Australian Government

acma

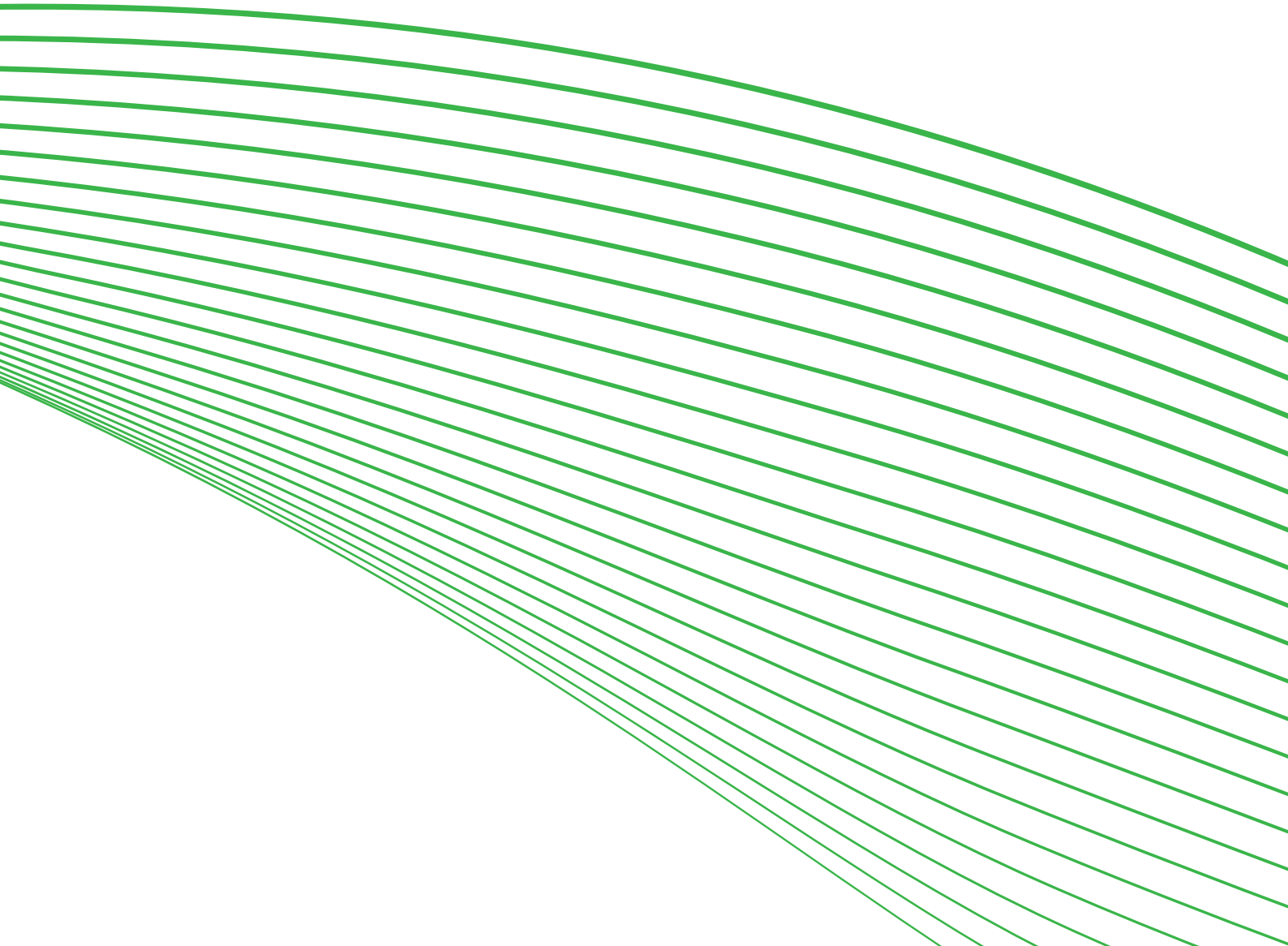
Australian Communications and Media Authority

researchacma

Sharing digital identity

Digital footprints and identities research
Short report 2

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 **1**
Protecting personal data 1
The three digital identities 1
Ramifications for providers of online services 1

Key findings **3**
Three digital identities—changing with context 3
Hopeful and confident about privacy settings 3
Privacy policies—readability and trust 4
Reactions to the vulnerability of digital footprints 5
Strong reservations about third-party identity services 7
Transparency may encourage trust, even after a critical incident 7

About this research **9**
researchacma 9

Summary

Protecting personal data

Australians want control of information about themselves held by providers of online services, sites and applications because they do not fully trust the online world to look after their digital identities.

Data collected for a single activity today is likely to be stored for an extended period and put to a variety of uses in the future. Consequently, the extent of consumers' trust in online providers is linked to how transparent providers are about how personal information is used.

Consumers are responding to this challenging environment by taking steps to protect their personal data. These steps include providing false, misleading or minimal identity information.

Many (61 per cent) say they would withhold information if it appeared not to be needed for the service offered.

The three digital identities

Digital identities can be broadly grouped into professional, transactional and social identities. This research explored the transactional and social identities.

Australians want to keep any transactional identity, such as an online shopping account, within the narrowest parameters possible. They do this, for example, by withholding all information except what is necessary for a successful result.

The majority of the research participants saw social networking identities as digital presentations of their everyday personal and family lives. Users strictly control social identity information, trying to limit access to their personal data such as photos, addresses and phone numbers. Their main concern is that they do not want this data to be reassembled in public on the internet. They want to be assured that only those they select as 'friends' or 'followers' have access to the information.

The research revealed that there are contexts, such as career development, where users are willing to make their personal information more widely available. With services such as LinkedIn now used by over four million Australians, a third type of digital identity—the professional identity—appears to be emerging.

Ramifications for providers of online services

Do customers really know why you need their information?

Customers are more inclined to provide you with accurate personal information when they understand why the information is needed. You need to carefully consider why each piece of personal information is required, and communicate this clearly and succinctly.

Your customer data may be less valuable than you think

Some consumers prefer not to give you their real name if they don't have to. It's called 'pseudonymity'. This means that the data you collect about them may be less valuable

than you hoped. Consider whether your business needs to identify all its customers using their 'real' name.

You need to balance security and privacy
You need to consider whether improved security is introduced at the expense of customer privacy.

Improve your communication
You need to consider how best to communicate how you handle personal data. The more consumers understand how their personal data is used, the more they are inclined to trust you.

Disclose data breaches
Consider the value of openly disclosing a malicious or unintended breach of data security—consumers value transparency.

Help consumers to choose consciously
Australians want to be equipped with information which enables them to make thoughtful and informed choices when they are online. This research shows the importance to Australians of transparent and easy-to-use information about privacy and security. See www.cybersmart.gov.au/digitalcitizens for more information and resources.

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

Three digital identities—changing with context

Australians surveyed do not see themselves as managing digital identities. Instead, they see themselves performing a range of specific tasks such as:

- identifying themselves
- protecting themselves from unwanted intrusions, embarrassment and financial loss.

With 61 per cent of respondents saying they would withhold information if it appeared not to be needed for the service offered, online providers should consider whether they require personal identity information when it is not clear to consumer that it is necessary.

Digital identities can be broadly grouped into professional, transactional and social identities.

This research explored transactional and social identities.

Australians want to keep any transactional identity, such as an online shopping account, within the narrowest parameters possible, for example, by withholding all information except what is necessary for a successful result. Social networking service identities are seen, by the majority of the research participants, as digital presentations of their everyday personal and family life. This social identity information is strictly controlled, with users attempting to limit access to their personal data such as photos, addresses and phone numbers. Their main concern was that they did not want this data to be reassembled in public on the internet. They want to be assured that only those they select as 'friends' or 'followers' have access to the information.

> 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: 18–29, more social than transactional*

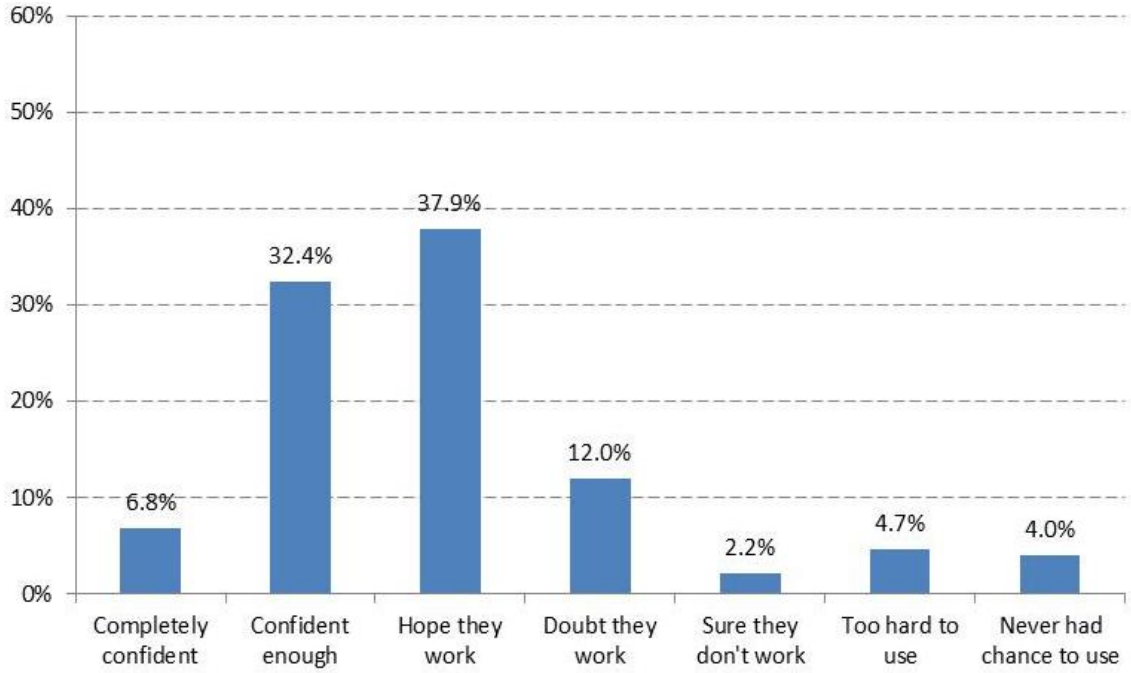
The qualitative study revealed that there are contexts, such as career development, where users are willing to make their personal information more widely available. With services such as LinkedIn now used by over four million Australians, a third type of digital identity—the professional identity—appears to be emerging.[1]

Hopeful and confident about privacy settings

Nearly all survey participants acknowledged that they have some degree of control over their privacy through tools made available by providers of devices, browsers and applications. They were asked about how confident they were in achieving the level of privacy they wanted through choosing a preferred privacy setting.

[1] Fitzsimmons, Caitlin, '4 million members and counting: LinkedIn Australia finds connections get you places', Business Review Weekly, 14 March 2013, accessed 27 August 2013.

Figure 1 Confidence in privacy settings



Base: Total sample, N=2,509

The results show that nearly four in 10 were confident that privacy settings work, rising to 52 per cent of 18 to 24-year-olds. However, another four in 10 were more hopeful than confident about the effectiveness of privacy settings. And about one in five had an overall negative view:

- 12 per cent were doubtful
- only two per cent were sure they did not work
- five per cent found them too hard and confusing to use.

Overall, there is significant scope for consumers to better understand how privacy settings operate and to trust them.

Privacy policies—readability and trust

> 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*

Privacy assurances are usually outlined in a set of terms and conditions that users are asked to accept, or in a provider's privacy protection policy. The qualitative research found that neither thoroughly reading of terms of use, nor even just skimming them to check privacy assurances, was widespread. The reasons given for not paying more attention to privacy assurances included:

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

A recent study by the Office of the Australian Privacy Commissioner supports these findings. The study found that the average privacy information on websites was 2,600 words long and judged by more than 50 per cent of the study's respondents to be difficult to read.[2]

Despite these barriers, the *Digital footprints and identities* research found most internet users still wanting to understand what they were signing up for. A majority (54 per cent) reported making some attempt to read through terms of use. This compares with less than one in five reporting that their default is to click through without reading. This suggests that information presented in concise, simple language will be welcomed by many internet users.

Reactions to the vulnerability of digital footprints

Digital footprints refer to the trail, traces or 'footprints' that people leave behind online. This is information transmitted online, such as registration details, emails, uploading videos or digital images. All leave information about individuals that is available to others online.

> Total privacy is a thing of the past
> *Group 3: 30–39, High transactional & social*

Qualitative participants were shown a short video produced by an overseas regulator. The video described how digital information generated from a person's everyday transactions can be collected and used by private companies and organisations, without express permission. Responses ranged from shock and anger to resignation. Older participants tended to be more aware of the possibilities and calmer in their reactions.

> I think mostly we understand that it is now a fact of life.
> None of it surprises me.
> *Group 9: 65+, mixed use*

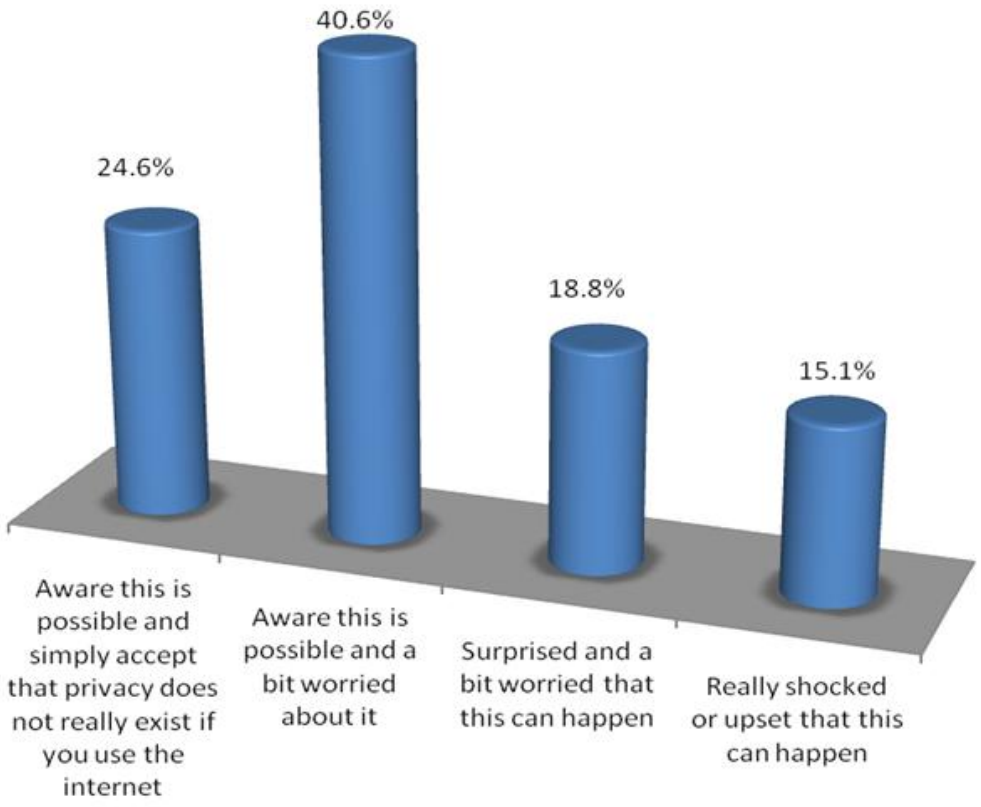
In the youngest groups, words like 'shock' and 'surprise' appeared most often in response to the idea that personal information was being gathered and shared.

> … 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: 18–29, high transactional & social*

The national quantitative survey confirmed the range of reactions found among qualitative participants. As Figure 2 shows, the majority indicated they were aware of the possible vulnerability of digital footprint data and how it could then be used (65.2 per cent). However, one in three indicated they had not previously been aware of this vulnerability.

[2] Office of the Australian Privacy Commissioner, *Privacy Commissioner: Website privacy policies are too long and complex*, media release, 14 August 2013.

Figure 2 Reactions to vulnerability of digital footprints



Base: Total sample, N=2,509

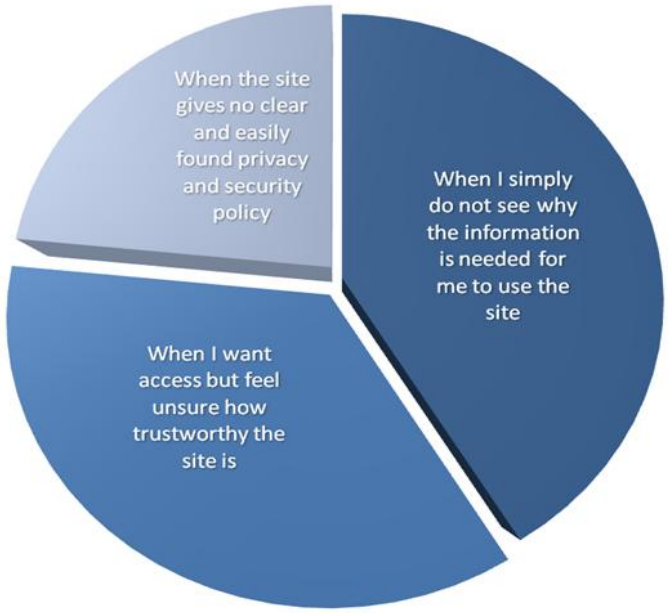
Data integrity and pseudonymity

Recently, attention has been paid to the potential for 'big data' to transform information about users' preferences and activities into an increasingly valuable currency. However, many Australians are making deliberate choices either to not share personal information online or to provide inaccurate information. Internet users are doing this for a variety of reasons but they all point to a problem of trust, which is a barrier to the overall integrity of digital data collection.

Providing inaccurate personal information was a strategy reported by research participants. Without an option to be anonymous, users seek what might be termed 'pseudonymity'. They do this by using false, inaccurate or different versions of one or more of their real name, age or date of birth, and their email or physical address.

Forty-seven per cent of survey respondents acknowledged that they would sometimes provide inaccurate information. They were asked for their reasons. Relevance ('I do not see why the information is needed for this site/service') is the strongest reason to provide inaccurate information. Security and transparency are also important.

Figure 3 Reasons participants had given inaccurate information



Base: N=1,189

One clear message for collectors of identity information is that the integrity of their data may be under significant pressure where individuals are reluctant to provide accurate identifying information.

Strong reservations about third-party identity services

A growing number of online services offer a user the ability to log onto the site using existing credentials, for example, their login and password from a social networking or webmail service. The research showed four out of five were aware of these services but 71 per cent of those who know about them have chosen not to use them. Respondents were also presented with a list of potential advantages that a third-party login service may offer, such as reducing the number of logins and passwords to be kept track of or reduced time registering for a new site. Despite this, the most common response was that such a service had nothing attractive to offer.

When the reservations were explored, survey respondents said that they:

- preferred to keep different sites separate
- wanted to avoid having data held by these sites gathered in one place
- were concerned that the login site might pass on information without their knowledge or permission.

Transparency may encourage trust, even after a critical incident

The research also explored which (if any) kinds of privacy breaches would prompt a user to stop using a site or service. Figure 4 lists these in order, from events that would prompt the most people to stop using a site to the least annoying. These responses show which issues are of greater concern or sensitivity than others.

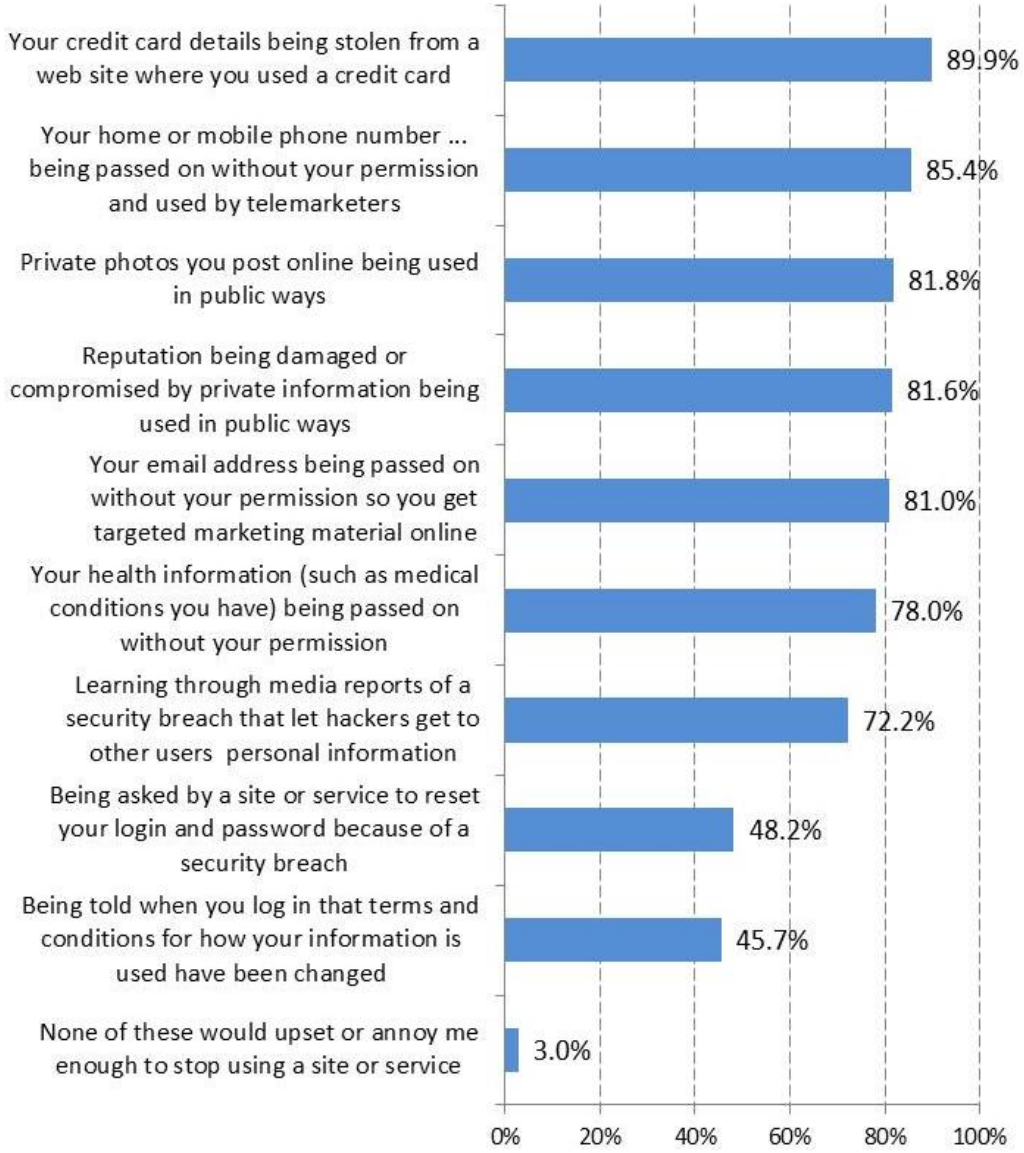
Seven of the nine events described would be grounds to stop using a site or service by at least three in four of the sample. In particular:

> having the security of your financial and personal information or personal images compromised

> experiencing reputation damage by personal information being spread

> becoming the target of unwanted marketing, especially offline.

Figure 4 Which of the following would upset or annoy you so much you would stop using that site or service?



Base: Total sample, N=2,509

The research also shows that if there is a security breach it is clearly better for a supplier to inform its users directly rather than them learning about it through the media. This was evident in the much higher response to being annoyed about learning of a security breach through media reports (over seven in ten) than to being told of a breach by the provider. Just under half indicated they would be upset by this.

About this research

This is the second of three short papers 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.

Definitions of key terms about digital information are evolving. In this report, 'digital footprint' is the trail of data created arising from a user interacting with an online network. A 'digital identity' is used to mean a collection of digital information which contains a set of identifying attributes, which may or may not reflect the attributes of a real person.

research**acma**

The management of digital information and identity is becoming an increasing focus in digital communications for business, individuals and governments worldwide. The current research is part of the ACMA's research program, and is aimed at understanding the behaviours and attitudes relevant to the creation, use and management of an individual's digital identity, the management of digital information online, and 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 practice and design.

This is the second of three short papers that contributes to the ACMA's research theme on digital society, which is directed to identifying 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

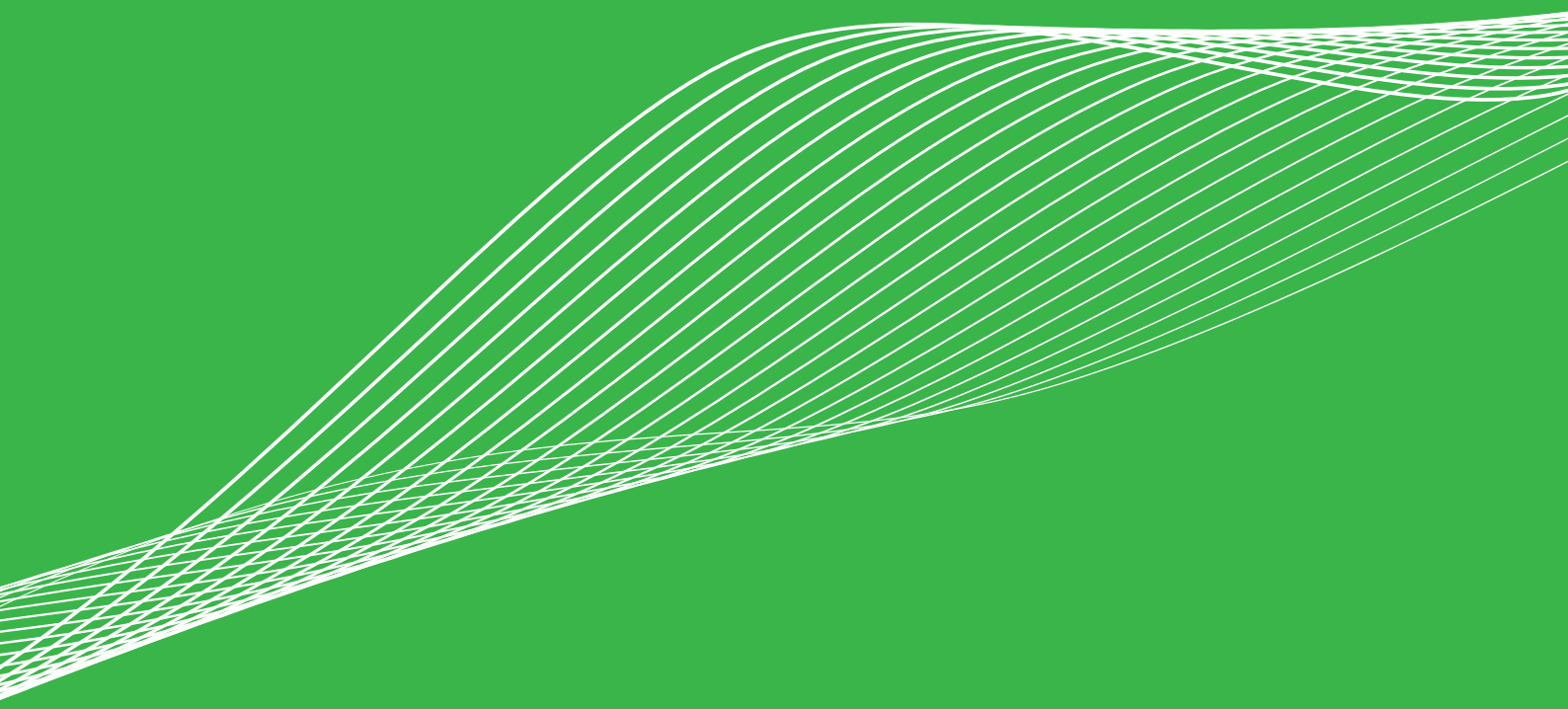
T +61 3 9963 6800
F +61 3 9963 6899

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