Australian Government

Australian Communications and Media Authority

researchacma

Identity and responsibility

Digital footprints and identities research Short report 3

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

Manager, Editorial and Design
PO Box 13112
Law Courts
Melbourne VIC 8010
Tel: 03 9963 6968
Email: candinfo@acma.gov.au

Contents

Summary

Taking protective action

Australians trust government with their digital identity information but they are sensitive to unnecessary requests for information.

Their response is a range of protective strategies, including withholding information or deliberately providing inaccurate information.

They want reasonable control over how their information is shared and need clear and easy-to-understand information about how their data is stored and used, including how it is used by government.

Their views about the role of government in protecting personal information are broad. While some realised that the nature of the internet sharply limited the potential effectiveness of nationally-based regulatory schemes, others wanted and expected support from government, particularly in standards-setting and public education.

Over 80 per cent wanted government to take a role in protecting online users' personal information, with half wanting government to enact and actively enforce legislation.

Sharing responsibility for protecting information

While Australians recognise that there is a clear role for government in protecting personal data, most see *primary* responsibility resting equally with individual users, service providers and government.

When considered with the high level of support for an active government role in protecting personal information from misuse, these results suggest that Australians see a strong role for government. However, government is just one part of the picture, with individuals and service providers also expected to take responsibility.

As far as complaining about misuse of personal information online is concerned, there was no clearly identified channel for making complaints beyond complaining to the service provider.

Modelling best practice

There is an opportunity for government to model best practice and 'set the bar' for service providers in maintaining the trust of users.

Australians support government in setting standards and providing a means to resolve issues. However, they see current responsibilities distributed across a number of regulatory bodies and levels of government, all of which have legitimate interests in maintaining the effectiveness of the safeguards they administer.

From a whole-of-economy perspective, the increasing scale and breadth of citizens' online interactions support increased attention to digital identity management.

Major economies such as the United Kingdom, the United States and New Zealand have seen new forms of trusted identity verification emerge, with government either taking the lead in establishing identity products or coordinating with industry in the adoption of a common approach. However, there has been limited progress in Australia on developing trusted identity measures. Establishing common protocols for handling identity information that are understood by consumers, providers and government will generate economies of scale through increased acceptance and interoperability. This will support innovation and competition and enhance Australia's ability to be a leader in the development of the global digital economy. There may be substantial benefit in formulating a coherent national framework within which trusted identity products and services can be developed.

A coherent regulatory framework for managing digital identity and personal online security will need to ensure there are adequate processes to deal with complaints and concerns. These processes will need to be widely known and understood by digital citizens and industry operators.

This short report, which looks at the role of government in protecting personal information, 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

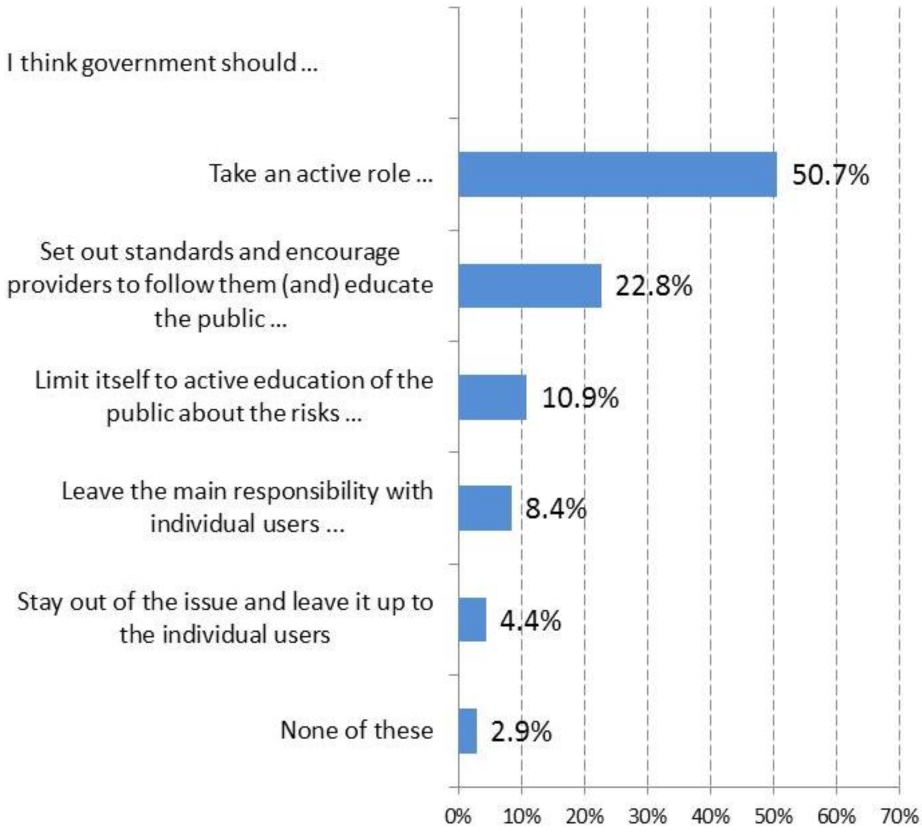
Citizens expect government to be active

There is a generally high level of trust in the personal data management practices of government organisations. However, digital citizens are sensitive to unnecessary requests for information. This leads to a range of protective strategies, including withholding information or deliberately providing inaccurate information. The findings point to citizens' wanting to exercise reasonable control over how their information is shared. They also need clear and easy-to-understand information about how this data is stored and used, including how it is used by government.

Research participants revealed a broad range of views about the expected role of government in protecting personal information. Some recognised that the nature of the internet, with many service providers based outside Australia, sharply limits the potential effectiveness of nationally based regulatory schemes. Others wanted and expected support from government, particularly in standards-setting and public education.

The national survey asked respondents to say what role they believed that government should take in protecting internet users from the misuse of their personal information.

Figure 1 What role if any should government have in protecting you from misuse of personal information you have given online?



Base: Total sample, N=2,509

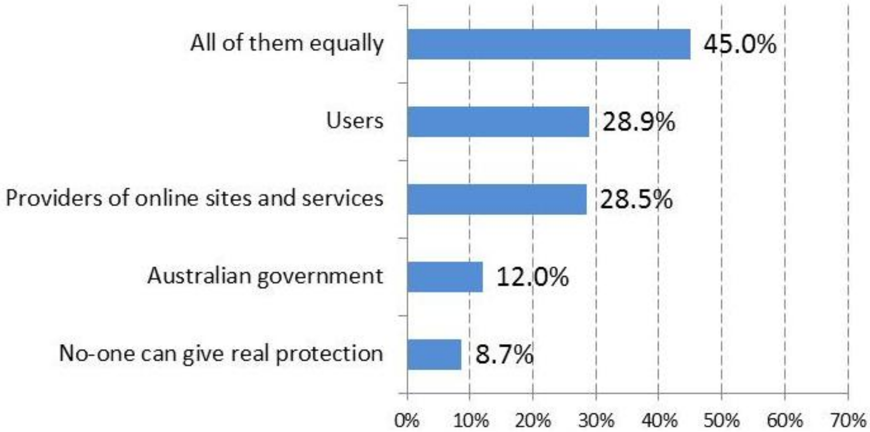
Note: '…' indicates the option has been abbreviated—for the full text see Appendix 2 of the Digital footprints and identities *research report.*

Over 80 per cent wanted government to have a role in protecting online users' personal information, with half wanting the government to enact and actively enforce legislation. Twenty-three per cent wanted the government to be active in both educating and warning users, and encouraging providers to follow government prescribed standards. A further 11 per cent said the government should actively educate the public about risks, but not beyond that.

Shared responsibility for protecting information

The research also probed whether the *primary* responsibility for protecting personal data lies with individual users, service providers or with government. The most common response, by nearly half the sample (45 per cent), was that the responsibility lies with 'all of them equally'.[1]

Figure 2 Who is primarily responsible for protecting individual users from misuse of personal information they have given online?



Base: Total sample, N=2,509

Note: Total is >100 per cent as 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 percent), older age groups, those aged 65 or more (17.2 per cent), were more likely to hold this view than younger age groups (5.8 per cent to 9.6 per cent).

When coupled with the high level of support for an active government role in protecting personal information from misuse, these results suggest that Australians see a strong role for government, but as just one part of the picture. Individuals and service providers are also expected to take responsibility.

Options to complain not clear

Consumer protections relating to personal information are currently shared by a range of Commonwealth and state regulatory bodies, including the Office of the Australian Information Commissioner and the ACMA. Although a proportion of research participants 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*

[1] The prompted options 'all of them' and 'No-one can give protection' had been expressed in the qualitative discussions.

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

The responses to the survey question about where respondents would go to complain about misuse of personal information online (see Figure 3) indicated that there was no clearly identified channel for making complaints, beyond complaining to the service provider.

The findings reveal four main categories of response:

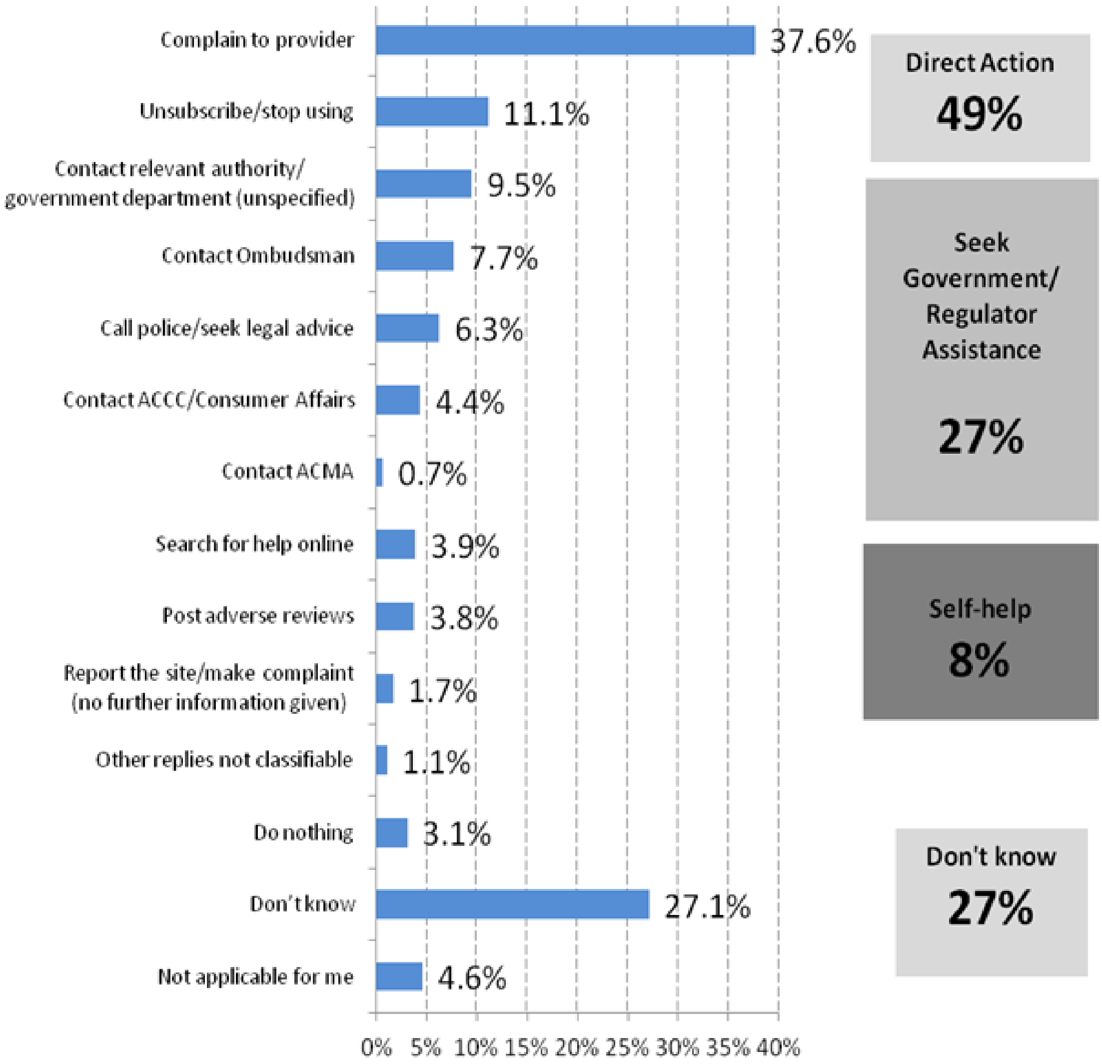
> 49 per cent of respondents would take direct action—complaining to the provider directly or stopping using the service

> a further 27 per cent would seek assistance from a regulator or similar body

> about eight per cent would take matters in their own hands by searching for help online, posting adverse reviews, or reporting the site through online tools

> 27 per cent did not know what action they could take.

Figure 3 Making complaints about misuse of personal information



Base: Total sample, N=2,509

Note: Total is >100 per cent as some respondents gave more than one reply

Complaining to the service provider was more often volunteered by those aged under 65 (44 per cent for those aged 18 to 24 and 36 to 40 per cent for those aged 25 to 54) and less often by those aged 65 or more (30 per cent). Replying 'Don't know' increased from 21 per cent of those aged 18 to 24, up to 35 per cent of those aged over 65.

Developing a coherent approach to identity management

The *Digital footprints and identities* research points to an increasingly complex relationship between individuals and the services they use online. Government has the opportunity to model best practice and 'set the bar' for service providers in maintaining the trust of users.

The clear desire for government to actively protect user information is reflected in a range of existing consumer privacy protections and education activities. As well as generally applicable legislation such as the *Privacy Act 1988*, there are specific legislative protections for telecommunications privacy, unsolicited communications (including telemarketing and spam), and broadcasting.

From a whole-of-economy perspective, the increasing scale and breadth of citizens' online interactions supports increased attention to digital identity management. The research indicates support for government to set standards and provide a means to solve issues as they arise. However, current responsibilities are distributed across a number of regulatory bodies and levels of government, all of which have legitimate interests in maintaining the effectiveness of safeguards they administer.

Building on the trusted role of government

To participate in a networked economy, individuals and organisations need to be certain and confident about the rights and obligations relating to the use of their personal data. They also require skills and knowledge, and to adopt behaviour, that enables them to engage effectively as digital citizens. The research shows that among Australians there is a variable combination of low levels of trust and misplaced confidence in their knowledge and/or abilities and understanding of how digital footprint information is collected and used.

The recent launch of the ACMA's *Digital Citizens Guide* is an example of government working with the digital economy sector to promote consistent messages of confident online engagement. The Guide brings together a number of Australian Government and industry resources that support citizens to make better, informed choices and build stronger online communities.

Standards setting and common protocols

Major economies such as the United Kingdom, the United States and New Zealand have seen new forms of trusted identity verification emerge. Government is either taking the lead in establishing identity products or working with industry to adopt a common approach. However, there has been limited progress in Australia on developing trusted identity measures. The research indicates that, for a number of reasons, citizens are reluctant to accept services that require more than a login and password.

Establishing common protocols for handling identity information that are understood by consumers, providers and government will generate economies of scale through increased acceptance and interoperability. This will support innovation and competition and enhance Australia's ability to be a leader in the development of the global digital economy. Therefore, there may be substantial benefit in formulating a coherent national framework within which trusted identity products and services can be developed.

Working with industry

Government can play a role in developing initiatives through independent research, devising good practice principles and stakeholder engagement. The research indicates a mixture of concern and lack of knowledge about the use of digital footprint data which points to a need for broad engagement on the implications of the growth of 'big data'. One example of a self-regulatory response to digital footprint concerns is the *Social Advertising Best Practice Guidelines* developed by the Interactive Advertising Bureau Australia.[2] The guidelines include recommendations that consumers be given opportunities to opt in and out of certain data collection practices plus guidance on how social media profile data should be captured, used and disclosed in marketing activities.

Clear paths for consumers to seek redress

Redress is an important and enduring regulatory concept in media and communications. The public is entitled to have confidence in media and communications safeguards that should reflect community standards and norms for consumer transactions. These safeguards should also provide users with effective and accessible avenues of complaint and redress if standards are not met.

A coherent regulatory framework for managing digital identity and personal online security will need to ensure there are adequate processes to deal with complaints and concerns. These processes also need to be widely known and understood by digital citizens and industry operators.

[2] See http://iabaustralia.com.au/sitecore/shell/Controls/Rich%20Text%20Editor//-/media/IAB/Resources/Presentations%20and%20Guidelines/Social%20Advertising%20Paid%20Guidelines%20April%202013.pdf

About this research

This is the third and final short paper 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 best practice and development.

This is the final 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