Australian Government | acma

Australian Communications and Media Authority

Attitudes towards use of personal information online

Qualitative research report

AUGUST 2009

communicating | facilitating | regulating

Canberra
Purple 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
TTY 03 9963 6948

Sydney
Level 15 Tower 1
Darling Park
201 Sussex Street
Sydney NSW

PO Box Q500
Queen Victoria Building
Sydney NSW 1230

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

Published by the Australian Communications and Media Authority

Attitudes towards use of personal information online

Qualitative research report

AUGUST 2009

Contents

Contents (Continued)

Executive summary

This report presents the findings of research conducted by TNS Social Research on behalf of the Australian Communications and Media Authority (the ACMA) into adult Australians' attitudes towards the use of personal information in the context of digital media and communications consumption.

The role of the ACMA includes the provision of information and advice to the community about communication matters and administration of a range of consumer protection measures.

Australian adults' use of personal information in this context appears as a new priority issue for research, with this research being undertaken in order to further the ACMA's understanding of adult Australians' behaviours and attitudes in providing, sharing and protecting personal information when using digital media and communications.

In total eight focus groups were conducted between April 16 and May 4, 2009. Each focus group ran for approximately two hours in duration and included (on average) seven participants.

Key findings are as follows:

Research participants universally interpreted the term 'digital media and communications' to mean 'online activity' or 'interaction via the internet'. Only limited use was made by research participants of advanced mobile technologies such as web enabled phones—many noted that although they *could* access the web via their mobile phones, they chose not to. More widespread usage of mobile technologies was seemingly limited by cost barriers, lack of perceived need, connectivity issues and general unfamiliarity with operation of mobile devices in this context; rather than being due to any associated security concerns.

'Personal information' was seen to encompass anything and everything that could be used to identify an individual, or that could be used as a means of obtaining knowledge that an individual considers to be "private".

Personal information can be classified broadly as 'hard' information and 'soft' information. Hard information (which participants thought was more sensitive) is linked to *identifying* an individual, or is in some way *unique* to an individual, whereas soft information (which participants thought was less sensitive) more generally *describes* an individual.

In using digital media and communications participants accept that they will, by the very nature of their activity, be sharing personal information. Many participants expressed an accepting or a resigned attitude towards their ability to protect their personal information online, a consequence of the widespread perception that breaches are inevitable.

The type of, and level to which, personal information is disclosed is seen to be within an individual's control and a matter of personal choice.

More specifically, the decision to disclose personal information is based on an assessment of the *benefits* that will be afforded by the disclosure of such information, versus the *risk* inherent in such information being disclosed.

The instances in which adult Australians choose to divulge personal information can be broadly categorised into two key areas:

1/ **transactional provision**, with the provision of such information being necessary to obtain a good or service that the individual requires.
2/ **networking or social disclosure** whereby information is disclosed by an individual within an online community in order to share and exchange opinions, beliefs and details of activities.

The types of risks associated with personal information being used in a way contrary to the intent for which it was provided include:

> risks to **personal safety and wellbeing**, or the safety of others (and in particular children)
> risk of **identity theft**
> risk of **financial loss**/fraud/theft (could include malicious software)
> risk of **damage to reputation**
> risk of an **invasion of privacy**, (access to personal information without permission)
> risk of exposure to **unwanted communications** (spam or push marketing).

Consideration of the inherent risk associated with each adverse outcome is a factor of the perceived likelihood of the outcome occurring versus the severity of the consequences that would result if such an adverse outcome was to occur.

The research also identified a number of factors or attitudes influencing perceptions of risk:

> belief that privacy breaches are inevitable
> distinction between online transactions and interpersonal interactions
> generational differences
> risk as a trade off for convenience
> unspecified (and in some cases irrational or unjustified) fear
> magnitude of the perceived risk.

In terms of risk avoidance, a number of strategies were reported by participants, and can broadly be categorised as active and passive risk mitigation strategies.

Active strategies involve an individual making deliberate decisions and active choices in their online behaviour that assist in protecting the security of their personal information. These strategies include:

> password management
> managing email addresses and spam
> judicious use of credit cards or the use of alternative pay methods
> managing information shared on social networking sites.

Passive strategies relate to an individual's reliance on the software platforms or the security systems of providers to protect an individual's personal information. Trust is placed in the integrity of these systems to the extent that they are seen as being sufficient to protect the personal information of the individual.

Passive strategies also include reliance upon password management being dictated by the protocols of the site with which the individual wishes to interact.

Although there is widespread knowledge as to what constitutes effective risk management strategies across a range of circumstances, there are nonetheless several areas where it has been identified that adult Australians have a limited understanding of how to best protect personal information in these contexts, or alternatively are not aware that there is a need for caution to be exercised. These situations include:

> end user licensing agreements;
> location being revealed by a mobile device;
> Bluetooth networking;
> Biometrics.

In terms of how adult Australians have developed their risk management knowledge and minimisation strategies, this education has typically been informal and largely gleaned through discussions with families and friends, in general, and through consultation with that family member or friend known to be the 'IT expert', in particular.

Such knowledge is also being learnt in schools and the workplace, and is being transferred back into the home, particularly in relation to file protection and password management. There is scope for the ACMA to explore these backdoor channels as effective means to distribute empowering information.

Responsibility for the safeguarding or protection of personal information is considered to be multi-layered, with the individual, the ISP, the online entity and the government all having a role to fulfil.

There was a general consensus among participants that the first line of defence in the protection of personal information is at the individual level.

Australians feel themselves to be relatively well informed as to how to protect their personal information online. This is undercut by a number of factors which will need to be addressed if online security is to be improved in real terms.

These factors include:

> a pervasive belief among adult Australians that security breaches are inevitable, leading to some complacency in adopting appropriate risk management strategies;
> the sheer pace of technological change makes it difficult to stay up to date with new technologies and platforms ,and protected from the latest risks

Consequently, there is a danger that anxieties stemming from these two factors can discourage full and open participation in the digital environment by some groups and hinder their social inclusion.

Research findings suggest that Australians are learning about protecting their personal information in largely informal ways. They indicate that they see a role for government education. The challenge for government is to utilise the full range of communication channels – including unorthodox channels such as workplaces or via schools – to educate adult Australians. In this way, government can augment the informal learning that is currently occurring, and in so doing, counter the fatalism that is currently undermining Australian's efforts to manage the risks they face in the digital environment.

Research objectives

The role of the Australian Communications and Media Authority (the ACMA) includes the provision of information and advice to the community about communication matters and administration of a range of consumer protection measures.

To date, the ACMA's education and awareness matters relating to the disclosure of personal information through digital media and communications has been focused on the protection of young people online. Australian adults' use of personal information in this context appears as a new priority issue for research, with this research being undertaken in order to further the ACMA's understanding of adult Australian's behaviours and attitudes in providing, sharing and protecting personal information when using digital media and communications.

More specifically, this research seeks to gain insight and understanding as to the attitudes and behaviours of the adult Australian population in relation to:

- Use of personal information in the context of digital media and communications:
  - What are the attitudes to use of personal information on digital media and communications among adult Australian users of digital media and communications?
  - Do the attitudes and behaviours vary depending on type of personal information that they are disclosing? Do the attitudes and behaviours vary depending on the context of use?
  - Is some information considered more sensitive than others? Are there different levels of concerns depending on type of personal information?
- Risks related to use of personal information online and in a variety of other contexts, with a particular focus on social networking sites:
  - Are there differences in the attitudes of adult Australians to the protection of their personal information and privacy depending on the circumstances?
  - What are the reasons for wanting to protect personal information?
  - What is the understanding and awareness of risks related to use of personal information on digital media and communications among adult Australian users of digital media and communications?
  - How do awareness and attitudes towards protection of personal information on social networking sites compare to attitudes towards other online risks?
  - Are there differences in the attitudes and behaviours depending on the type of technology involved?
  - Do attitudes and behaviours differ when use of personal information is on a mobile phone device through mobile internet, TXT or SMS, compared to use of e-mail or internet connection from a computer?
  - Are there specific concerns in relation to use of mobile phones, GPS, and other location based services?
  - Are there specific concerns in relation to possible risks linked to use of un-secured Bluetooth networks for transactions or exchange of personal information?
  - Differences in attitudes and behaviours depending on types of device or technology being used (if any).

- Protection of privacy:
  - What is the degree of awareness of and preparation to use different risk mitigation strategies?
  - Are adults using the tools available to protect their privacy, and if not, why are they not using them—is it because they don't care, or they don't know about them?
- Expectations in relation to safeguards:
  - What are the expectations in relation to responsibility and safeguards for protecting personal information?
  - Do Australians expect industry players or service providers to take steps to protect their privacy online?
  - What do they expect from a regulator or government agency?
  - Are there other players they expect to play a role (e.g. media, consumers association)?
  - Do they understand they also have a responsibility to protect their information?
- Information sources and needs concerning use of personal information online:
  - What are the information needs in relation to use of personal information online, related risks and existing risk mitigation strategies
  - What knowledge and information would be useful to enable users to undertake risk mitigation practices for themselves?
  - Where do users seek out information?
  - What are regarded as trusted sources of information?
  - What would be the best way for adult Australian users to learn more about online risks and risk mitigation strategies?

The information collected in this research is aimed to assist the ACMA in the development of appropriate measures to raise awareness of risks related to use of personal information collected or disclosed through use of digital media and communications devices and to promote use of simple self-protective measures.

Methodology

In total eight focus groups were conducted between April 16 and May 4, 2009. Each group went for approximately two hours in duration and included (on average) seven participants.

Capital city, regional and rural representation was sought with groups further stratified according to life stage, current behaviours relating to disclosing personal information online and technological use. This group stratification is detailed below.

Table 1 Sample segmentation

Location	Date of group	Age/Life stage*	Online disclosure of personal info**	Technology usage***	Gender
Sydney	16 April 2009	Early	High	High	Mixed
Newcastle	16 April 2009	Late	Low	Low	Mixed
Geelong	20 April 2009	Early	Moderate	Moderate	Mixed
Melbourne	21 April 2009	Mid	High	High	Mid
Perth	22 April 2009	Mid	Moderate	Moderate	Mixed
Adelaide	22 April 2009	Late	Low	Low	Mixed
Alice Springs	23 April 2009	Early	High	High	Mixed
Orange	4 May 2009	Mid	Moderate	Moderate	Mixed

*Early = no kids, to 39 years / Mid = kids at home, to 59 years / Late = no kids, to 75 years.

** The degree of online disclosure of personal information was determined based on a number of behavioural statements asked in the recruitment stage.

***The degree of technology usage was determined based on a number of behavioural statements asked in the recruitment stage.

Within each group the moderator used a pre-prepared discussion guide (developed in consultation with the ACMA), included in Appendix A.

Participants were given an incentive payment of eighty dollars to reimburse time and travel costs (as well as encourage participation) and were recruited by a professional recruitment agency.

Research findings

Understanding what constitutes digital media and communications

Research participants universally interpreted the term ‘digital media and communication’ to mean ‘online activity’ or ‘interaction via the internet’.

Typically such online or internet access was undertaken via computers (both desktop and laptops) with the majority of research participants using PC based applications as opposed to Macs.

Only limited use was made by research participants of advanced mobile technologies such as web enabled phones—many noted that although they *could* access the web via their mobile phones, they chose not to. More widespread usage of mobile technologies was seemingly limited by cost barriers, lack of perceived need, connectivity issues and general unfamiliarity with operation of mobile devices in this context; rather than being due to any associated security concerns.

> *Yeah I just couldn't be bothered… I have got the laptop I have got the work I don't need that.*
>
> *Just couldn’t be bothered paying for it.*
>
> *I probably wouldn’t buy anything with my phone just because I am crap at the screen thing and I would probably push the wrong button.*
>
> *They are supposed to be less secure but I don't really know so.*

Where use of online applications via mobile devices was made, it was largely for email communication only.

Other digital media applications such as GPS enabled devices and Bluetooth technologies were not automatically considered to be a form of online activity or communication; participants needed prompting to consider their behaviours’ in regard to these devices. It was also apparent that not all participants were familiar with these technologies.

Understanding what is 'personal information'

'Personal information' was seen to encompass anything and everything that could be used to identify an individual, or that could be used as a means of obtaining knowledge that an individual considers to be "private".

Personal information can be classified broadly as 'hard' information and 'soft' information. 'Hard' information (which participants thought was more sensitive) is linked to identifying an individual, or is in some way unique to an individual, whereas 'soft' information (which participants thought was less sensitive) more generally describes an individual.

'Hard' personal information includes:

> information that was considered to be specific and unique to an individual, such as tax file number, Medicare number, or, drivers' license number
> information that was considered to be linked to the financial status or situation of an individual, such as bank details, credit card details and income
> medical records
> information that identified the residence of an individual, such as home address and home phone number
> passwords.

'Soft' personal information includes:

> information about an individual's interests and activities
> memberships or political affiliations
> relationship status or sexual orientation
> family structure and information about an individual's children or other dependents
> social activities
> details about an individual's employment or career
> descriptions of an individual's physical details (such as weight, eye colour, height etc)
> details of an individual's online activity
> photographs and videos of an individual.

Interestingly, mobile phone numbers were distinguished from home phone numbers or landlines by most participants, and in many cases a mobile number was classified as a piece of soft personal information.

This was due to the perception that mobile phone numbers are perceived as 'disposable' i.e. easily replaced, and unlike home phone numbers, are not linked to a fixed address. Calls to mobile phones are also more easily screened: greater control can be exerted over who gets through.

Attitudes towards disclosure of personal information

In using digital media and communications, participants accept that they will, by the very nature of their activity, be sharing personal information.

> *I think it is part and parcel of the way we live, it is like saying … why do we choose to drive a car when we know that they are dangerous and people kill themselves in cars ... because it is convenient and it is easy and it is part of modern life, that is why we choose to do it.*

> *I don't know. I think it is like it is a risk you take but like everything it is sort of like we are so dependent on the internet and things like that that it is a part of life I guess, when you start doing your banking online and you start purchasing things online and you are putting those details out there…*

Many participants expressed an accepting or a resigned attitude towards their ability to protect their personal information online, a consequence of the widespread perception that breaches are inevitable:

> *The other point of course is that if people really want to hack into your computer, they will hack into it regardless of how much security you have got. One of my son's mates reckons he can hack into anything … there are lots of kids out there that are like that, so really you can put up as much security as you like … it is not going to keep them out.*

This acceptance is not just restricted to digital privacy:

> *I use it for pretty much everything, my whole world is my computer so I am on it all day, every day, most nights … and yeah most of my information is on the internet so anybody could probably find out anything about me, but in my own personal experience anyone can find out anything about you whether or not you have the internet. So yeah, if they want to know they will find out.*

> *They can just as easily grab your mail or look it up in the phonebook.*

However, the type of, and level to which, personal information is disclosed is seen to be within an individual's control and a matter of personal choice.

More specifically the decision as to whether or not adult Australians disclose personal information is based on an assessment of the *benefits* that will be afforded by the disclosure of such information, versus the *risk* inherent in such information being disclosed.

The instances in which adult Australians choose to divulge personal information can be broadly categorised into two key areas:

1/ Transactional provision, with the provision of such information being necessary to obtain a good or service that the individual requires. Such activity relates to the purchase of goods and services online, as well as to interaction with service providers and entities in order to appraise that entity, or receive from that entity required

information. The benefit to the individual is the convenience that the interaction affords them in obtaining the required good, service or information.

Transactional provision of personal information occurred across all ages and life stages.

2/ Networking or social disclosure whereby information is disclosed by an individual within an online community in order to share and exchange opinions, beliefs and/or details of activities. The benefit to the individual in such instances is the ability to stay connected and the fulfilment of social needs.

Networking or social disclosure of personal information was considerably more prevalent among younger adults who saw such activity as being a key means of social interaction. By comparison older adults were less likely to perceive any benefits that would be afforded to them by such activity and as such were considerably less likely to engage in this type of behaviour.

Why would you want to, who has the time?

Can't you just pick up the phone or write an email?

Furthermore, many of the older adult Australians who were active in social networks claimed to have been pressured into joining by younger family members and friends, or alternatively had joined in order to be able to better monitor the online activity of their dependant children.

They made me.

I must admit I couldn't be bothered but I did feel a bit out of it when a friend assumed I knew something because they put it on Facebook, so I ended up joining.

Inherent risks in disclosing personal information

Types and consideration of risk

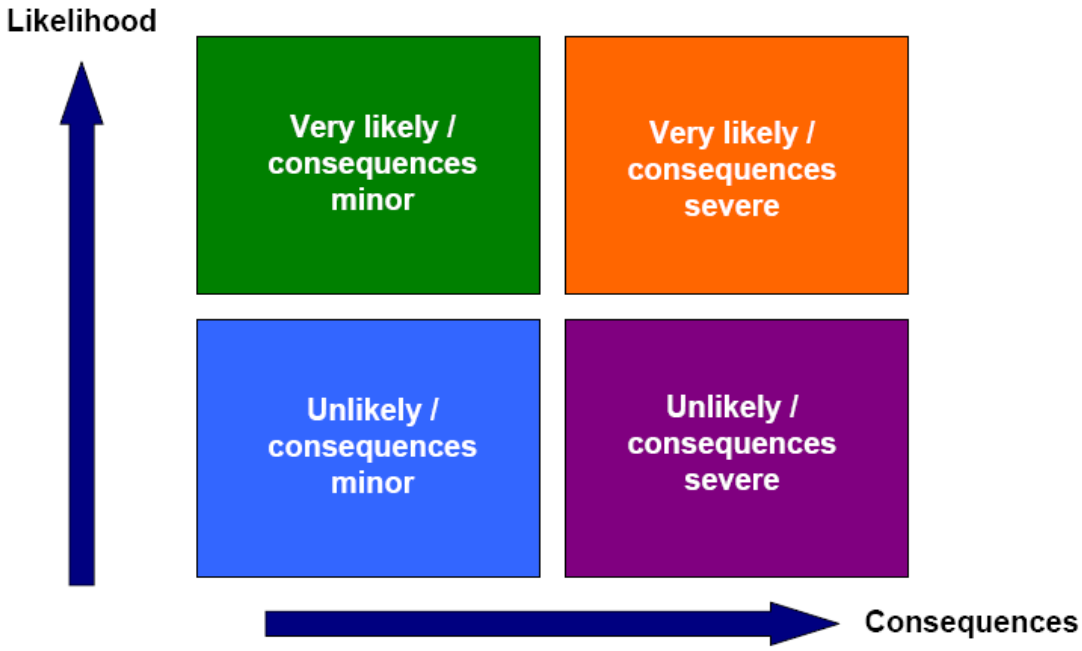
Participants saw that any provision or disclosure of personal information carried an inherent risk of that information being used in a way that was unintended, possibly resulting in an adverse outcome.

Types of risks associated with personal information being used in a way contrary to the intent for which it was provided include:

- risks to **personal safety and wellbeing**, or the safety of others (and in particular children)
- risk of **identity theft**
- risk of **financial loss**/fraud/theft (could include malicious software)
- risk of **damage to reputation**
- risk of an **invasion of privacy** (access to personal information without permission)
- risk of exposure to **unwanted communications** (spam or push marketing).

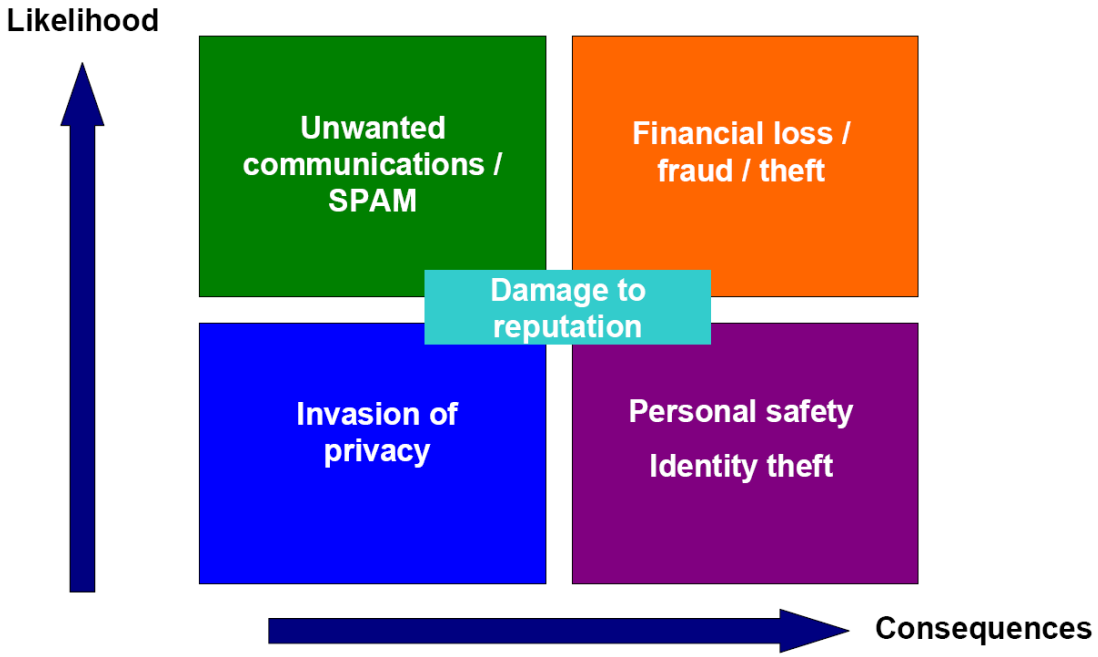
Consideration of the inherent risk associated with each adverse outcome is a factor of the perceived likelihood of the outcome occurring versus the severity of the consequences that would result if such an adverse outcome was to occur.

Figure 1 Framework used to map risks according to perceived severity



Risks identified by respondents as associated with use of personal information on digital media and communications have been positioned according to their perceived likelihood and severity as illustrated on graph below.

Figure 2 Perceived severity of risks associated with use of personal information online



Unlikely to occur/minor consequences

Risk of an invasion of privacy (access to personal information without permission)
An 'invasion of privacy' depends on a subjective assessment of what an individual considers private. Many participants talked about what they saw as a generational shift at play in this arena.

> *Now you can communicate with hundreds of people straight away … I think that it is a different paradigm … someone of my generation, we don't have that "I am open to everybody" type attitude, we are very reserved and we were brought up to be that way; privacy was important. (But) the kids in the new generation don't seem to have any concept of privacy or what it is like to be private. To have 'privacy' is basically a different paradigm altogether.*

Breaches of privacy were typically discussed in relation to income or medical information being made publicly available.

> *It is your personal medical history … you don't want people to know what conditions you suffer from to discriminate against you for any particular reason, if the job is for health insurance or anything like that.*

> *It is your last boundary, isn't it? It is you. You have got your physical boundary, your house and your gates, and then it is about you, I don't like it … it is between you and your doctor for a reason.*

The consequence of a breach of this kind was personal discomfort and embarrassment, which was judged as less severe compared to consequences of other types of risk.

Very likely to occur/minor consequences

Risk of exposure to unwanted communications (spam or push marketing)
Unwanted communications are considered to be the most likely to occur, with the least severe consequences. Participants talked about the consequences in terms of 'inconvenience' and 'annoyance', but at the same time were disturbed by what they perceived as the shadowy mechanics at play in tracking their online activities:

> *And I guess, when it comes to regulation, it should be probably more targeting software that is literally stalking you online.*

> *Yeah (advertisers) can stalk someone online. Basically what you are viewing, visiting … that (stalking) is legal.*

> *Following someone online should be considered the same as driving around following someone in a car.*

Others saw this type of information-gathering as a doorway to collecting or accumulating more sensitive pieces of personal information:

> *I would be worried about the fact that someone has access to my income, or knowledge of my income, because if they have knowledge of my spending they have some idea of what my earnings might be, or what my income could be, and that is very private.*

Generally, the main consequence is the inconvenience associated with unwanted marketing material:

> *I was hit with an onslaught of spam a couple of years ago, I don't know what happened – I am blaming one of the kids with a hotmail address – and I just got bamboozled and it was like hours a day I was trying to get rid of it, and in the end I don't know how I got onto it but I had to pay someone in the US for a spam fighter program, and then I still spent a bit of time each day blacklisting all these bits of spam … it was quite a while for real emails and stuff to get through.*

Unlikely to occur/severe consequences

Risks to personal safety and wellbeing

Risks to personal safety were universally considered to be the most severe or serious consequence that could arise from a breach in protecting personal information. This risk manifests when personal data that can be used to target an individual is obtained, and can range from bullying and cyber stalking to physical harassment, and in extreme cases physical violence.

> *Yeah look my 19 year old, she broke up with her boyfriend a little while ago, and things sort of settled down where there was no contact between them at all, and suddenly he started contacting her again and saying some nasty things about her, and I said, 'don't pay attention to it, just delete it; if you see a message from him, don't read it, delete it'. But she won't do that, she can't … she allows herself to be drawn into it.*

> *That to me is one of my fears with (my) eight year old: as she gets older she's going to be exposed to more and more of this stuff, maybe there is potential for cyber bullying and stuff like that.*

I think that is why I have the problem about my address… I don't really like giving out my home address unless it is absolutely necessary … if I buy something on the net then obviously you have got to give out your address but I am not as keen to give out my address as I would be to give out my email address.

When pressed, participants conceded that the risk of physical or psychological harassment is generally remote, and that it arises in particular circumstances. Older adult Australians were more often concerned about younger people exposing themselves to potential risks to their personal safety through unguarded online interactions. There was a tacit assumption that the risks to personal safety are more acute for women than for men.

Risk of identity theft

Awareness of identity theft was high among all groups and there were no participants who were not aware of the phenomenon. However, understanding of what identify theft entails was low, as was an understanding of the potential ramifications of falling victim to identify fraud.

Participants ranked the severity of the risk of identity theft as very high, driven largely by two factors:

1/ the potential for financial loss or damage and in particular the ongoing nature of bad credit or debts fraudulently run up in an individual's name

2/ not fully knowing or understanding what having ones' identity stolen actually means or entails.

Someone might commit a crime in your name. It might be hard for the police to see the difference between you and this other person, you could get in trouble for it … basically clocking up [debt] on someone's credit card or something under your name.

But also you would be worried about it forever, if it happened to you once you would be so scared about it always… You don't know what it is, it just ruins your entire life, you could go to jail, and you could owe forty thousand dollars.

But there is also the risk of identity fraud for your children as well. I have often heard in the press where people have discovered that their children's identity has been used to secure loans and things like that, and you are not going to know that until your child is in a position where they possibly want to buy a home or something like that. The damage has been long done …

Participants' awareness and knowledge of identify theft is largely drawn from media reports, and they concede that many of these reports are potentially sensationalised. They also understand that it is relatively rare, but are still concerned by the potential extent of the harm it can do:

It is not that common … credit card fraud is quite common but identity theft … it may not be common but it is just so serious when it happens and it is a bit of a worry.

There was awareness among participants that identity theft is not exclusively associated with breaches in personal information in a digital environment:

You see you don't actually need the internet for identity theft.

Very likely to occur/severe consequences

Risk of financial loss/fraud/theft

Closely linked to identity theft is the risk of financial loss—in particular credit card fraud, perpetrated through stolen credit card details. The risk is seen as more severe where an individual's own money is concerned—many adult Australians distinguish credit cards as 'the bank's money'.

There is some ambiguity as to the consequences of credit card fraud with many participants noting that credit stolen through details accessed online is generally insured or covered by the credit card issuer.

> *You get it back; it happens all the time. One of the reasons that we pay such high interest is because of credit card fraud, banks have to cover themselves for the insurance because it costs them, and if there wasn't any credit card fraud we wouldn't pay anywhere near the amount of money we do for credit cards. Having said that though it is fifty days of free money so why wouldn't you use your credit card.*

Being liable for stolen funds is a pressing concern for a subgroup of adult Australians (generally older, less web savvy and less engaged), and they consequently see the risk as more severe.

A number of adult Australians had experienced some kind of financial loss, or had in some way been exposed to it. Interestingly they discussed the inconvenience factor:

> *Time is a big factor. It takes a long time to change your credit cards and change your (other banking details), (it can be) really painful…inconvenient and time consuming.*

Other risk classifications

Risk of damage to reputation

In discussing damage to reputation, participants talked about unintended future consequences. While this has a number of impacts, the danger was primarily seen in relation to future employment:

> *Potential employers, if they had a look at all your other information… could just see what sort of a person you are … like if you have been on a bender for the last five days … the sort of lifestyle that you lead outside of your workplace.*

It should be noted that some adult Australians think that screening potential employees is good practice:

> *It's actually responsible for an employer to get as much history as they can because while you're interviewing there are certain rules now around privacy that you cannot ask, so if people are – I was going to say, 'stupid enough' – if people are willing to put their details up there for every man and his dog to see it, employers need to cover themselves; that's responsible employment.*

A more general consequence perceived in relation to this outcome was that potentially damaging personal information could be available in perpetuity:

I think it becomes harder to live down your reputation … I've moved around a lot and it's nice to have a few reinventions, you know, you move somewhere new and nobody knows you, you can be the person that you want to be instead of what you've gotten caught down in because of your teenage years. I think that social networking sites will make that a lot harder for people to grow up because you're constantly going to be brought back to who you were two, three, five years, ten years ago, and people will still be judging you on the sort of things you did when you were 15, 16, and not who you are now.

Many participants, particularly those who are older, saw this as being especially pertinent for young people and teenagers, due to the perception that younger Australians are less discriminating in both what they choose to disclose and whom they choose to provide it to.

Kids live so much in the moment … most people of our age group would think, 'well do I want to put this photo up? Do I really want to put that photo of me jumping off a bridge naked?' Whereas kids just go, 'oh yeah my friends will have a laugh', and they don't think about that.

On the whole, participants felt that the overall rating of risk to reputation was moderate, rather than severe, due to the consequences being less tangible, and manifesting in the future.

Factors affecting the perception of risk

The research identified a number of factors or attitudes influencing perceptions of risk. These are:

> belief that privacy breaches are inevitable
> distinction between online transactions and interpersonal interactions
> generational differences
> risk as a trade off for convenience
> unspecified (and in some cases irrational or unjustified) fear
> perceived magnitude of the risk.

Belief that privacy breaches are inevitable

One of the main factors that informs the way Australians view and assess the risks they take in releasing personal information online is a belief that privacy breaches are largely beyond an individual's control and are unavoidable.

This attitude was prevalent across all groups, and was typically expressed in relation to discussions around a lack of action or preparedness in protecting personal information. For many Australians, accepting the inevitability of a privacy breach can, at best, excuse inaction on their part, and in some cases can actually encourage recklessness.

A slightly different expression of the same idea involves seeing online transactions or interactions as inevitable, and that risk-taking is part and parcel of this type of interaction.

It is a risk you take, but … we are so dependent on the internet. Things like that are a part of life I guess. When you start doing your banking online and you start purchasing things online, and you are putting those details out there and you know there are risks, I guess you have to weigh up the two sides of it: do you want like this easier lifestyle with the risk of losing it, or going down to the bank each

day? I guess everyone accepts that there is a risk and still use the internet.

This attitude is influenced by the pace with which the digital environment evolves and new technologies are developed. In practical terms it is seen as being difficult (if not impossible) to effectively police. There is a sense that you cannot really protect yourself (or be protected) in this continually evolving environment:

I think the other concern that I have is that in the olden days … protections were there in physical terms - police forces, people locking things up - and because the world hadn't changed that much these were effective.

With the digital age, the change has happened very quickly….and the protections and the regulations haven't kept pace: that is why phishing and spamming is a billion dollar industry… If there is identity theft … it is because the criminal element is actually ahead of the game, far ahead of the regulators of digital enforcement, of the policing of the internet.

Distinction between online transactions and interpersonal interactions

Another factor influencing attitudes towards risk-taking is a person's propensity to engage in the types of online activities they see as being intrinsically higher risk—interpersonal interactions (i.e. social networking or personal communications) as opposed to transactions with organisations/ institutions:

And I guess that is why I don't think about it as a risk, it doesn't affect my life at all. I don't think about it because I don't and I choose not to engage in a lot of the more public sort of forum, and I have never blogged in my life.

I wouldn't do any of that: not because I have made a moral decision but simply it is just not me … it is of no interest to me, it makes no sense to me whatsoever but that is purely who I am, that is just the way I live my life … so I don't see the small amount that I do as being high risk behaviour, so therefore it doesn't concern me at all.

Generational differences

Attitudes towards privacy were also pointed out by one participant as being generational, suggesting that a paradigmatic shift was driving loosening attitudes towards risk:

Now … you can communicate with hundreds of people straight away … and so I think that it is a different paradigm … someone of my generation, we don't have that 'I am open to everybody' type attitude, we are very reserved and we were brought up to be that way; privacy was important. [But] the kids in the new generation don't seem to have any concept of privacy or what it is like to be private. To have your 'privacy' is basically a different paradigm altogether.

Risk as a trade off for convenience

The nature of digital data itself is often a factor that influences the way risk is perceived. The speed and ease which it can be mined, searched and exploited is seen as a sufficient trade-off for the risk involved:

Online, an electronic database of even one megabyte has a huge amount of information, and it is very mobile, it is very quick to manipulate, you can search it in seconds and find particular people by filtering it.

Unspecified fear

A more general, and in some cases irrational or unjustified, fear may also be restricting or limiting participation in the digital environment. For example:

I use internet banking, email, but I don't do any of the social stuff like Facebook … as far as I am concerned they are sort of evil … I just have a really negative impression of them … it is not necessarily a rational feeling … you hear on the news about some teenager committing suicide because their Facebook friends have all condemned them[1]*.*

However, there is also a counter argument against this type of thinking, with a different participant saying:

I feel that the whole English speaking world has gone way overboard on this safety business.

Perceived magnitude of the risk

Attitudes toward risks also change with the scale of the risk:

Well it depends on the magnitude of the transaction and also the sensitivity of the personal information.

[1] Participant is referring to a recent high-profile situation that occurred in the United States on MySpace.

Risk mitigation strategies

This chapter discusses the range of strategies that are currently being employed to protect personal information online. These strategies can broadly be categorised as active and passive strategies.

Active risk mitigation strategies

Active strategies involve an individual making deliberate decisions and active choices in their online behaviour that assist in protecting the security of their personal information. Details of active risk management strategies employed (and the extent to which they are employed) by adult Australians are detailed below.

Password management

The main risk posed by lax password management is a breach in security, leading to unauthorised access to a site or online service. The key risk factors are the danger of:

> using one password for numerous sites.

> using a simple password/one that can be guessed.

> not changing passwords over time.

The main challenge that adult Australians report in the mitigation of such risks is being able to keep track of and remember the passwords that they have, with an additional risk factor being introduced if passwords are written down or stored in hardcopy (especially if stored near the computer). To facilitate this there was a distinct trend for adult Australians to maintain a roster of passwords, rotating between three or four.

Other strategies that adult Australians use to facilitate stronger password management include:

> using alpha-numeric combinations.

> adopting 'strong password' advice where available (when choosing a password the website will advise whether password security is weak, moderate or strong).

> adopting at a broader level the protocols that are mandated for password setting by either their online banking provider or by their employer (and considered to be best practice).

> using SMS validated or generated passwords where available.[2]

[2] System by which an individual receives a unique, one-time-use password via SMS each time they need to log into a given online application.

Managing email addresses and spam

In order to control how online email communications are both disseminated and received, adult Australians tend to have a hierarchy of email addresses and disclose them accordingly.

> Work email addresses are the most sensitive and are generally only used for business purposes.

> Personal email addresses are considered less sensitive than a work email address and more broadly used for personal communication and registration for online services. This email address is either provided by their Internet Service Provider (ISP) or is web-based (e.g. Hotmail, Gmail etc).

Predominantly, this management and selected usage of email addresses is largely due to what adult Australians describe as the 'inevitable onslaught' of spam which is a consequence of being online. To this end some adult Australians also discussed having a third or even fourth email address, known as their 'junk email', that is used in situations where spam messages are likely to occur once disclosure of the email address is made and is often a free web-based account.

Judicious use of credit cards and/or alternative payment facilities

With financial fraud being seen as a key risk associated with online activity, it is not surprising that adult Australians use a range of strategies to minimise the risk of such financial fraud occurring. These strategies centre on the judicious use of credit card details and payment facilities, including:

> Only using credit cards with reputable vendors—reputable vendors are large and well known, or known to the individual prior to transacting. Adult Australians also report looking for security accreditation such as Verisign, denoted by padlock symbols in the browser. This behaviour was relatively widespread in adoption, but by no means universal.

> Actively managing accounts by checking the balance of their credit cards periodically, checking for unauthorised payments and checking the details of authorised payments. Again this behaviour was relatively widespread in adoption, but by no means universal.

> Maintaining a specific credit card for online use only, where the credit limit that has been deliberately restricted (alternately, using a debit card with a limited balance). This was a lesser used strategy.

Several participants in the research reported that they rely on bank policy as an insurance against financial responsibility if theft occurs— that is, the bank will cover funds stolen online.

As an adjunct to strategies for managing the protection of credit card details, some adult Australians (particularly those using eBay) reported using alternative payment methods. PayPal (owned by eBay) and BPay are methods which employ third parties to distribute funds, alleviating the need to provide credit card details. Additional security is provided in that funds can be withheld for faulty or missing goods, and the schemes are backed by large, financially secure companies.

Controlling information shared on social networks and via online forms

There are two dynamics at play in terms of protecting personal information voluntarily shared on social networks:

> controlling *the information* that is posted

> controlling *access to that information*

Controlling the information that is posted involves *limiting* what is posted, choosing not to reveal or release certain pieces of information or types of information. In terms of what is considered to be best practice limitations this can include:

> personal identifiers such as date of birth, address, etc.

> photographs, especially those of children, or that reveal potentially embarrassing situations

> anecdotes or opinions, which, in a different context, may be seen as inflammatory or indiscrete.

While adult Australians cited the above examples of where discretion should be exercised in terms of the types of personal information disclosed, in practicality most of those actively engaged in social networking on a regular basis were routinely ignoring such suggestions and engaging in these types of activities.

For adult Australians who are highly engaged in social networking, releasing personal information is seen to be one of the key purposes of involvement on the social network, and hence discretion runs counter to the purpose. This is particularly true of novice users. Furthermore, the premise of social networking operates on a participation model whereby the trading of personal information is currency, i.e. you gain access to other people's personal information by disclosing your own.

Strategies used in controlling access to personal information discussed by adult Australians included:

> Using privacy settings on profiles; however it was apparent that there are often difficulties in understanding and applying settings, with an associated lack of understanding as to inherent limitations that these settings may provide in terms of the protection they afford. Individuals who are less engaged are unfamiliar with setting privacy controls and are instead more likely to restrict the information they post.

> Restricting access of all information to 'friends-only' viewing.

> Screening/vetting friends carefully, only accepting people that are known.

> On Facebook, setting up groups of friends and setting access levels.

> Monitoring photo tags on pictures uploaded to a friend's profile (or requesting the removal of such tags in order to ensure that your own security settings are not inadvertently able to be breached by friends of friends).

Participants in the research did note that they have no direct control over the information that other people post about them, or the metadata appended to photos such as tagging.

The other key aspect to the management of personal information provision related to transaction-related activities, such as the completion of online forms. Information management strategies in this context were largely consistent across all age groups and life stages.

> Typically, adult Australians fill in compulsory or starred fields only. This decision is based on judging whether the provision of such information is of relevance to the transaction being undertaken (with a view that if not compulsory it was typically not relevant).

> If the information required becomes too sensitive or too irrelevant to the task at hand, then a red flag is triggered and unless there is an overly compelling need for the transaction to be made the form will be abandoned in its entirety.

> Adult Australians were found to generally avoid the giving of their phone numbers to strangers but they will give it to commercial entities if necessary. To this end mobile phone numbers are seen as less sensitive than landlines because they are not linked to location and can be more easily monitored and calls screened. Likewise an email

address will be given in preference to a mobile number as again unsolicited or unwanted communications are felt to be more easily managed through this medium.

Passive risk mitigation strategies

Passive strategies relate to an individual's reliance on the software platforms or the security systems of providers to protect an individual's personal information. Trust is placed in the integrity of these systems to the extent that they are considered sufficient to protect the personal information of the individual.

These strategies include reliance upon password management being dictated by the protocols of the site with which the individual wishes to interact. This is particularly true in relation to online banking.

Similarly while an individual may have actively minimised risk through the purchase of a particular type of hardware known to be more secure, or the purchase and instillation of an anti-virus software, if the individual then relies on these active decisions alone to provide protection, then such a reliance strategy becomes passive. This is particularly true in relation to anti-virus software if updates are not regularly made.

The most effective of the passive strategies employed by adult Australians is the belief that, if an individual is not sure as to the validity of a communication, it is best to do nothing. This relates in particular to the ignoring of all unsolicited requests for password confirmation, financial details, etc.

Activities where risk mitigation strategies are generally absent

Although there is widespread knowledge as to what constitutes effective risk management strategies across a range of circumstances, there are nonetheless several areas where it has been identified that adult Australians have a limited understanding of how to best protect personal information in these contexts, or alternatively are not aware that there is a need for caution to be exercised. These situations include:

> End-user licensing agreements, with adult Australians often seeing this as being the fine print and something they have to accept if they wish to proceed with the online interaction. There is only limited understanding as to the incorporation within a licensing agreement as details (and permissions) covering the extent to which personal information can be stored, used and even shared.

> Location being revealed via a mobile device, with this being a new concept for consideration for most Australians. The potential for such information to be firstly accessed and secondly misused was considered to be an undesirable outcome, however as the likelihood of this occurring was also seen as remote, concern in relation to this was low.

> Bluetooth networking—there was little uptake of this application among research participants, largely due to unfamiliarity with the technology, and hence unfamiliarity with any inherent risks that may be contained in the usage thereof.

> Biometrics was another area where there was little uptake and understanding of the technology evident. For many research participants biometrics were considered to be almost science-fiction like in their application, with one respondent stating that if it came down to his security being breached then he would prefer that his password was hacked as opposed to his finger hacked off.

Sources of information

In terms of how adult Australians have developed their risk management knowledge and minimisation strategies, this education has typically been informal and largely gleaned

through discussions with families and friends, in general, and through consultation with that family member or friend known to be the 'IT expert', in particular. Such information is also being sourced through schools and brought home and shared by children.

Learnings gained through the workforce are also being transferred back into the home, particularly in relation to file protection and password management.

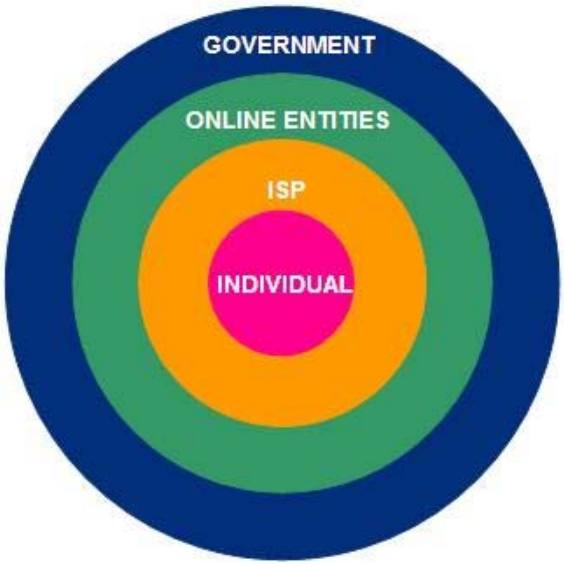
To a lesser extent there is also some reliance on the media, especially the technology press (notably the IT column in the Australian) in order to keep abreast of the latest trends and developments in security applications.

Responsibility for safeguarding personal information

Who is responsible?

Responsibility for the safeguarding or protection of personal information is considered to be multi-layered, with the individual, the ISP, the online entity and the government all having a role to fulfil:

Figure 3 Key players perceived as responsible for protection of personal information online



The role of the individual

There was a general consensus among participants that the first line of defence in the protection of personal information is at the individual level. Ultimately it was seen to be an individual's choice as to whether or not they provide personal information via digital media and communications. Hence any adverse outcomes from inappropriate use of personal information are considered to be a consequence of the individuals' decision to disclose. It was also seen to be the responsibility of the individual to ensure the safeguards necessary for the protection of any personal information they provide are in place prior to the provision of that personal information.

As one participant stated:

> *We certainly have to take responsibility ourselves for our own lives; I mean if you fall over a crack in the sidewalk, you shouldn't be suing the council for it… you watch where you walk and you are careful.*

This overarching sense of self or individual is largely underpinned by a faith in the integrity of the regulations and systems surrounding the storage and usage of such information. It is within this broader framework that ISPs, online entities and the government are perceived to have a role and level of responsibility.

The role of Internet Service Providers (ISPs)

Internet Service Providers (ISPs) are seen as being the means of connectivity between the individual and the world of digital media and communications. At a base level the role of ISPs in relation to the protection of personal information is considered to be the same as any other transaction-based business, entity or service with whom the individual interacts.

However, at a broader level it was felt that an individual had the right to expect that their ISP would act to restrict the volume of spam email received, provide protection against viruses and not use details of an individual's surfing behaviour for commercial applications.

It was felt that a potential role an ISP could play was in the area of education—providing its members with information on good practice for online behaviour and risk minimisation strategies when signing up with them.

> *If you sign up with a service provider, why can't that provider provide you with not just access but with the tools to protect yourself?*

The role of online entities

Participants used a variety of terms to refer to those entities on the internet with which they interact and disclose personal information, with such terms being either: the website domain name, the business name or the name of a government department, or being a generic description such as 'businesses', 'providers', the 'Government', etc.

The perceived role that each of these entities should, or could, play in regard to the protection of personal information which was provided/ disclosed to them was highly dependent upon the nature of the provision or disclosure. In general:

- Provision to commercial (including banks) and government entities was seen to be transactional in nature—high perceived responsibility of entity to protect personal information that they are provided.
- Disclosure to content providers and networking sites was seen to be more social/ informative in nature—high perceived responsibility of individual to manage what type and level of personal information they disclose and responsibility for controlling access to that information.

Commercial and government entities

As detailed previously, provision of information to commercial and government entities is largely transactional in nature and undertaken to obtain access to a service. In this instance the underlying decision to provide such information is based on an assessment as to the integrity of the service provider versus the requirement for the service itself.

> *It is a perception of what their security is compared to what you need.*

> *I am not so worried with the Australian ones because I know how harsh the compliance is in updating the security systems all the time, but some of the international ones I would never provide information on because I know that they don't have the same security protocols that we do.*

> *Faith in the people we are giving that information to, and that is where you filter out who you want to give it to and who you don't.*

Inherent within such an assessment of integrity is a belief that the commercial or government entity has sufficient safeguards and systems in place to ensure that all information provided is able to be uploaded in a secure format, and once provided is stored securely with minimal risk of third party access.

> *I would be more worried about people hacking into their stuff though; I mean banks have got a responsibility.*
>
> *It is not just that is you personally protecting your information it is them being obligated to also protect that information because you have to provide it you don't have a choice.*

The imperative for commercial and government entities to meet and maintain high standards and policies to protect the personal information that they have been provided is largely seen to be an issue of self-preservation and interest. More specifically, commercial and government online entities will seek to protect the personal information that they are provided in order to avoid the negative publicity and loss of business that would result from personal information being inappropriately used.

> *I think the people that you are giving the information to have got enough self-interest themselves and so on and so forth that they have got their own reputation to protect and they have got to make sure that they are a reliable place to put your money, and they are the people that are going to protect that end and you are going to protect this end.*

In a similar vein, commercial and government entities are seen to be able to be held accountable by an individual for any negative financial consequence that could occur as a result of a security breach.

That ethical businesses and entities should only use personal information for the purposes for which it was provided was also clearly expressed. In particular, detail as to how information would be used should be clearly stated and any provision of information to a third party provider should only be made with the express permission of the individual.

Adult Australians also have an inherent assumption that there is a regulatory framework in place that governs how commercial and government entities can use, and must protect, personal information in their possession.

Content providers and networking interfaces

With regard to the disclosure of information for the purposes of social interaction through sites such as MySpace and Facebook, it was seen to be the responsibility of such site administrators to provide sufficient safeguards which restrict access to posted information to approved viewers or friends only.

> *Well that is the thing, I only put on there what I want people to know, I mean they are only my friends, Facebook aren't giving other people that don't know me access to all this information.*

There is a seeming acceptance that such sites have potentially lower security parameters regarding the use of and access to personal information than those applied by more transaction-based online services such as businesses and government entities. As such, breaches of personal information security are considered more likely to occur.

Similarly, with participation in such networks seen as being entirely voluntary without transactional benefits being accrued, there was a sense that in participating, individuals had accepted the inherent risk of a personal information security breach. Thus, grounds for recourse to the site administrator are diminished.

There was also an expectation that any commercial use of personal information provided is made transparent, stipulated in clear English, and only done with the consent of the individual. In particular, this related to the use of details provided for unsolicited marketing offers.

Regulation as to inappropriate content being displayed on social interaction and networking sites was considered to be problematic and difficult to enforce due to the subjective nature of what is considered to be inappropriate. However, mention was made as to the expectation that, or need for, social interaction and networking sites to have a mechanism whereby inappropriate content could be reported.

The role of government

It was generally believed by participants that some form of regulation exists in relation to how operators in the digital space are required to protect the personal information they have in their possession. Associated with this belief was the further assumption that it is the government who has been (and continues to be) responsible for the application and enforcement of these regulations.

This assumption is largely based on default reasoning rather then upon actual awareness, with no specific recall being made of any government activity in this area. (NB: Spontaneous discussion was had in relation to the establishment by the government of the Do Not Call Register in the telecommunications space).

While there is clear consensus that the government is (or should) be playing a role in the regulation of how operators in the digital space are required to protect the personal information they have in their possession, there are a range of different viewpoints held as to what the nature and/ or scope of that role is.

More specifically, some participants expressed concern that government measures aimed at the protection of an individual's rights in regards to the protection of their privacy could in effect equate to censorship of information:

> *But I don't think they (the government) should be able to tell us what we can and can't look at.*
>
> *It's my choice.*

For other participants there was a sense that if government regulation in this area is too omnipresent it will lead to complacency and an abdication of self-responsibility:

> *They shouldn't be held responsible for everything I mean people are copping out all the time.*
>
> *I think you are aggregating the responsibility to government when it is the parent's responsibility to tell the children what to do.*

There was also a sense that the ability of the Australian Government to be an effective regulator for the protection of personal information provided through online activity is limited, given the borderless nature of the internet, and the anonymous nature of many operators in this space:

With the internet it is a whole different ballgame, and you haven't got that interface to prove that the person is over eighteen and whatever, I just I haven't got my head around how you protect and how you protect the young people and how you protect the rights of adults to choose for themselves.

Aside from fulfilling a regulatory role, the majority of participants felt that the government is ideally placed to play an educational role. It was felt there was a clear and compelling need for Australians to be better informed as to the potential risks involved in their provision or disclosure of personal information through online activities, as well as a need for greater education about the appropriate safeguards or risk minimisation strategies individuals should employ to protect the personal information that they choose to disclose.

The government was felt to be ideally placed to fulfil this role, given their resources and the credibility that would be attached to such communications if being endorsed by the government. It was also felt that this fell within the government's responsibility and mandate to anticipate and service the needs of Australians.

It was interesting to note that in each group, regardless of the life stage, there was a consensus that the need for education among adult Australians was not as necessary for their cohort as it was for the life stage or age cohorts above them.

Participants who tended to be transactional users felt that their own level of knowledge was sufficient to allow them to minimise the risk of their own activities. As such, they were more interested in learning about strategies to minimise risks associated with disclosure of personal information via social networking activities, with such education being largely so that they would be better equipped to safeguard and monitor the activities of their children.

In a related vein, it was also seen as being important (or even the priority) that education as to such matters targeted school-aged children, with teenagers generally viewed as being the most vulnerable due to a tendency to disclose personal information without thought as to potential consequences:

Well I don't see why the government can't play a role in educating us to you know, protect ourselves and our families and I suppose a good start is in schools, and unfortunately as you've said, it's failing but I suppose if parents were – like I don't think I've got the necessary tools to help my kids protect themselves on the internet because I don't know enough about it myself.

Implications of the research findings

Australians feel themselves to be relatively well informed as to how to protect their personal information online. This is undercut by a number of factors which will need to be addressed if online security is to be improved in real terms:

- Pervasive belief about the inevitability of a security breach acts as a barrier to risk management strategies, and in some cases is being used as an alibi for doing nothing. Australians need to be empowered in this regard; they need to feel that their actions will be effective.
- The pace of technological change means that with new technologies and platforms being added to the digital environment exponentially, new threats to privacy are constantly arising. Possible implications of this include:
    - In terms of perception this is daunting for many Australians: it perpetuates the belief that breaches are inevitable and makes it difficult for everyday users to stay in a position where they feel sufficiently informed to adequately protect themselves.
    - It is intimidating to novice users who struggle to learn the basics, let alone adapt to new technologies and platforms.
    - In practical terms it makes the job of educating people that much more difficult as new strategies need to be developed and disseminated in response to new threats.

Consequently, there is a danger that anxieties stemming from these factors can discourage full and open participation in the digital environment by some groups, and have negative impact in terms of social inclusion.

Research findings suggest that Australians are learning about protecting their personal information in largely informal ways. They indicate that they see a role for government education. The challenge for government is to utilise the full range of communication channels, including unorthodox channels such as workplaces and schools, to educate adult Australians. In this way, government can augment the informal learning that is currently occurring, and in so doing, counter the defeatist attitudes that are currently undermining Australian's efforts to manage the risks they face in the digital environment.

Appendix A

Focus group discussion guide—April 2009

Australian Communications and Media Authority Protecting personal information in the digital environment 27806	Focus Group Discussion Guide FINAL April 2009

		NB: PARTICIPANTS TO COMPLETE 'DIGITAL PROFILE' WORKSHEET PRIOR TO GROUP
AIM		OUTLINE OF DISCUSSION TO BE COVERED
Explain the research process and effect introductions		<u>Introductions</u> • Reassure re confidentiality, explain recording, role of moderator, purpose of the discussion, etc. • Recording – both audio and video. Also explain viewing and observers. • Ground rules • Introduction to project: *The research we are conducting is about people's attitudes towards the use of personal information on digital media and communications. When we talk about* ***personal information*** *we mean information that can be used to identify you, or which discloses things about you that you think are sensitive. When we talk about* ***digital media and communications*** *we mean the internet in general including commercial and non-commercial websites and social networking sites, mobile phones, other mobile devices like GPS navigators and other networks like Bluetooth.* • Participants to introduce themselves, family and interests, and home location
What are the attitudes to use of personal information on digital media and communications among adult Australians users of digital media and communications?		<u>1. Awareness of and sensitivity towards different types of personal information</u> We want to understand the different types of personal information that could be used or disclosed through digital media and communications. What types of personal information are there? As a group, write them down. PROMPT What else? Anything else? ALL TYPES TO BE WRITTEN ON SEPARATE CARDS ONCE SPONTANEOUS RECALL IS EXHAUSTED PROMPT FOR ANY OUTSTANDING: What about … • Your name • Religion • Health

		• Marital / Relationship status • Income • Address • Phone number • Credit card details • Banking details • Pictures • Physical location We want to understand how *sensitive* these different types of information are. As a group please rank them from the MOST SENSITIVE to the LEAST SENSITIVE. (Group to discuss and rank) For each information type discuss: (1) How is INFO TYPE sensitive/ not sensitive? What is it about INFO TYPE that makes in sensitive/ not sensitive? (2) UNPROMPTED: Does this sensitivity change under different circumstances/ context? Which circumstances/ context? (3) PROMPT FOR CONTEXT*:* What about … Does this sensitivity change when you are • Voluntarily sharing personal information on social networks? • Filling out an online form? • Using online banking facilities? • When your personal information is available through third party resources like Google Street View or Whereis? • When you are spammed (or receive unwanted communications)? • When your physical location can be revealed through a mobile device? (4) When using a mobile phone or other device? How secure is your personal information? Why do you say that? UNPROMPTED: What do you do to protect your personal information? When online? When using a mobile?
What is the understanding and awareness of risks related to use of personal information on digital media and communications among adult Australians users of digital media and communications?		<u>2. Awareness of and understanding of risks arising from disclosing personal information</u> UNPROMPTED: What are the different risks associated with releasing or using personal information online or through mobile devices? PROMPT What else? Anything else? For each information type: What are the risks in releasing INFO TYPE? How severe is the risk? Why do you say that? PROMPT FOR UNMENTIONED: And what do you think about … • Online fraud/ identity theft • Financial loss through scams • Damage to your reputation

		• Balancing your private life versus your career • Physical security – the risk of being harassed or stalked • Risks to children • Avoiding SPAM or other unwanted/ unsolicited information
What is the degree of awareness of and preparation to use different risk mitigation strategies?		<u>3. Risk mitigation</u> What things do you currently do to protect yourself from risks arising from putting personal information online/ on mobile phones or other devices? What else? Think about the following: • When managing you passwords? • Voluntarily sharing personal information on social networks? • Filling out an online form? • Using online banking facilities? • Accepting an online licensing agreement (End User Licensing Agreement) • Using other online payment facilities like PayPal or BPay • When your personal information is available through third party resources like Google Street View or Whereis? • When you are spammed (or receive unwanted information)? • When your physical location can be revealed through a mobile device? • When using Bluetooth networks? • Biometrics? • Using a Mac rather than a PC? How often do you follow through? Why? Why not? Have you heard of any other methods? Strategies friends and family use? What are they? Who should be responsible for protecting personal information? Why do you say that? PROMPT what about: • Government? • Internet service providers? • Content providers? • Media? • Members of the public? • Myself?

What are the information needs in relation to use of personal information online, related risks and existing risk mitigation strategies?		4. Other information Where do you currently get information about protecting your personal information? Which sources? Why do you trust these sources? What information would you like but haven't found?
To ensure all relevant points have been covered and check for any questions from observers		6. Summary and Conclusions • Summarise main points • Any other thoughts before we finish up • Check if any questions from observers THANK PARTICIPANTS AND CLOSE

Canberra
Purple 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
TTY 03 9963 6948

Sydney
Level 15 Tower 1
Darling Park
201 Sussex Street
Sydney NSW

PO Box Q500
Queen Victoria Building
Sydney NSW 1230

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

acma research

www.acma.gov.au