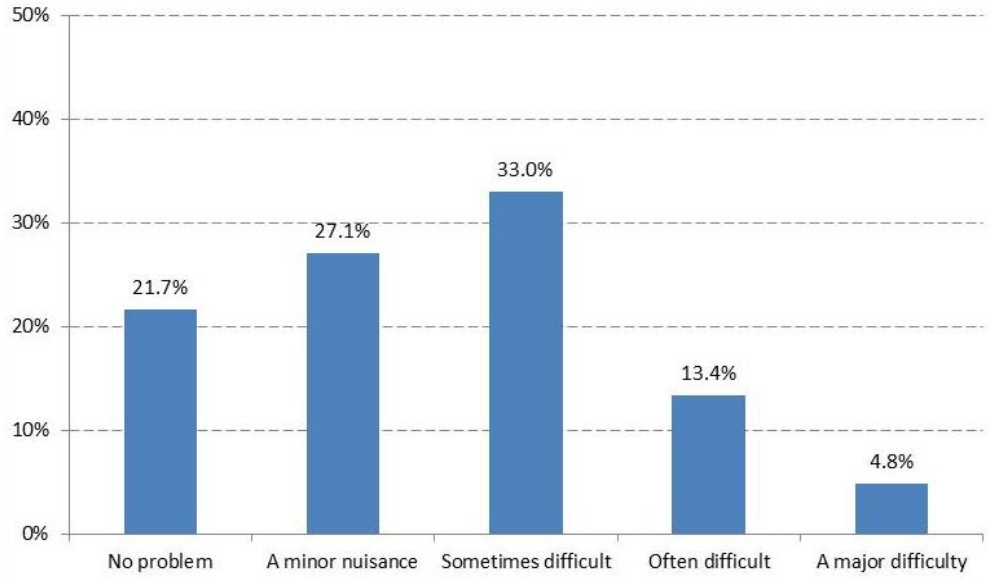


Base: Total sample, N=2,509

Keeping track

Respondents were then asked how easy or difficult they found keeping track of their logins and passwords. Figure 2 shows that around half (48.8 per cent) did not find this management task more than 'sometimes difficult', saying it is either 'no problem' or a 'minor nuisance'. However, around half could find managing logins and passwords challenging, with 33 per cent saying that it is 'sometimes difficult' and 18.2 per cent that it is 'often difficult' or 'a major difficulty'.

Figure 2 Managing passwords and logins, level of difficulty



Base: Total sample, N=2,509

Increased use of online banking, shopping and social communities means that users are frequently required to register their details and provide authenticating information. This authentication is typically a login and password. Participants in the qualitative research talked about how they keep track of this critical information by:

- making paper lists
- memorising systematic rules to generate passwords ('theme and variations')
- using online identity management services.

Perceptions varied on whether or not the demands of managing the identifiers was a negative aspect of their online experience.

> Different websites have different requirement(s) or rules of the format of my login and password. Therefore I need to create many different logins and passwords and it's so hard to remember all.
> *Group 4: 30–49, transactional more than social*

> I have a book with all my passwords ... which I do not keep near my computer and each site has a different password
> *Group 9: 65+, mixed use*[1]

Understanding the risks

There are growing concerns about the vulnerability of the login/password form of identity authentication. Deloitte recently warned that 90 per cent of login/password combinations may be vulnerable to hackers.[2]

In May 2013, Google announced a plan to protect itself and its customers from the increased capabilities of what it calls 'the bad guys'. This will eventually require Google's customers to have stronger forms of authentication than a single

[1] The nine groups of participants in the qualitative research were grouped into age cohorts and by their type and level of use of the internet between transactional and social use.

[2] DeloitteTMT Predictions 2013, P@$$1234: the end of strong password-only security, 2013.

login/password to access any account.[3] These could include device-based identity tokens and SMS confirmations.

In combination, the results from the discussion groups and the national survey suggest that:

- users did not recognise that the strategies they have adopted to simplify the task leave them vulnerable
- they are not sufficiently concerned about the risks to give up the convenience of simple coping strategies, such as repeated use of the same password.

Constructing multiple identities

When it comes to sharing information about who they are and what they do, the research findings show that Australians put thought and care into the construction of their digital identities. They reveal or conceal personal data based on what they deem appropriate for a specific interaction.

Research participants had a consistent message—that information about the administration of their day-to-day lives should be shared only carefully and narrowly. This 'transactional' identity' is seen as multiple sets of information that are the minimum required to make a specific task work. Underpinning this kind of identity is an implied individual contract of trust between internet users and an organisation or service. This may be, for example, a financial institution, insurance company, online retailer or government agency.

Social networking services, blogging and micro-blogging activities, and the popularity of online dating, mean that most Australians in all age groups and demographics are now sharing some form of personal data across online communities. The concern among research participants for this 'social identity' data was that information considered to be a risk to reputation or personal safety should not be able to be found via a search engine. This included photos of themselves, family or friends, and dating profiles.

In contrast, with their 'professional identity', internet users want to be locatable online to provide people they don't already know with a positive image of their skills, experience or business offering.

Trusting the government

Nearly all discussion group participants felt safer giving personal information to government organisations (for example the Australian Taxation Office, Centrelink and Medicare) than to commercial or non-government organisations. Government organisations such as these are thought to pay considerable attention to data security, obtain extensive information about individuals from other organisations, and share some of this with each other.

Given the relatively high level of trust in government organisations expressed in the discussion groups, respondents in the national survey were asked what information they would provide to gain access to an online government service or offer.

Full name, gender and date of birth appeared to be the least sensitive, with at least three in four willing to provide them. Around half the respondents said they would provide their home address, phone number(s) and place of birth. From there, trust fell sharply with about only 28 per cent willing to provide their current location and over 20 per cent agreeing to provide employment details.

[3] Google, Stronger Consumer Authentication - 5 year report, 2013.

> I feel most comfortable with large government agencies handling my data, as they have the most to lose through the mishandling of it.
> *Group 5: 30-49s, social more than transactional*

When dealing with other organisations, and private businesses in particular, participants in the qualitative study explained that they relied on a range of indicators to decide whether a provider could be trusted with personal data. These included:

- whether they had a relationship with the business offline
- the reputation of the business
- whether the site appeared fully professional
- whether the site had some symbol of certification as a genuine and trustworthy site or used stronger encryption.

A common view was that if there was not a good reason for the request, respondents were reluctant to supply information about themselves.

The survey respondents were asked if they were willing to share as much information with businesses or other non-government organisations sites, services or applications as they were with government organisations.

Figure 3 Organisations respondents would give the same personal information they would give a government organisation

Base: Total sample, N=2,509

Almost of half of those surveyed would not give any type of organisation as much information as they would give a government organisation (see Figure 3). Only one option—being known and trusted offline—won as much trust as a government organisation from nearly half of the sample (46.8 per cent). Being a well-known and reputable business that the respondent has not previously dealt with would lead about one in four to give the provider as much information as they would give a government organisation. The other potential 'triggers for trust' only persuaded about eight per cent of the sample. These results indicate widespread caution about providing identifying personal information to many providers of sites, services and applications.

Telling the truth? Defensive inaccuracy

Giving inaccurate personal information was a strategy reported by the qualitative research participants. They made use of 'defensive inaccuracy' when they wanted to access a particular site, service or application but felt that excessive information was required to register. Without the option of being anonymous, users seek what might be termed 'pseudonymity'. This involves using false, inaccurate or different versions of one or more of their real name, their age or date of birth and their email or physical address. However, some participants (mostly those aged over 50) said they were completely unwilling to provide inaccurate information as a way around the problem.

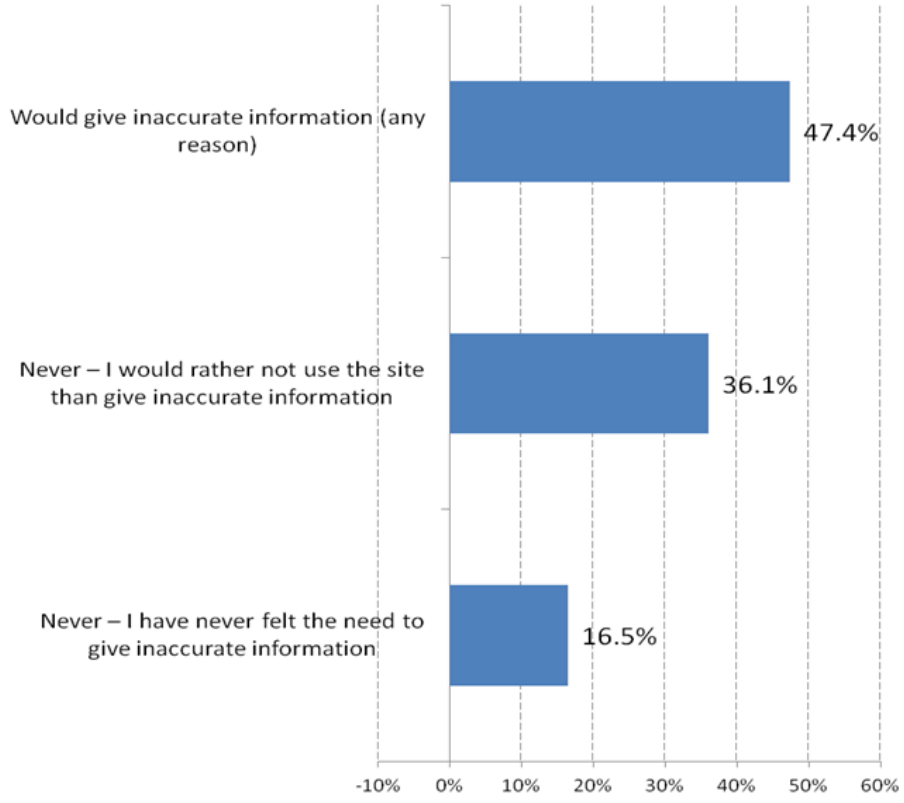
> I indeed [have] given information online that is not accurate and I will gladly explain why I have done so:
>
> 1. To protect my identity, location, and friends, family.
> 2. When people start asking me all the wrong questions and can't explain why.
> 3. When I think I am talking to some village's 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*

Survey respondents were asked whether they would give inaccurate information about themselves in different circumstances that emerged from the qualitative discussions. Figure 4 shows the percentage of respondents endorsing each justification for giving inaccurate information.

Survey respondents appeared to be sharply divided on this issue with:

- just under half (47 per cent) willing to acknowledge giving inaccurate information in at least one situation
- about one in three (36 per cent) reporting they would rather not use a site than give inaccurate information
- one in six (17 per cent) said that they had never felt the need to give inaccurate information.

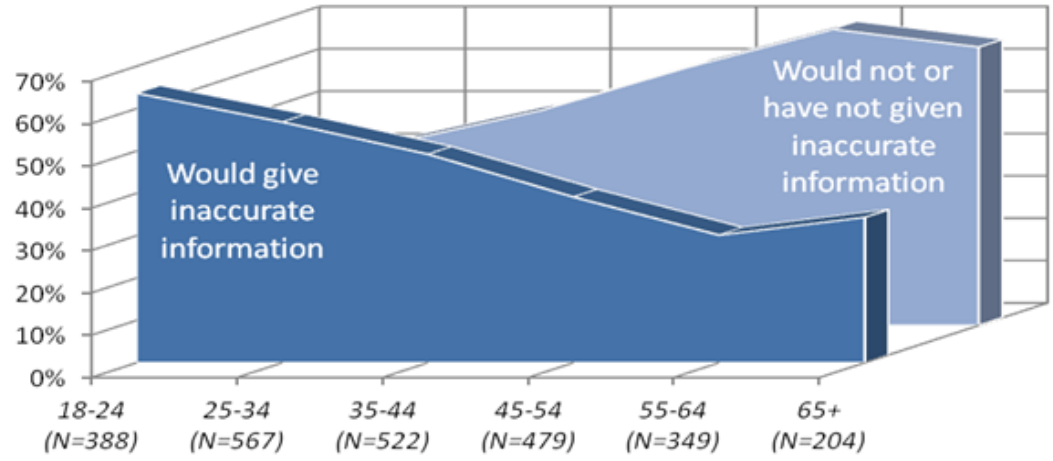
Figure 4 Giving inaccurate personal information



Base: Total sample, N=2,509

The national survey demonstrated that responses to requests for unnecessary information change significantly with age (see Figure 5). The percentage who reported a willingness to give inaccurate information was highest for those aged 18–24 (64 per cent) and fell to between 30 per cent and 40 per cent in the older age groups.

Figure 5 Willingness to give inaccurate personal information, by age group



Base: Total sample, N=2,509

The most widely endorsed triggers for providing inaccurate information were:

> seeing the information requested as unnecessary

> not being sure the site asking for the information can be trusted.

The lack of a clear and accessible policy about security and privacy was a less significant reason, but would still lead one in four of those aged under 35 to give inaccurate information.

Deciding who to trust

The qualitative research participants were asked what aspects of the content and the look and feel of a website they took into account when deciding on how much it could be trusted.

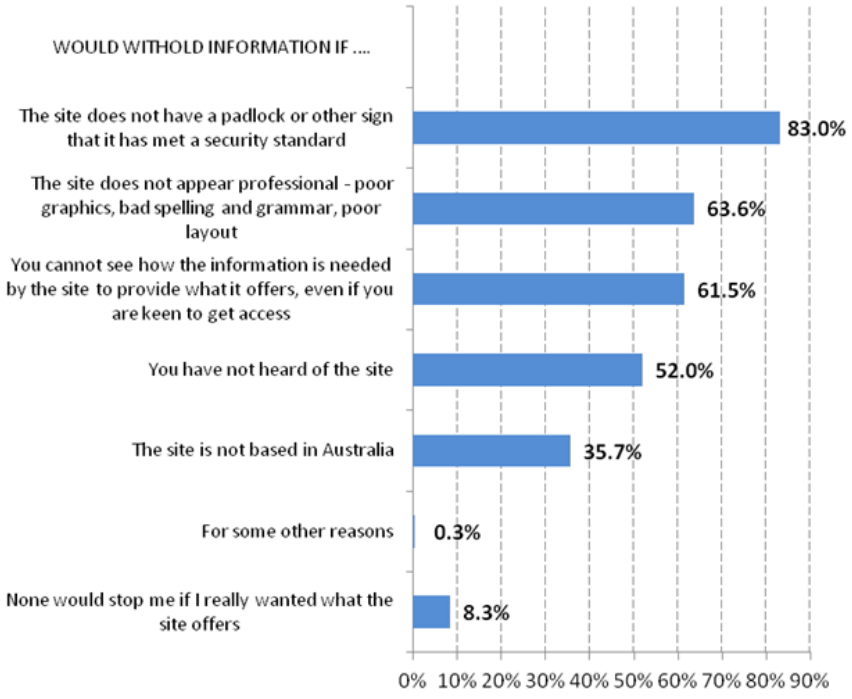
Sites that lack a padlock or other security assurances prompted most of the sample to say they would withhold personal information (83 per cent).Over half the sample would withhold personal information if:

> the site did not appear professional, for example, had poor graphics, bad spelling and grammar, or poor layout

> the information the site asked for was not relevant to the offering

> the website was unknown to them.

Figure 6 Circumstances in which personal information would be withheld



Base: Total sample, N=2,509

These results indicate that many internet users in Australia are using a mixture of defined knowledge (digital and general literacy) and personal value judgments to make decisions about who to trust with their personal information.

A website not being based in Australia would be a barrier for one in three of all those surveyed. However, this figure rose sharply to 56 per cent of those aged 65+.

Staying in control

The research shows that Australians have developed a range of ad hoc and sometime risky strategies to feel in control of how their personal data is used online. But there are a number of strategies that can help Australians take control of their online identity management and enhance their security and privacy. They include:

1. Conduct a personal identity audit

Consider all the activities you do on a PC, tablet or smartphone and make sure you understand:

- who you are sharing your information with?
- what the information will be used for?
- whether the personal data is discarded once it is not required
- if your personal information has commercial value, is the trade-off worth it?

2. Use privacy-enhancing tools

A range of privacy-enhancing tools (PETs) has now emerged to meet consumer demand for the improved management and protection of personal data. They include personal data vaults, anonymisers and personal data monitors. Some are cloud-based while others work through a smartphone application or browser plug-in.

3. Be informed

As a digital citizen, make sure you know how to protect your digital privacy. See www.cybersmart.gov.au/digitalcitizens for more information.

About this research

This is the first short paper in a series of three discussing the findings of the *Digital footprints and identities* community attitudinal research.

Taverner Research completed the project for the ACMA in two stages:

- qualitative research using participation in nine online forums in November and December 2012
- a quantitative survey of a nationally representative sample of 2,509 Australian adults in March 2013.

research**acma**

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. It is aimed at understanding behaviour and attitudes to the:

- creation, use and management of an individual's digital identity
- management of digital information online
- the identification of what triggers an individual's willingness to provide personal information online.

research**acma** 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 is the first of three short papers that contribute to the ACMA's digital society research theme, which aims to identify the regulatory settings and interventions to assist citizens in protecting their personal information and digital data in an information economy. The other short reports and the full report, *Digital footprints and identities,* can be found on the ACMA website.

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

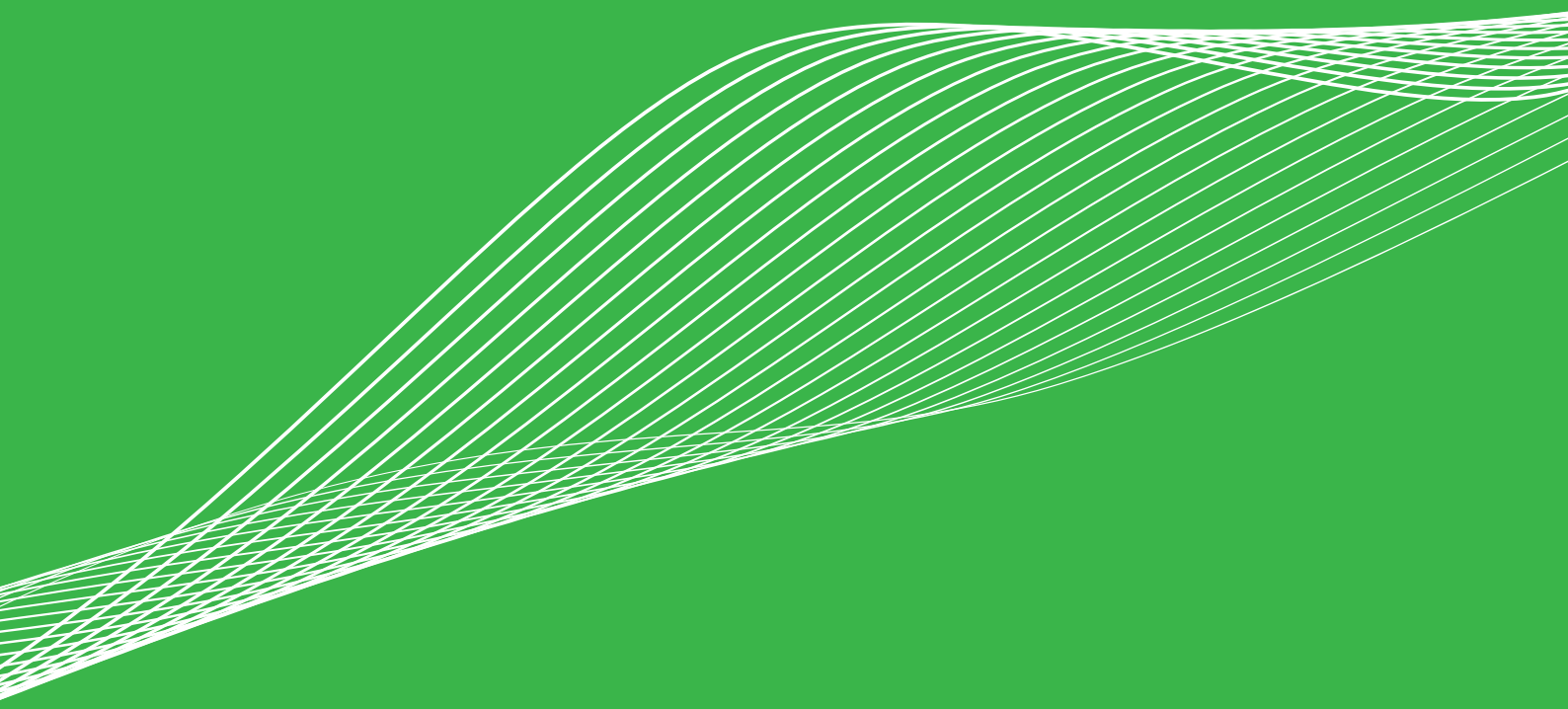
T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

researchacma



acma.gov.au