# 5

# Breaches of privacy and identity theft

## Introduction

5.1 This chapter explores the links between identity theft and breaches of privacy, and also addresses the complexities of third parties collecting personal information.

## *Privacy Act 1988* (Cth)

5.2 The *Privacy Act 1988* (Cth) does not make special reference to young people, on the basis that they have the same rights to privacy as adults. In practice, primary care-givers are usually responsible for exercising their rights under that Act until individuals reach levels of maturity and understanding to make independent decisions.[1]

5.3 The Office of the Privacy Commissioner commented that:

> this approach to the privacy of young people is appropriate, as it accommodates different rates of development. Mature young people are entitled wherever possible, to make decisions about their personal information as soon as they are able, rather than on reaching a prescribed age. It is the Office's view that this level of autonomy should be maintained in respect of young people's privacy.[2]

---

1 Office of the Privacy Commissioner, *Submission 92*, p. 4.

2 Office of the Privacy Commissioner, *Submission 92*, p. 4.

5.4 However, the NSW Government expressed concern that:

> children's privacy is subject to some specific risks. Children and young people are more vulnerable in the sense that they are less likely to have the nous or capacity to be alerted to potential privacy breaches, to read and understand the fine print of contracts with internet service providers and web page administrators, or to know what action may be available to them if their privacy is breached.[3]

5.5 Australian privacy legislation does not impose any obligations on individuals acting in a private capacity, but instead relates to how organisations deal with the personal information of others. As there are also exemptions for small businesses with annual turnovers of $3 million or less, a large proportion of the Australian private sector is not subject to any privacy laws.

5.6 Such legislation may be insufficient to protect young people from cyber-safety risks occurring as a result of individuals acting in private capacities.[4] The Victorian Privacy Commissioner stated that:

> I have identified in the submission the gaps in privacy laws, with one of the greatest being small business exemption and also the fact that privacy laws do not apply to individuals acting in a private capacity. That gap was identified by the Australian Law Reform Commission, which recommended that it be filled by a statutory tort of privacy.[5]

5.7 The Committee supports Recommendation 3 in the Senate Environment and Communications References Committee's recent Report.[6] It therefore recommends:

3 NSW Government, *Submission 94*, p. 14.

4 Victorian Privacy Commissioner: *Submission 59*, p. 3; Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, pp. CS68, 79.

5 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS68.

6 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

**Recommendation 4**

**That the Australian Government consider amending small business exemptions of the *Privacy Act 1988* (Cth) to ensure that small businesses which hold substantial quantities of personal information, or which transfer personal information offshore, are subject to the requirements of that Act.**

5.8 The Committee supports Recommendation 3 in the Senate Environment and Communications References Committee's recent Report.[7] It therefore recommends:

**Recommendation 5**

**That the Australian Privacy Commissioner undertake a review of those categories of small business with significant personal data holdings, and make recommendations to Government about expanding the categories of small business operators prescribed in regulations as subject to the *Privacy Act 1988* (Cth).**

## Privacy and young people

5.9 Young people desire to maintain a degree of privacy but are less cognisant than adults about what privacy actually entails. For example, young people most often discuss privacy in the context of independence from their parents or teachers, and not in the adult or legalistic way of appropriately securing private personal information.[8]

5.10 The Mental Health Council of Australia identified privacy as one of five major risks for young people, with potential impacts on their health and well-being.[9] The Consultative Working Group on Cybersafety believed that inappropriate handling of private information was likely to be

7 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix. Tabled on 7 April 2011.

8 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 5; Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS71.

9 Mental Health Council of Australia, *Submission 52*, p. 4.

significant and have long-term implications for Australians into the future.[10]

5.11 The Office of the Privacy Commissioner stated that little Australian research has been done about the awareness or attitudes of young people to privacy issues.[11] The Association of Independent Schools of SA submitted:

> It is apparent that many students are not fully cognisant about the permanent nature of postings on the Internet. It appears they lack the foresight to realise that once a photo, phone number or rumour is posted onto the Internet, it is out of their control. An example used in schools to teach children about this is asking them if they would like that photo enlarged and shown at school assembly.[12]

5.12 However, the Victorian Privacy Commissioner commented that:

> It is certainly the case in my view that young people do value their privacy and are open to understanding and educating themselves about how they can make themselves safer online.[13]

5.13 The 2010 Social Networking Education and Awareness Campaign run by the South Australian Government recorded 'a large number' of concerns about the level of access others can have to an individual's information. These concerns included:

- Over-sharing of personal information;
- Third party access to information;
- Apathy about privacy settings;
- Lack of information on how information can be used for identity theft;
- Being too trusting and accepting anyone as a 'friend';
- Pressure to collect 'friends'; and
- If an individual has many 'friends', many other people can have access to her/his information.[14]

---

10 Consultative Working Group on Cybersafety, *Submission 113*, p. 9.

11 Office of the Privacy Commissioner, *Submission 92*, p. 5.

12 Association of Independent Schools of SA, *Submission 19*, p. 11.

13 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS69.

14 South Australian Office for Youth, *Submission 98*, p. 3.

5.14 The Office of the Privacy Commissioner expressed concern that:

> The available evidence suggests that more effort needs to be directed to ensuring young people gain the skills needed to make sensible decisions around privacy and to understand their rights and obligations under the Privacy Act.[15]

5.15 The many ways of interacting on the online environment exposes people to a wider public than is possible offline. Young people are particularly at risk, as they frequently post personal and identifying material without being fully informed of the consequences and risks.[16] Chapter 4 noted in the discussion of cyber-stalking, potential offenders often do not have to look long for targets because personal information about other people is so easily found online.[17] Chapter 7 provides the results of the Committee's consultations with young people about their perceptions of what it is appropriate to post online.

5.16 When people go online, a 'disinhibition effect' occurs: there are no consequences when they put things on the screen. The online environment speeds up the disclosure process, so that what would normally take a long time to disclose face-to-face happens quickly and without incurring an immediate, visible consequence. Young people are therefore more likely to post material online without considering possible consequences.[18]

5.17 Young people can also be victims of their peers, as online identities can be assumed and used as part of abuses such as cyber-bullying. Email accounts can be opened in other names to send malicious emails. Embarrassing or hurtful material can be sent after social networking accounts have been hacked into, or passwords shared and then re-used maliciously.[19]

5.18 Armorlog International noted that many networks do not prevent users using easily guessed passwords, and allow user names and passwords to be stored in Internet browsers:

> Some networks have unfortunately incorporated procedures in the management of their systems, sometimes in order to try and control fraud, that inadvertently actually result in greater amounts

15 Office of the Privacy Commissioner, *Submission 92*, p. 5

16 Australian Psychological Society, *Submission 90*, p. 11.

17 Alannah and Madeline Foundation, *Submission 22*, p. 19.

18 Dr Barbara Spears, Senior Lecturer, School of Education, University of South Australia, *Transcript of Evidence*, 11 June 2010, p. CS25.

19 Attorney-General's Department, *Submission 58*, p. 7; Ms Kelly Vennus, Programs and Training Manager, Stride Foundation, *Transcript of Evidence*, 9 December 2010, p. CS18.

> of private information being revealed about users that actually facilitates identity crime as it provides opportunities for fraudsters to accumulate further knowledge about a target that assist in change user details to take over their accounts & thus identity.[20]
>
> Most networks facilitate users duplicating passwords used elsewhere. When this occurs users are at greater risk in regard to identity theft.[21]

5.19 Similarly, the Committee's *Are you safe?* survey asked if respondents had felt unsafe online. Many respondents chose to comment in free text spaces to explain their answer. The following comment was submitted in response to that question:

> i was chatting to a friend of mine, but slowly realised that it didn't seem like her. i asked and they replied that they were her cousin. without writing anything else i signed of and deleted that account (Female aged 16).[22]

5.20 The Murdoch Children's Research Institute referred to anecdotal evidence linking cyber-bullying to breaches of privacy. People often use the same password for many accounts and, if this can be guessed by a friend, it can be used to post bullying material about others, posting embarrassing stories or photos.[23]

## Privacy settings

5.21 The South Australian Office of Youth have found that a large proportion of people do not engage their privacy settings.[24] While notices and settings exist on the majority of sites, including social networking sites, ways of protecting privacy are often so complex and difficult that people frequently do not examine, understand or even set them.

---

20 Armorlog International, *Submission 4*, p. 3.

21 Armorlog International, *Submission 4*, p. 2.

22 For authenticity, throughout the Report, emails from young people have been incorporated in the form received.

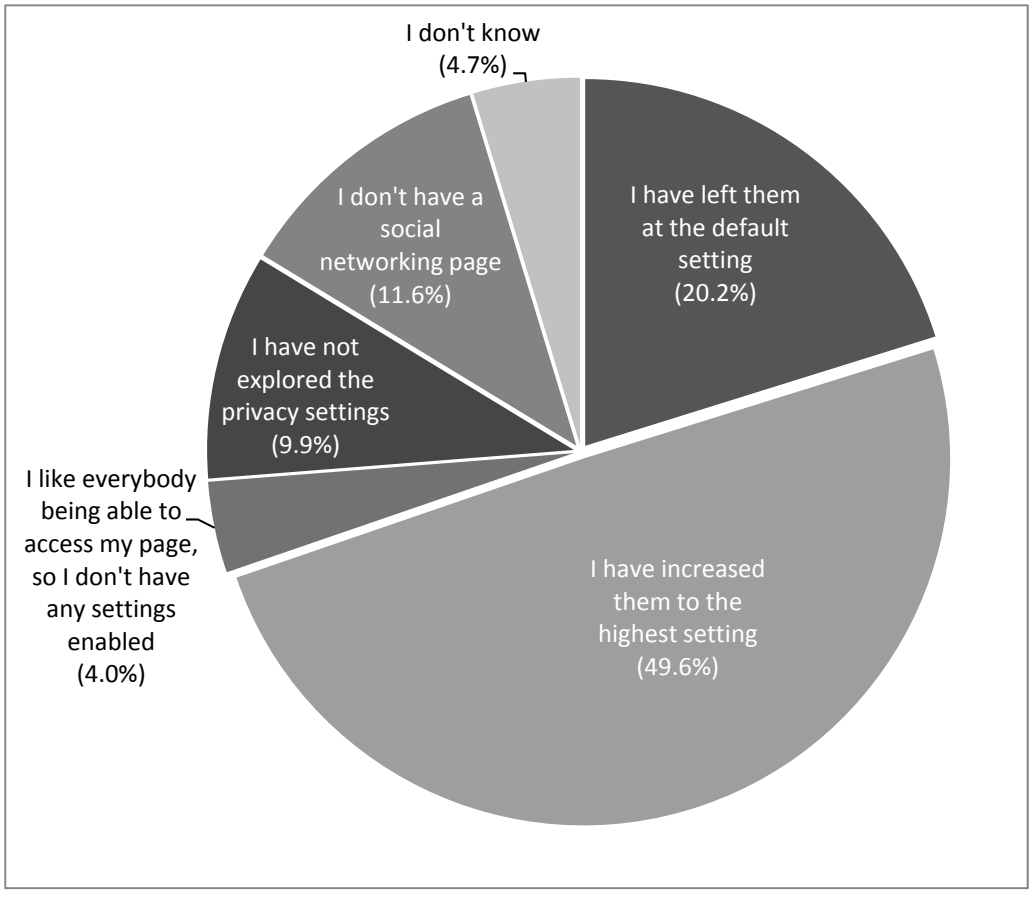
23 Murdoch Children's Research Institute, *Submission 111*, p. 4.

24 Mrs Tiffany Downing, Director, South Australian Office of Youth, *Transcript of Evidence*, 3 February 2011, p. CS25.

5.22 The *Are you safe?* survey asked participants aged 13 years and over about their use of privacy settings on their social networking and gaming sites. The survey found:

- 49.6 percent identified they had increased them to the highest setting;
- 20.2 percent identified they had left the settings at the default level;
- 9.9 percent identified they had not explored the privacy settings at all; and
- 4.0 percent identified that they have disabled all privacy settings to allow everybody access.

Figure 5.1 Have you explored the privacy settings of your social networking pages?




5.23 Figures 5.2a and 5.2b show the differences in between male and female respondents.

Figure 5.2a Have you explored the privacy settings on your social networking pages? *(Female)*

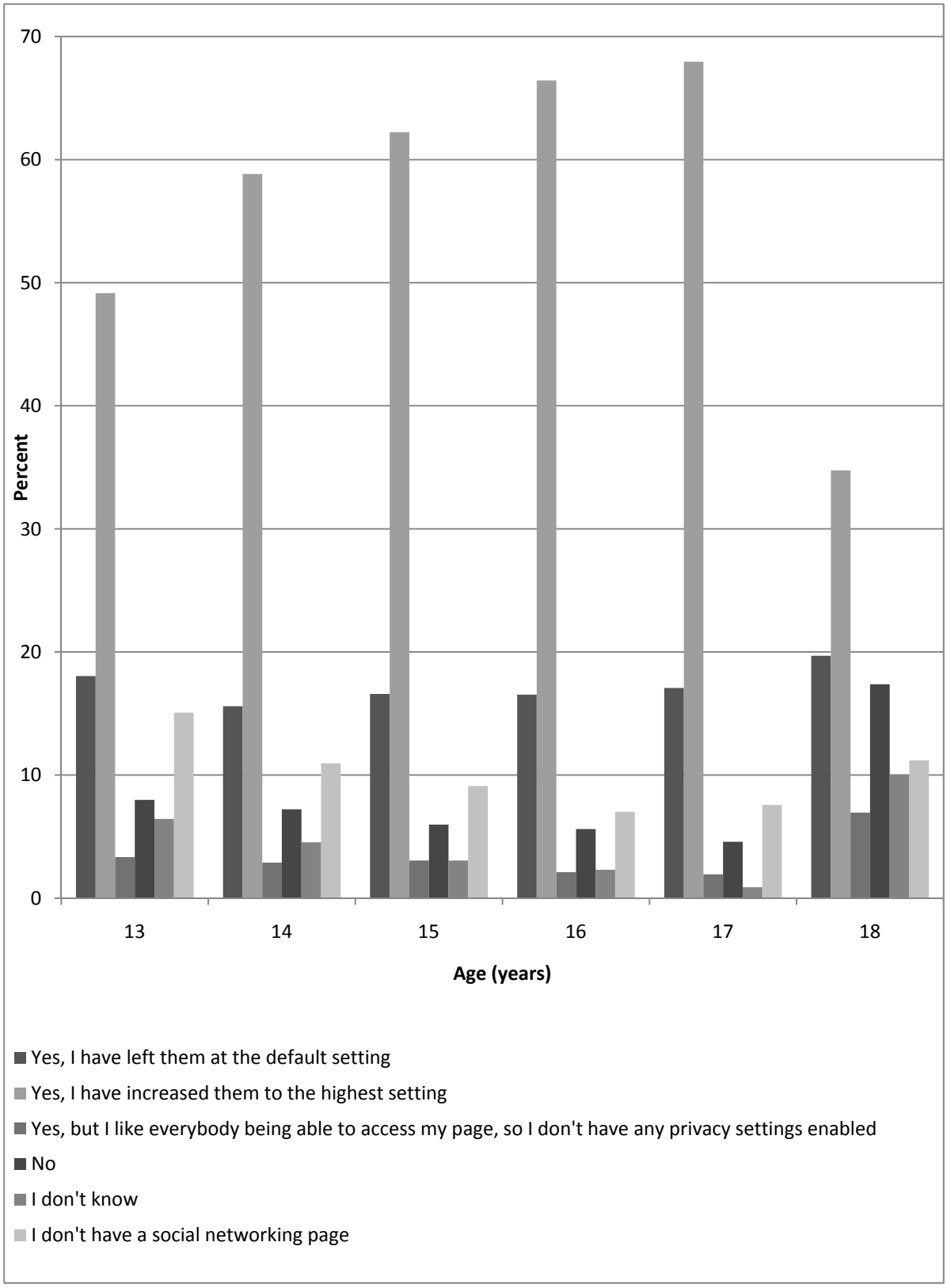


Figure 5.2b Have you explored the privacy settings on your social networking pages? *(Male)*

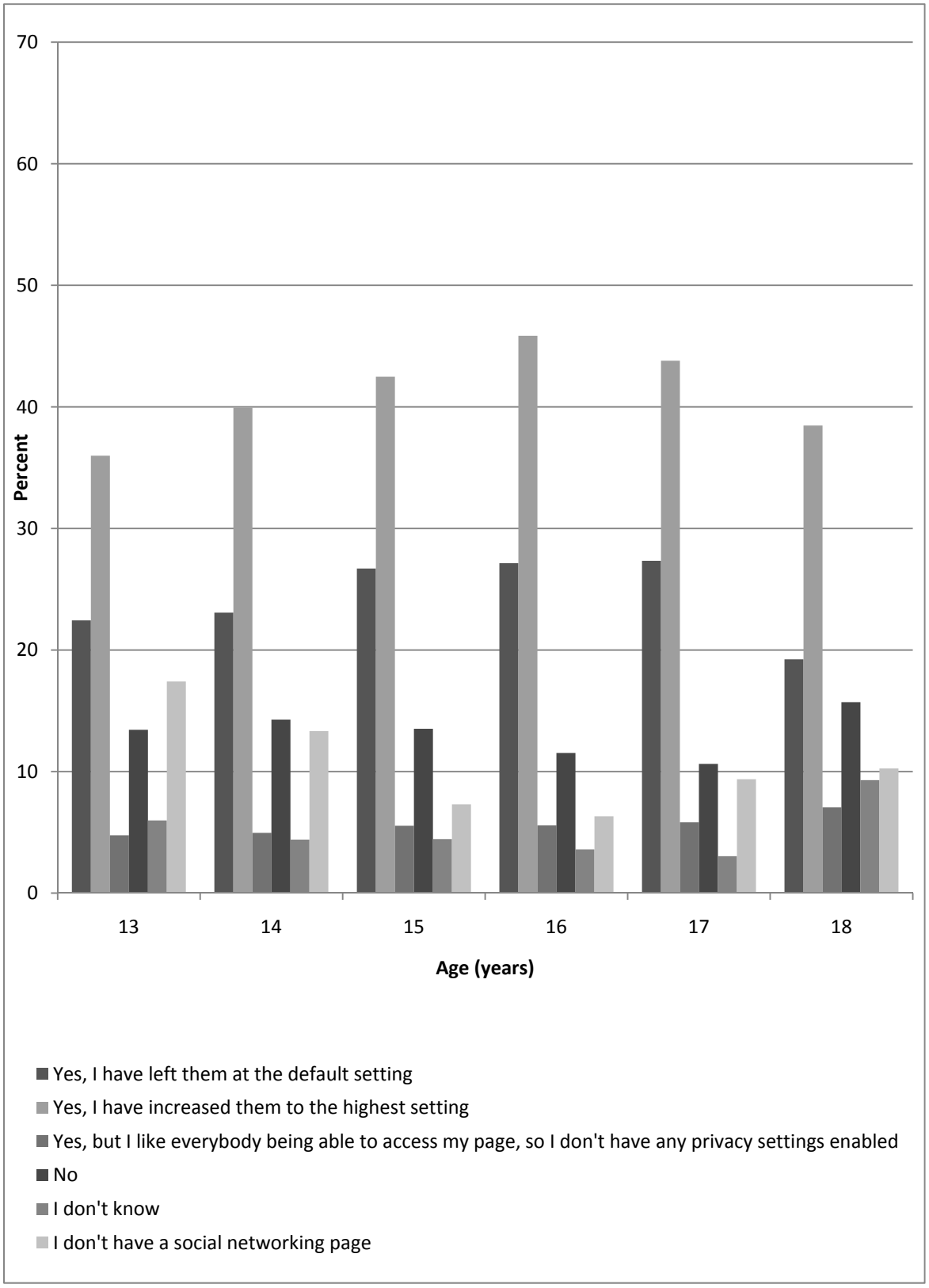


Table 5.1 Have you explored the privacy settings on your social networking pages?

| | | Yes, I have increased them to the highest setting | | Yes, I have left them at the default setting | | Yes, but i like everybody being able to access my page, so i don't have any enabled | | I don't have a social networking page | | I don't know | | No | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Sex* | *%* | *#* | *%* | *#* | *%* | *#* | *%* | *#* | *%* | *#* | *%* | *#* |
| 13 Years | M | 36.0 | 680 | 22.4 | 424 | 4.8 | 90 | 17.4 | 329 | 6.0 | 113 | 13.4 | 254 |
| | F | 49.1 | 1207 | 18.0 | 443 | 3.3 | 82 | 15.1 | 370 | 6.4 | 158 | 8.0 | 196 |
| 14 Years | M | 40.0 | 644 | 23.1 | 372 | 5.0 | 80 | 13.3 | 215 | 4.4 | 71 | 14.3 | 230 |
| | F | 58.8 | 1166 | 15.6 | 309 | 2.9 | 57 | 10.9 | 217 | 4.5 | 90 | 7.2 | 143 |
| 15 Years | M | 42.5 | 506 | 26.7 | 318 | 5.5 | 66 | 7.3 | 87 | 4.5 | 53 | 13.5 | 161 |
| | F | 62.2 | 855 | 16.6 | 228 | 3.1 | 42 | 9.1 | 125 | 3.1 | 42 | 6.0 | 82 |
| 16 Years | M | 45.8 | 370 | 27.1 | 219 | 5.6 | 45 | 6.3 | 51 | 3.6 | 29 | 11.5 | 93 |
| | F | 66.4 | 663 | 16.5 | 165 | 2.1 | 21 | 7.0 | 70 | 2.3 | 23 | 5.6 | 56 |
| 17 Years | M | 43.8 | 173 | 27.3 | 108 | 5.8 | 23 | 9.4 | 37 | 3.0 | 12 | 10.6 | 42 |
| | F | 68.0 | 386 | 17.1 | 97 | 1.9 | 11 | 7.6 | 43 | 0.9 | 5 | 4.6 | 26 |
| 18 Years | M | 38.5 | 120 | 19.2 | 60 | 7.1 | 22 | 10.3 | 32 | 9.3 | 29 | 15.7 | 49 |
| | F | 34.8 | 90 | 19.7 | 51 | 6.9 | 18 | 11.2 | 29 | 10.0 | 26 | 17.4 | 45 |

5.24 Figures 5.3a and 5.3b show the levels of concern about cyber-safety of those that have left their privacy settings at the default level. Similarly, Figure 5.4 shows that the majority of those respondents who have left their privacy settings on default, have not felt unsafe online.

Figure 5.3a Of those with privacy settings left at default, are they worried about their safety online? *(Female)*

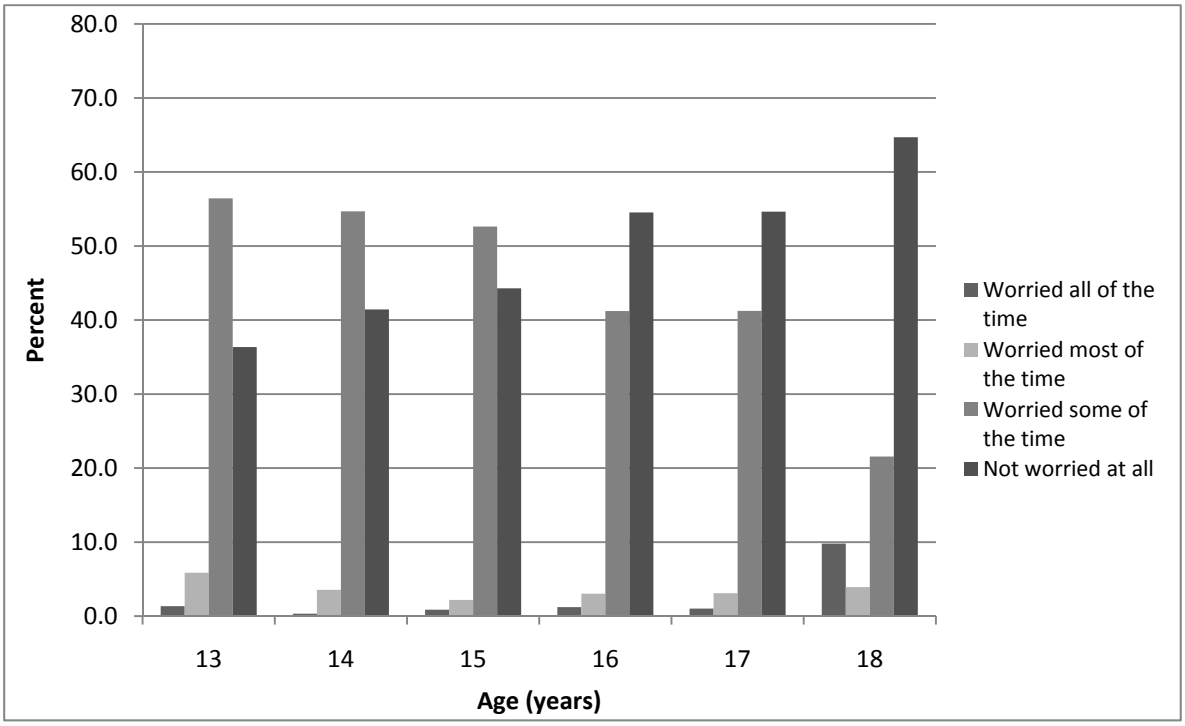



Figure 5.3b Of those with privacy settings left at default, are they worried about their safety online? *(Male)*

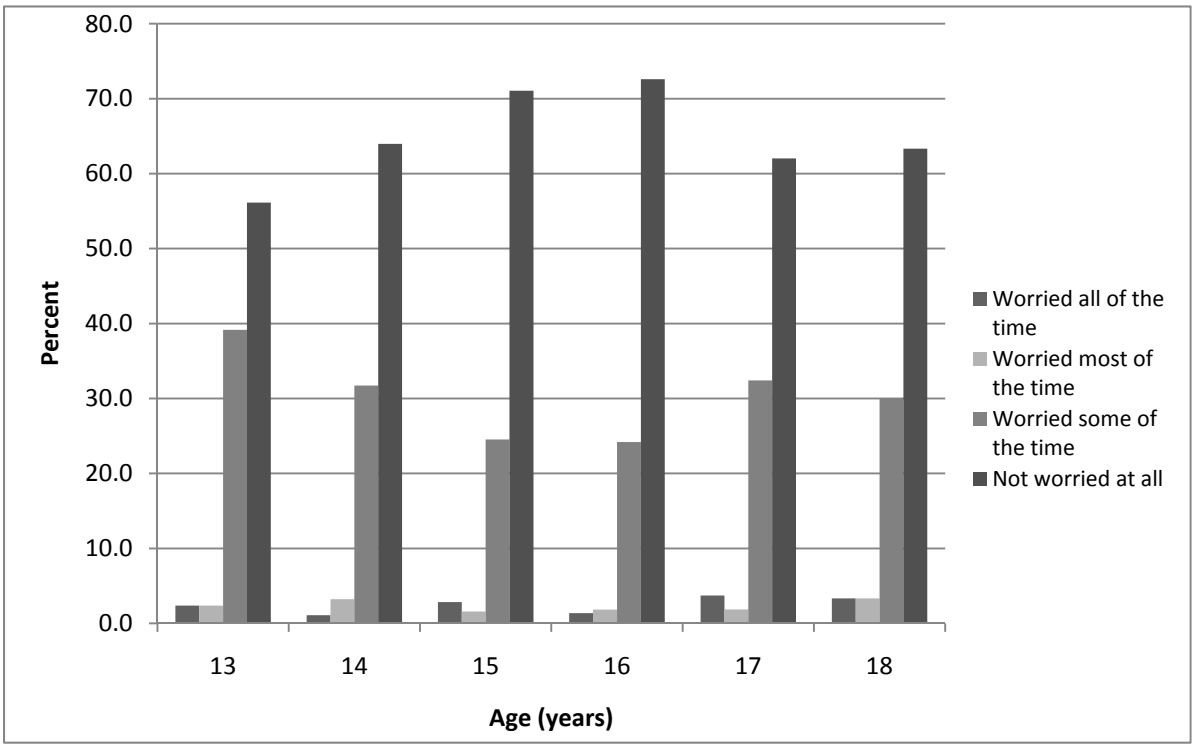
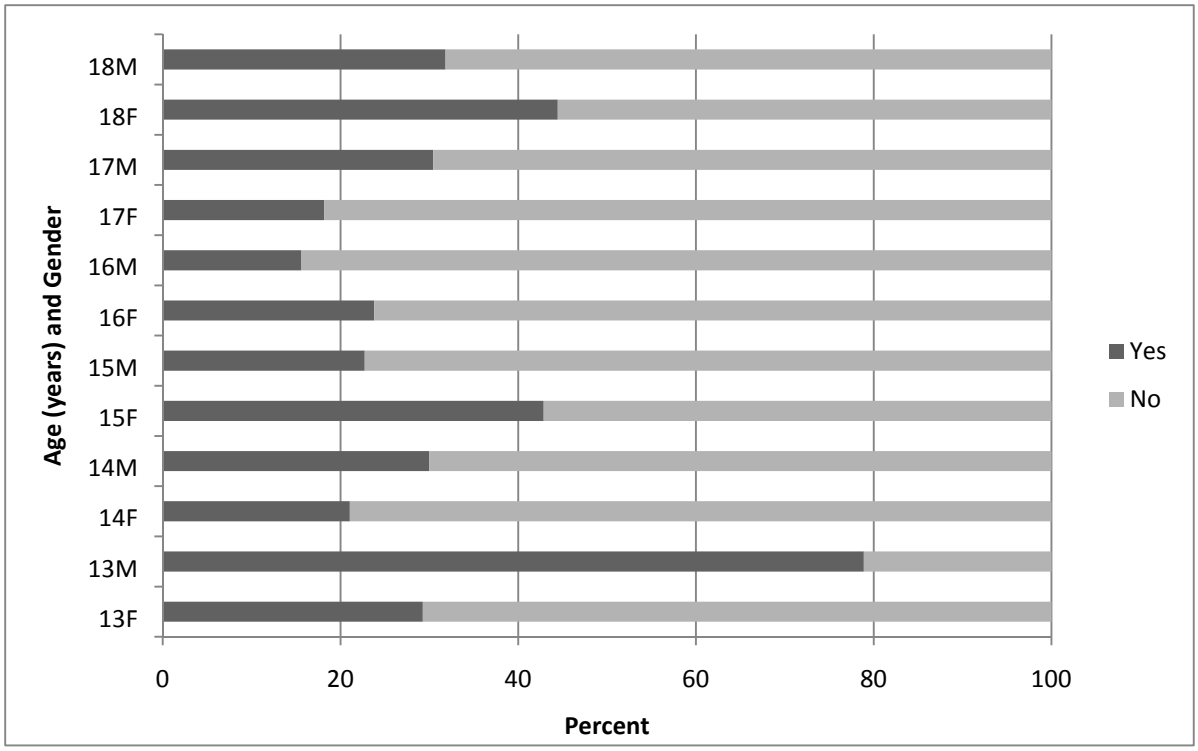


Figure 5.4 Of those with no privacy settings, have they felt unsafe online?




5.25 Canada's Privacy Commissioner investigated Facebook's privacy settings and found serious gaps in its handling of default settings that there was no privacy for anyone joining it. This resulted in changes to Facebook's privacy settings so that users had more control over personal information.[25] The Youth Affairs Council of South Australia suggested that:

> websites frequented by children and young people often have privacy policies that are wordy and difficult to understand. YACSA would strongly support AYAC's proposal that the government implement strategies to promote the use of youth-friendly, plain language privacy policies for online services, so young people can make an informed decision about disclosing their personal information.[26]

25 Victorian Privacy Commissioner: Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, pp. CS71, 79; *Submission 59*, p. 7; Mrs Tiffany Downing, South Australian Office of Youth, *Transcript of Evidence*, 3 February 2011, p. CS25.

26 Youth Affairs Council of South Australia, *Supplementary Submission 25.1*, pp. 16-17.

5.26 Ms Candice Jansz has found the default for privacy settings is an 'opt out' manner and they are constantly changing. She also commented on the capacity of young people to keep up with these changes:

> What is heartening is that young people are now illustrating considerable cognitive adaptations to the online environment, and take steps to actively manage their own privacy and safety, whilst still reaping the benefits of these powerful technologies.[27]

5.27 Privacy settings must be in 'very plain language – that is they are simple, short, clear and to the point'.[28] Further, representatives from the South Australian Office of Youth similarly commented:

> It would also be helpful if, when you set up an account, there were more prompts around setting up your privacy before you can finalise that, so that you have to do it as part of your setup.[29]

5.28 Facebook, however, pointed out that:

> there are many more pop-ups and direct engagement with users to tell them that if you click on this you need to see your privacy settings: 'click here'. There is much more engagement and, in fact, Facebook was the only site in history to ever take all of its users—I think this was about a year ago—and send them a message that said, 'You cannot continue to use Facebook unless you review your privacy settings, make adjustments that you want, and confirm.' That is something that is unheard of on the internet. I think that there is much more user engagement on Facebook. In fact, Facebook has also allowed users to vote on the privacy policy and vote on the terms of service.[30]

5.29 The results of a survey in 2007 by the Office of the Privacy Commissioner suggested that awareness of privacy had increased since 2004. Younger respondents, aged 18 to 24, continue to be less aware of their privacy rights than older respondents. The survey also showed that 50 percent of respondents were more concerned about providing information over the Internet than they had been two years earlier. However, a higher

---

27 Ms Candice Jansz, S*ubmission 44*, p. 4.

28 Dr Russell Smith, Principal Criminologist, Manager Global Economic and Electronic Crime Program, Australian Institute of Criminology, *Transcript of Evidence*, 24 March 2011, p. CS12.

29 Ms Suellen Priest, Policy and Program Officer, Office of Youth SA, *Transcript of Evidence*, 3 February 2011, p. CS26.

30 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, pp. CS7-8.

proportion of respondents aged 18 to 24 claimed to be less concerned than other age groups.[31] The Australian Youth Affairs Coalition stated:

> According to the Office of the Privacy Commissioner, the number of young Australians were concerned about internet privacy has quadrupled in past two years. However factors like peer pressure and incentives (such as quizzes, prizes or discounts) lead young people to disclose personal information online. AYAC believes education and transparency are key to supporting and empowering young people.[32]

5.30 The Office of the Privacy Commissioner survey also indicated that young people were less concerned about disclosing their financial information, and much more likely to disclose personal information to receive a discount, a reward or a prize. Such behaviour, and being less informed about privacy issues, could put them at risk of identity theft.[33]

5.31 The Victorian Privacy Commissioner believed that young people valued their privacy and were open to understanding and educating themselves about how they can make themselves safer online.[34] Recommendations made by a Senate Committee, in a report tabled in April 2011, suggest that all users of the online environment need more education about privacy.[35]

5.32 The Committee supports Recommendation 2 in the Senate Environment and Communications References Committee's report: [36] Accordingly, the Committee recommends:

---

31 Office of the Privacy Commissioner, *Submission 92*, p. 5. See www.privacy.gov.au/publications/rcommunity07.pdf for this survey. Accessed 9 February 2011.

32 Australian Youth Affairs Coalition, *Submission 28*, pp. 9-10, citing Office of Privacy Commissioner (2007) *Community Attitudes to Privacy*, Office of Privacy Commissioner, p. 61.

33 Office of the Privacy Commissioner, *Submission 92*, p. 5; Victorian Privacy Commissioner, *Submission 59*, p. 4.

34 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS69.

35 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

36 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

**Recommendation 6**

**That the Office of the Privacy Commissioner examine the issue of consent in the online context and develop guidelines on the appropriate use of privacy consent forms for online services and the Australian Government seek their adoption by industry.**

## Identity theft

5.33 Identity theft is a broad concept. It occurs when personal information, such as date of birth, credit card details, driver's licence numbers or passport or other identifying material, is obtained and is used to obtain a benefit or service. The Alannah and Madeline Foundation stated:

> Prevalence of identity theft among young people is difficult to establish, as most does not involve criminal activity as such. Indeed a recent ACMA study suggests that young people have 'a high level of awareness of the risks of Internet use particularly when involved in social networking on the Internet'.[37]

5.34 There have also been reports of social networking accounts being compromised for other purposes including fraud purposes.[38] For example, the Attorney-General's Department submitted:

> We also know of children and young people who have had experiences of unknown others using their photos and in some cases assuming their identity, resulting in them receiving a detrimental credit rating.[39]

5.35 It can also include use of an identity to harass or stalk a third person, and therefore activity of this kind can evolve into cyber-stalking.

5.36 While this theft is often associated with financial loss for adults, it can have serious consequences for young people if their information is used to fabricate fake documents, such as passports, or to commit further cyber-crimes.[40] The Federation of Parents and Citizens' Associations of NSW commented:

---

37 Alannah and Madeline Foundation, *Submission 22*, p. 27.

38 Attorney-General's Department, *Submission 58*, p. 7.

39 Childnet International, *Submission 18*, p. 4.

40 Office of the Privacy Commissioner, *Submission 92*, p. 6; Victorian Privacy Commissioner, *Submission 59*, p. 3

> Children and adolescents are often not even aware of the meaning of identity theft. They may fill out a profile on the internet pretending to be another student from their class or use another student's photograph without realizing the potential harm that they may cause. It is essential to educated people about possible risks especially with the many pathways available to access the online environment.[41]

5.37 Comments submitted in free text spaces of the Committee's *Are you safe?* survey indicate that the awareness of young people is growing in Australia. When asked if they had felt unsafe online, the following comment was made:

> I feel that identity theft is a huge issue, your name is the only secure piece of information i feel safe with sharing, i used to post other personal information but deleted it once i realised the risk (Male aged 14).

5.38 In 2007, the Australian Bureau of Statistics undertook a study of personal fraud with over 14,000 respondents aged over 15 years. The survey found that those from 25 to 34 years had the highest reports of identity theft (4.3 percent) against 2.1 percent of those aged 15 to 24 years. The 2007 Office of the Privacy Commissioner survey of people 18 years and older found that only 2 percent of respondents aged from 18 to 24 years had reported identity theft or fraud, compared with 9 percent of the total sample. While there is no immediate economic value in stealing a child's identity, once that person is 18 years old that identity becomes valuable. It can be used to apply for a 'proof of age' card, a driver's licence, passport or credit card. There is, therefore, a risk that criminals will collect personal information and wait before using the stolen identity.

5.39 Some young people also publicise personal information about parents, siblings and friends, thus exposing other people's information to the risk of identity theft.[42]

5.40 The Australian Bureau of Statistics estimated that 806,000 Australians over the age of 15 had been the victims of personal fraud in the previous year,[43] costing nearly $A1 billion per year.[44]

---

41 Federation of Parents and Citizens' Associations of New South Wales, *Submission 76*, p. 4.

42 Attorney-General's Department, *Submission 58*, p. 7.

43 Commander Grant Edwards, Acting National Manager, High Tech Crime Operations, Australian Federal Police, *Transcript of Evidence*, 24 March 2011, p. CS3.

44 Attorney-General's Department, *Submission 58*, p. 7.

5.41 Preventing these crimes is also important in reducing the threat of terrorism and other serious criminal activity often based on the use of false or multiple identities.[45]

5.42 In the past decade, there has been increasing awareness of the dangers posed by this abuse, but the Attorney-General's Department noted that there was a 'paucity' of data relating to young people and identity theft.[46] The Office of Privacy Commissioner added that:

> ... a range of measures are required to empower individuals to protect themselves in online environments and are essential to promoting effective privacy and cyber safety. These measures can include promoting education and awareness of the:
>
> - risks posed by various ICT environments and interactions;
> - measures that can be taken to mitigate risk, whether through technology or individual behaviour; and
> - remedies available should something go wrong.[47]

5.43 While the use of a pseudonym can be for constructive purpose for protection,[48] they can also be used:

> ... for the purpose of misleading people as distinct from merely covering one's most commonly used identity. I do not think that the incidence of this is vast but the impact of the individual instances can be quite significant. At this point we are talking about the concept of identity fraud. Identity theft goes much further. It is rare; it involves identity fraud being performed so comprehensively that the individual who used to use the identity cannot afford to keep using it.[49]

5.44 As so little is known about their awareness of identity theft, more research is needed to establish how Australian children view privacy, identify their concerns and work with them to develop effective strategies against this abuse.[50] The following comments were made highlighting the numerous topics requiring more research and development of policy options:

> Consideration need to be given to how organisations who work with children can best protect the privacy of children as

45 Attorney-General's Department, *Submission 58*, p. 7.
46 Attorney-General's Department, *Submission 58*, pp. 6- 7.
47 Office of the Privacy Commissioner, *Submission 92*, p.7.
48 Dr Roger Clarke, *Transcript of Evidence*, 21 March 2011, p. CS28.
49 Dr Roger Clarke, *Transcript of Evidence*, 21 March 2011, p. CS29.
50 Victorian Office Child Safety Commissioner, *Submission 30*, p. 5

> organisations increasingly use ICT to capture, record and share information about children.[51]
>
> Hacking often relates to unique complications specific to the digital age, but may also involve something as timeless as friends betraying one another's trust after sharing their passwords. Either way, the situation requires an appropriate legal, educational and policy framework to deal with these complications.[52]
>
> With the rise of online social networking sites and instant messaging programs, additional issues related to identity theft such as impersonation and the use of fake accounts for cyber-bullying purposes are becoming increasingly prevalent.[53]

5.45 Since 2005, measures have been taken that were intended to make it more difficult for criminals to create new identities or incorporate fabricated or inaccurate information into false credentials.[54] However, it is still the case that:

> Most networks facilitate users duplicating passwords used elsewhere. When this occurs users are at greater risk in regard to identity theft.[55]

## Collection of unnecessary information

5.46 In their dealings with organisations, some young people disclose significant amounts of personal information. As has been shown, this can be used for a variety of illegal purposes with possible consequences for those individuals later in their lives.

5.47 Inclusion of 'mandatory' fields in online documents was seen as a specific problem: unless they are filled in, it is not possible to complete some online documents.

> We need to bear in mind that information collected through the use of mandatory fields is sometimes used for unrelated purposes, such as marketing, statistics, advertisements or even profit motives. Our submission refers to the fact that the sale of information databases is a large industry in the United States. I remind the committee that social networking sites such as

51 Victorian Office of the Child Safety Commissioner, *Submission 30*, p. 5.
52 National Children's and Youth Law Centre, *Submission 138*, p. 8.
53 Office of Victorian Privacy Commissioner, *Submission 59*, p. 3.
54 Attorney-General's Department, *Submission 58*, pp. 6, 7.
55 Armorlog International, *Submission 4*, p. 2.

> Facebook insist that real people register. Obviously that is for good reason but it does mean that people are again forced to provide quite a lot of personal information. For example, Facebook limit the age of people who use it to 13 years and over, but of course that is a very difficult thing for them to actually verify. The downside of doing a proper verification process would be that people would have to provide even more information. So that is one concern.[56]

5.48 Joining social networking sites such as Facebook requires users to provide real names, dates of birth and other personal information. Facebook takes down fake sites very quickly:

> Facebook, because it is a real-name culture, attracts a different kind of person. Because people tend to form groups according to family, friends and people they know, there is a certain degree of community policing that goes on. For example, child predators do not necessarily like to go to Facebook because if they have to use their real name or a verified email address you can find them. But there are a group of people who really do not care if you know who they are or not, because it is about power: they want you to know who they are. Now, what a company like Facebook does is use technology to try to root out aliases and fake accounts, and to look at patterns of conversation that indicate bullying or some sort of inappropriate behaviour. But one of the most valuable tools is to allow people within groups to report people who they think are doing bad things, and it is a remarkably effective tool. It is easier to be a bully if you are on text messaging or chat rooms and other things ...[57]

5.49 The Deputy Victorian Privacy Commissioner commented on Facebook's policy:

> Although this in itself is a bit of a concern for privacy people, they are kind of monitoring the community. People who are genuine friends of someone do realise that the child should not be on there. There is some kind of self-monitoring in a sense happening in

56 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS68.

57 Hon Mozelle Thompson, Chief Privacy Advisor, Facebook, *Transcript of Evidence*, 11 June 2010, p. CS16.

> these online communities in the same way that that happens in real world communities.[58]

5.50 The Victorian Privacy Commissioner added that:

> Some people actually notify Facebook if they realise that there is a child under 13 clearly using Facebook.[59]

5.51 The Commissioner commented on the requirement for the provision of personal information where, for example:

> a young person registers with a social networking website. This may result in the collection of a child's full name, address or associated information: for instance, Facebook's Terms of Service states that real names and information must be used to register an account. Young persons may also be more likely to reveal personal information about themselves to receive a reward or discount - such as is required when signing up for an online game or contest.[60]

5.52 The Commissioner noted that Facebook had 'quite intricate mechanisms' for looking at the information a would-be user has to provide, and this detected some children less than 13 years who seek to join. Anecdotally, there seemed to be users whose language skills do not reveal that they are less than 13 years old.[61]

5.53 Commenting more broadly, the Victorian Privacy Commissioner made the point that:

> On certain sites such as instant messaging or chat rooms, children may also assume that using the Internet is anonymous and therefore appears 'safe'. This may increase the likelihood of a young person sharing their own personal information with someone they otherwise would not.[62]
>
> Current Australian privacy legislation contains provisions relating to the collection of personal information. The Victorian

58 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS74

59 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS74.

60 Office of Victorian Privacy Commissioner, *Submission 59*, p. 4, citing Report of the Child Health Promotion Research Centre, *Review of existing Australian and International Cyber-Safety Research,* May 2009.

61 Victorian Privacy Commissioner: *Submission 59*, pp. 4- 5; Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, p. CS74.

62 Office of Victorian Privacy Commissioner, *Submission 59*, p. 4.

> information Privacy Act and Commonwealth Privacy Act requires Victorian and Commonwealth public sector organisations, as well as some private sector organisations, to 'only collect personal information that is necessary for its functions or activities'.[63]
>
> For organisations interacting and collecting directly from children, organisations should consider whether their current collection notices are reasonably easy to understand so that children are able to exercise their privacy rights and make informed decisions.[64]

5.54 Privacy NSW commented that:

> In the case of internet sites which require an agreement to participate (excluding contractual matters) such as social networking sites, the question is therefore whether a child or young person has the capacity in the circumstances to consent to the use ... the capacity to consent should be measured on a sliding scale of factors, such as age, the ability to communicate consent, the individual's understanding of the issue in question, support from parents or other authorised representatives and the context in which the issues arise.[65]

5.55 From an organisational perspective, the Victorian Privacy Commissioner expressed concern at the trend for organisations to collect personal information for unrelated purposes:

> Over-collection leaves organisations open to larger and more damaging consequences when the security of a database is breached[66]

5.56 Organisations may not require all the personal information they collect, other than to verify the provider's identity. If this information is not kept securely, it can be lost or disclosed to unauthorised persons. It may be transmitted and stored outside Australia, despite national and State/Territory privacy laws.[67] The Victorian Privacy Commissioner stated:

> The effectiveness of privacy laws are limited in an online environment. Data is increasingly transmitted and stored globally,

63 Office of Victorian Privacy Commissioner, *Submission 59*, p. 5.

64 Office of Victorian Privacy Commissioner, *Submission 59*, p. 3.

65 Privacy NSW, *Submission 61*, p. 3.

66 Office of Victorian Privacy Commissioner, *Submission 59*, p. 5.

67 Victorian Privacy Commissioner: *Submission 59*, p. 6; Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, p. CS68; Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS74.

> despite privacy regulation occurring at a state and national jurisdictional level.[68]

5.57 The Alannah and Madeline Foundation noted that:

> Privacy is a notion that does not technically exist in the online environment. If a technical system can be built by developers, it may be broken by hackers. However, privacy or the lack of privacy affects the average online user when information is shared and an embarrassing or unflattering incident occurs...
>
> A common complaint in relation to social networking sites is the difficulty of controlling personal information and adjusting the privacy settings. With the growing awareness of the importance of protecting personal information comes an increased expectation of user control over how much other people can view of their digital footprint.[69]

5.58 Material so collected can be used for unrelated purposes, such as marketing, statistics, advertisements, and tends to become increasingly comprehensive. The sale of information databases, compiled from material provided by customers or consumers, is a large and important industry in the United States.[70]

5.59 Privacy laws also impose obligations on an organisation to take reasonable steps to inform individuals of:

- the identity of the organisation that is collecting the information and its contact details;
- the individual's ability to access the information;
- the purpose for which the information is collected;
- to whom the organisation usually discloses the information;
- any law requiring the information to be collected; and
- the main consequences for the individual if the information is not provided.[71]

---

68 Office of Victorian Privacy Commissioner, *Submission 59*, p. 6.

69 Alannah and Madeline Foundation, *Submission 22*, p. 27.

70 Ms Helen Versey, *Transcript of Evidence*, 9 December 2010, p. CS68; Victorian Privacy Commissioner: *Submission 59*, p. 6.

71 Office of Victorian Privacy Commissioner, *Submission 59*, p. 2, citing *Information Privacy Act 2000* (Vic) and *Privacy Act 1988* (Cth).

5.60 In response to questions from the Committee in relation to selling information to third parties for marketing purposes, industry groups provided the following responses. Microsoft stated that did not 'just sell' information without having a business case.[72] ninemsn stated that it:

> has recently signed up to the Australian online behavioural advertising guidelines. That is a cross industry initiative. It is very broadly supported. We have now agreed to abide by certain standards regarding the way that we collect and use that sort of information. One of the key requirements is that we need to disclose where we are collecting behavioural information from and using it for third party online behavioural advertising targeting. There has also been an industry website launch that provides consumers with information about online behavioural advertising practices and will have opt-out capability for consumers to use so that they can opt out of that sort of advertising.[73]

5.61 Facebook explained that there are companies that engage in data mining and data scraping without the consent of users and stated that:

> Facebook does not sell information. It does not provide it to marketers. There are some people who we have seen in the press allege that, but it does not make sense from a business model standpoint. The reason that Facebook is valuable is because it keeps the sanctity of the data that belongs to individuals and if advertisers want to advertise to them, they have to go through Facebook. If they gave away the data or sold it, then Facebook would be less valuable.[74]

5.62 Yahoo!7 added that the legislation requires that personal information be stored securely, therefore, it does not share personal information without the user's consent. It is a signatory to the Australian Best Practice Guidelines for Online Behavioural Advertising.[75] Yahoo!7 also provides

---

72 Mr Stuart Strathdee, Chief Security Adviser, Microsoft Australia, *Transcript of Evidence*, 21 March 2011, p. CS16.

73 Ms Jennifer Duxbury, Director, Compliance, Regulatory and Corporate Affairs, ninemsn, *Transcript of Evidence*, 21 March 2011, p. CS16.

74 Hon Mozelle Thompson, Advisory Board and Policy Adviser, Facebook, *Transcript of Evidence*, 21 March 2011, p. CS17.

75 Ms Samantha Yorke, Legal Director, Asia Pacific Region, Yahoo!7, *Transcript of Evidence*, 21 March 2011, p. CS17.

the capacity for users to turn off advertising or finetune their preferences.[76]

5.63 Dr Roger Clarke cautioned, however, that:

> The word 'selling' is a trap in the questioner's mouth. We always have to get rid of the word 'selling' when we are asking those kinds of questions and talk about 'transfer under any circumstances'. I do not care whether it is trading, gifting or exchange, because there are many uses of weasel words by organisations that are trying to avoid telling the truth. There is definitely considerable availability through various means of that profile data to many companies other than the company that originally collected the information ... A lawyer can quibble on behalf of the large corporations because they construct their terms in such a way that you have consented to everything that they might ever do.

5.64 The Committee supports Recommendation 3 in the Senate Environment and Communications References Committee's Report.[77] Accordingly, the Committee recommends:

**Recommendation 7**

**That the Australian Government amend the *Privacy Act 1988* (Cth) to provide that all Australian organisations which transfer personal information overseas, including small businesses, ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.**

5.65 The Privacy and Data Protection Commissioners are currently considering:

> making the organisations more responsible in terms of ... giving more notice, and also controlling, and not forcing children, or anyone really, to give over lots of information. That goes back to the amount of information you have to give to get access. So really those are the basic rules around data protection: only collecting

76 Ms Samantha Yorke, Legal Director, Asia Pacific Region, Yahoo!7, *Transcript of Evidence*, 21 March 2011, p. CS18.

77 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

> what is necessary to be able to provide the service, not forcing people to provide more information than is needed to access a particular service, and putting controls on what other organisations get access to that service.[78]

5.66 Dr Anthony Bendall referred to the 'do-not-track' model where the user can choose not to be tracked for the purposes of behavioural advertising.[79] Apple also offers technology to block particular types of applications, and these approaches could be applied by parents.[80] He also said that:

> Depending on what you are going to use the information for, you give proper streamlined notice about that and have templates that allow people to use it rather than long legal documents. Notice should be given at the time that you are asking the person to make the decision so that the point at which they decide to provide the information would be the point at which the notice would be given rather than a generic document that they are meant to look at the first time they go online or every time they go online and which can be changed whenever a business likes—which is another practice that some online businesses engage in.[81]

5.67 The Committee supports Recommendation 4 in the Senate Environment and Communications References Committee's report.[82] Accordingly, it recommends:

78 Ms Helen Versey, Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS73.

79 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS70, citing the Federal Trade Commissioner's Report *Protecting consumer privacy in an era of rapid change: a proposed framework for businesses and policymakers.* Released December 2010.

80 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS73.

81 Dr Anthony Bendall, Deputy Victorian Privacy Commissioner, *Transcript of Evidence*, 9 December 2010, p. CS70.

82 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

### Recommendation 8

**That the Office of Privacy Commissioner, in consultation with web browser developers, Internet service providers and the advertising industry, and in accordance with proposed amendments to the *Privacy Act 1988* (Cth), develop and impose a code which includes a 'Do Not Track' model following consultation with stakeholders.**

5.68 The Committee supports Recommendation 5 in the Senate Environment and Communications References Committee's report.[83] It therefore recommends:

### Recommendation 9

**That the Australian Government amend the *Privacy Act 1988* (Cth) to provide that an organisation has an Australian link if it collects information *from* Australia, thereby ensuring that information collected from Australia in the online context is protected by the *Privacy Act 1988* (Cth)**.

5.69 The Committee supports Recommendation 6 in the Senate Environment and Communications References Committee's Report.[84] Accordingly, the Committee recommends:

### Recommendation 10

**That the Australian Government amend the *Privacy Act 1988* (Cth) to require all Australian organisations that transfer personal information offshore are fully accountable for protecting the privacy of that information.**

5.70 The Committee supports Recommendation 6 in the Senate Environment and Communications References Committee's report.[85] It therefore recommends:

83 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

84 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

### Recommendation 11

**That the Australian Government consider the enforceability of provisions relating to the transfer of personal information offshore and, if necessary, strengthen the powers of the Australian Privacy Commissioner to enforce adequate protection of offshore data transfers.**

5.71 The Committee supports Recommendation 7 in the Senate Environment and Communications References Committee's report.[86] Accordingly, the Committee recommends:

### Recommendation 12

**That the Australian Government continue to work internationally, and particularly within our region, to develop strong privacy protections for Australians in the online context.**

85 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix.

86 Senate Environment and Communications References Committee: *The adequacy of protections for the privacy of Australians online*, pp. vii-ix