REVIEW OF EXISTING AUSTRALIAN AND INTERNATIONAL CYBER – SAFETY RESEARCH

Child Health Promotion Research Centre
Edith Cowan University
May 2009

REVIEW OF EXISTING AUSTRALIAN AND INTERNATIONAL CYBER–SAFETY RESEARCH

Authors
Dr Julian J Dooley
Professor Donna Cross
Dr Lydia Hearn
Robyn Treyvaud

Contributor
Garry Putland

Citation
The citation below should be used when referencing this report:
Dooley, J.J., Cross, D., Hearn, L., Treyvaud, R. 2009. Review of existing Australian and international cyber-safety research. Child Health Promotion Research Centre, Edith Cowan University, Perth.

The research reported in this publication was commissioned by the Australian Government Department of Broadband, Communications and the Digital Economy.

The information and opinions contained in it do not necessarily reflect the views or policy of the Department of Broadband, Communications and the Digital Economy.

Table of Contents

List of Tables

List of Figures

Executive summary

Information and communication technologies have permeated almost all areas of society and become an important component of daily functioning for most Australians. This is particularly true for Internet and mobile phone technology. The majority of Australian households (67% in 2007 – 2008) have access to the Internet and over 11 million Australians use the Internet as an integral part of their personal, social and occupational activities. By mid-2008, there were over 22 million active mobile phones being used in Australia, which equates to more than one phone for every citizen.

There are many benefits associated with Internet and mobile phone use; however, there are also risks, particularly with the Internet. In fact, there is almost daily media discussion of these risks and dangers. However, to ensure that the information contained in this review was as accurate as possible, we primarily sourced quality research literature published in scientific journals both in Australia and overseas. In addition, quality material not published in scientific journals was consulted and included where appropriate, thus ensuring that this review was based on reliable research studies containing the most current and accurate research evidence available. From the outset, it is important to note that there are several methodological and ethical issues in relation associated with the measurement and examination of many cyber-safety risks. The nature of this type of research makes it

very difficult to address certain risk areas, in particular those that relate to children (e.g., online grooming).

In general, our review of the scientific and non-scientific literature revealed significant and major gaps in most areas of cyber-safety research, particularly for Australian-based research. Most of the areas addressed in this report have been subjected to only cursory examination in the literature. Further, our review revealed that topics often addressed in the popular media have received scant attention in the scientific literature. For example, online grooming is a risk associated with the use of the Internet that has not been subject to thorough scientific investigation in methodologically sound research studies. Further, cyber-bullying research is still new and, consequently, little is known about the motivations of those who engage in these behaviours as well as the long-term effects of this type of victimisation.

Our review revealed significant gaps in Australian research in several areas above and beyond what is observed in other countries. For example, only very preliminary Australian research has been conducted on the effects of exposure to pornography whereas this area has attracted much attention especially in the US. Other topics have received only cursory examination, including: cyber-stalking, promotion of inappropriate social and health behaviours (although a sizeable amount of ongoing work is addressing the promotion of smoking on the Internet), online grooming as well as exposure to certain types of inappropriate and illegal content (e.g., online hate websites, pro-anorexia websites). However, significant work has been and is being conducted in Australia

examining the various aspects of cyber-bullying. Therefore, it is necessary to extrapolate from overseas research findings to estimate the prevalence and consequences associated with some cyber-safety risks to Australian youth.

Keeping in mind that much of this review was based on international research studies, the following are the major findings:

1. Cyber-stalking, grooming and sexual solicitation

Cyber-stalking is an emerging phenomenon that, unlike other cyber-safety risks, most often does not have its origins offline. Indeed, research with adults in the UK has suggested that cases, where the stalking began online and transferred offline, were the most dangerous. Although exact prevalence data were not available, overseas estimates of the proportion of young people in Australia affected by cyber-stalking is approximately 7%. Cyber-grooming and sexual solicitation is potentially the most serious of all cyber-safety contact risks. Prevalence rates for Australia are not yet available; however, overseas results suggest that the majority of solicitations are received from other adolescents (43 – 48%) or young adults under the age of 21 years (20 – 30%). Again highlighting the relationship between online and offline behaviours, those who received sexual solicitations were more likely to share personal information with strangers online and engage in offline risky behaviours.

2. Cyber-bullying

Cyber-bullying is emerging as a significant risk to cyber-safety for young people. Whereas rates of up to 50% of being cyber-bullied have been reported among young people in the US and Europe, prevalence rates in Australia are much lower (less than 10%). Despite the anonymity offered by the Internet or mobile phone, it appears that the majority of students are aware of the identity of the perpetrator. Further, again highlighting the relationship between online and offline behaviours, a large proportion of those who engage in cyber-bullying behaviours also engage in face-to-face bullying behaviours. Finally, overseas evidence suggests that those who report engaging in cyber-bullying behaviours are more likely to be older with rates increasing from 8% by age 11 years to 23% by age 14 – 15 years.

3. Exposure to illegal and inappropriate material

It is estimated that 84% of boys and 60% of girls in Australia report they have been accidentally exposed to pornography online while 38% and 2% of boys and girls respectively, were deliberately exposed. Several factors have been associated with intentional viewing of pornography on the Internet. For example, young people who intentionally view pornography were also more likely to self-report delinquent behaviour and substance use in the previous year, as well as experiencing symptoms of depression and lower levels of emotional bonding with parents or caregivers.

Other forms of inappropriate content include violent media, hate groups and content describing and depicting self-harm or suicide. We were unable to identify any study that specifically addressed the impact of Internet-based violent content. Although it is unclear how many young people in Australia are exposed to violent content on the Internet, estimates from Europe range from 15% to 90%. Estimates from the US suggest that 25% of young people using the Internet have viewed a website containing information about hate groups. Finally, those who use self-harm websites and bulletin boards are more likely to be females between 16 and 23 years of age, have concurrent mental health issues, a positive history of abuse and a poor relationship with parents.

4. Promotion of inappropriate social and health behaviours

There is ongoing debate about the appropriateness of the concept of Internet addiction. Prevalence rates vary with reported estimates of less than 2% in Finland to 61% in the US. A study involving young people (aged 15 – 23 years) from Taiwan demonstrated that Internet addiction was associated with symptoms of inattentiveness, hyperactivity and impulsivity as well as depression, social phobia and hostility. However, results for Australian university students did not reveal a relationship between the amount of time spent online and symptoms of depression, anxiety or social fearfulness. Overall, it has been reported that most problematic use of technology (including those aspects of Internet use that resemble other forms of addiction) appears to be related to the content rather than the medium.

5. Identity theft, privacy and online security:

Estimates of online privacy breaches are difficult to obtain but a recent Australian survey suggested that over 40% of university students have a photograph posted online without their permission. Despite young Australian's positive attitude to the Internet, over 75% consider technology a threat to their privacy. Results from an Australian based study of information disclosure on a social networking site demonstrated that peer pressure is a strong motivator for young people to share personal information – 47% of those younger than 14 years and 41% of those older than 14 years disclosed personal information on the Internet because they believe their friends were also doing it.

Overall, this report provides a detailed overview of Australian and international research literature on cyber-safety risks. In general, there are several risks associated with using technology and exposure to these risks, when not properly addressed, is associated with negative consequences. However, the literature (scientific and non-scientific) suggests that some of the most troublesome online risks are strongly associated with offline risks and that these two worlds do not exist independently. Thus, in order to address online risks, it is crucial that offline behaviours also be considered. Finally, the research indicates that as young people increase their use of information and communication technologies, such as the Internet, they increase their risk of being exposed to negative online experiences.

SECTION 1

METHODOLOGY

Section Summary

- Literature published in scientific and non-scientific journals reviewed.
- Quality literature not officially published (i.e., grey literature) reviewed.
- 128 keywords used; 44 databases searched; 55 websites searched.
- Additional searches conducted by contacting individual authors, organisations and companies.
- Specific issues (e.g., child pornography) were excluded as they were considered to represent more of an offline risk.

1.1 Overview

In conducting this review our goal was to identify and assess as much of the peer reviewed and quality grey literature[1] as was available, using comprehensive search techniques. Given the diversity of topics involved in the review, several strategies were employed to identify quality literature. It is important to note that, empirical, peer-reviewed literature addressing the risks associated with the issues outlined in this tender is relatively sparse. Much has been written on some topics (e.g., grooming and sexual solicitation) that is largely conjecture and not based on empirical evidence. If the accuracy of the information contained within could not be verified we did not include these reports, press releases, private company studies, or media reports in this review. A list of all

[1] Grey literature refers to materials (e.g., reports) that cannot be found easily through conventional channels such as publishers.

publications (including those that were not referenced directly in this report) was provided upon submission of the final report to the Department of Broadband, Communications and the Digital Economy (DBCDE). The key goals of this review included: identifying and critically assessing the Australian and international research literature addressing cyber-safety risks, examining the technical and behavioural measures employed by parents, teachers, students to mitigate cyber-safety risks, identify the major gaps in the research literature and provide strategies to maintain the currency of the information contained in this report.

1.2 Literature review process

The review and synthesis of information (databases, literature reviews and key informants) involved a number of key stages. Given that cyber-safety research is relatively new, only limited data were published in peer review journals and online reports. Initially, a list of 128 keywords addressing the issues outlined in the tender (see Appendix A) was generated and then entered into the following 44 databases (see Appendix B). Further, searches of specific publishing companies known to publish journals containing content relevant to the review were included (e.g., SAGE Journals Online). In addition, we searched specific scientific journals, such as Journal of Adolescence, to locate any relevant published material not identified using the database searches. Once we identified authors

who had published methodologically strong studies[2], we conducted searches by author name of all listed databases (e.g., Kimberly Mitchell, David Finkelhor, Michael Flood). The keywords listed were combined in a variety of ways depending on the issue that was being searched (e.g., cyber-stalking or grooming). Initially, keywords used were kept broad (e.g., "cyber" and "youth") and the most relevant publications were identified. As the search progressed, we used more specific and focused terminology (e.g., "grooming") to identify those publications that used very precise terminology. Further, once we identified a publication that addressed one of the issues relevant to this report, we added the keywords used by the authors to our list to ensure we were accounting for any cultural, regional or professional variations in how concepts were described (e.g., "cyber-bullying" versus "electronic harassment").

A 'snowball' search strategy was used for each risk area outlined in the tender (see Sections 2 – 6) whereby the most relevant publications were identified and the reference lists in each of these were examined to identify additionally relevant articles. This strategy was completed until we reached a saturation point (the point at which we were not locating any new references not already recorded in our database). In addition, we investigated reference lists for the most recent cyber-safety reports (e.g., the Byron review, the Internet Safety Technical Task Force [ISTTF] report) to determine if there were any additional, relevant references. If a publication had been identified and was not available via the library service at Edith Cowan University (ECU) we used the document delivery service, which enables a copy to be purchased from any library in Australia. If an article was not

[2] The strategy used to determine which studies were methodologically strong is outlined below.

available using this service, we made contact with the author(s) requesting a copy be emailed or faxed. In the same email, we also asked if the author had any additional publications that might inform our review.

Further, where possible we identified the Australian and international author(s) who had published in peer-reviewed scientific journals on each of the risk areas. Once identified, we contacted these authors and asked them to provide any additional materials (e.g., papers in press or under review) that were relevant to this review. In a number of areas (i.e., cyber-bullying and exposure to pornography) we identified the top three publishing authors in an attempt to ensure that as much of the literature was identified as possible. In most cases, identifying three authors working in each specific area of cyber-safety was difficult. For example, in relation to research investigating hate crime websites, one author was no longer active in the area after receiving a number of death threats. Of all the issues investigated for this review, it seems that the core group of active researchers investigating the impact of hate websites is very small. Nonetheless, several emails were sent out to a list of authors and they were asked if they were aware of any ongoing research (either their own or a colleague's) or if they had any scientific manuscripts either in press or under review that they would be willing to share. Using this strategy, we were able to identify and obtain a number of articles and reports that we had not previously been able to identify. Finally, we contacted a number of industry leaders (e.g., Google, MySpace, Cisco Systems) to determine if they had any resources, research data or other relevant information that would be informative for this report.

In addition to the above search for the scientific literature, we conducted a comprehensive search for grey literature. To this end, we used the same keywords as outlined above and used Internet-based search engines (e.g., Google, AltaVista) as well as known grey literature sources (e.g., The New York Academy of Medicine, 2009). As noted above, we requested reports and non-peer reviewed articles from authors who had previously published in the field. Further, to investigate the available web- and offline-based resources and educational materials that have been developed to address various cyber-safety areas, in particular cyber-bullying, an Internet search was conducted using the Google and Altavista search engines. We searched through the following cyber-bullying related websites and investigated the links sections (where available) of each website to identify additional resources (see Appendix C).

We initially identified a very large number of websites and then limited our search to those that had reported some evidence-base (theoretical or empirical) to the program's development. The programs on these websites were then thoroughly examined to determine if they were (1) theoretically based: that is, was the program developed according to a specific and recognised framework, model, theory, or heuristic that addressed safety; and / or (2) empirically tested: in the event that we were unable to identify any programs that were empirically evaluated, we included any programs that explicitly stated they were based on a specific study or the results of a study.

1.3 Selecting studies for inclusion

An extensive report on cyber-safety recently produced by the ISTTF (2008) selected only articles that reported original research and used the following five questions as criteria to guide their US literature review of cyber-safety issues:

- When was the research conducted?
- Where was the research conducted?
- What methodology was used?
- How representative was the sample?
- How rigorous was the evaluation (threats to internal and external validity)?

In addition to the above questions, we adapted and used the following ranking system to determine which studies would be included in this review (see Table 1.3.1). It was developed based on the work of David Soole and colleagues (Soole, Mazerolle, & Rombouts, 2008) who described the approach to assessing school-based drug prevention programs. Soole, et al. (2008) used the system to categorise the methodological rigour of studies. It is important to note that none of the resources we obtained received the highest ranking level (4). Further, we did not include any resources that were ranked at level zero. The majority of the grey literature was ranked at level 1 with the peer-reviewed scientific (and a small number of grey literature resources) ranked at levels 2 or 3.

Table 1.3.1 *Rating system used to determine methodological rigour*

Methodological Rigour Scale	
Ranking	Characteristics
4	Randomised experimental design, strong methodological design, participant groups generalisable to general public, minor study limitations – PEER REVIEWED SCIENTIFIC LITERATURE
3	Matched comparison quasi-experimental design (groups comparable; groups generalisable to general public, study limitations present but not fatal – PEER REVIEWED SCIENTIFIC LITERATURE / SOME GREY LITERATURE
2	Matched comparison quasi-experimental design (limited generalisabilty to general public, significant study limitations) – SOME GREY LITERATURE
1	Survey (limited information about methodology) – GREY LITERATURE
0	Opinion piece, review (no data presented) – NOT INCLUDED IN FINAL REPORT

1.4 Areas of exclusion

Several areas and issues have been intentionally excluded from this report. The focus of the report was on the threats to cyber-safety faced by young people, thus, we excluded those areas that were primarily considered to be "offline" risks. For example, we chose not to review the literature addressing the production and distribution of child pornography via the Internet. Further, child pornography has been described as an offline risk given that each image depicts the unwilling abuse of a child (Taylor & Quale, 2008). Lastly, our review was, as much as possible, based on the peer-reviewed scientific and

quality grey literature. As such, this resulted in a large amount of material (e.g., newspaper reports) being excluded. As a result we do not present a discussion of some of the high profile legal cases (other than to comment that the issue in question has resulted in court action)as these do not provide research-based evidence detailing cyber-safety risks.

Further, landmark cases may not be consistent with and characteristic of the general state of affairs. For example, in the cyber-bullying area, several high profile cases involving suicide have been discussed at length in the popular media. While we are aware that the potential for suicide exists, these cases are relatively rare and a discussion that presents them as a likely outcome may appear to normalise this response to bullying. Finally, there are other cases of online interactions that appear to be characteristic of episodes of "cyber-stalking" that were not included in this review. For example, the online stoush between the Anonymous group and the Church of Scientology represents one such excluded case. This case was specifically excluded for the following reasons. First, given that little is known about the members of Anonymous, we do not have sufficient data or evidence to engage in a meaningful discussion. Second, in the case of their interactions with the Church of Scientology, the "victim" was clearly an entity rather than a specific person or, more importantly, a child or young person. Although we are aware that individuals within the Church of Scientology were targeted we do not believe that the actions of Anonymous represent the same level of risk as the other areas outlined in the tender (DCON/08/93) as it is highly unlikely that a young person using the Internet will become the target of any sort of action perpetrated by Anonymous.

In all the literature that was reviewed (and is included) for this report only those publications that provided clear and detailed information about the perpetrator(s), victim(s), method(s), or other important factors were chosen. Although we anticipate that there may be an article or report that was not obtained in time for inclusion in this review, we believe that the reviews contained in this report are comprehensive and accurate at the time of completion. Every effort was made to obtain as many relevant and quality resources as possible while being conscious of presenting the information in a concise and clear fashion.

1.5 Report structure

The structure of this report closely follows the format presented in the tender document (DCON/08/93). For clarity, the literature related to each of the issues identified in the tender document (e.g., grooming, cyber-bullying) is reviewed as separate sections. Where appropriate (i.e., where there is sufficient literature available), the Australian-based research literature is discussed first followed by a discussion of the international research literature. Given the paucity of research literature in some areas, we have not structured our review by age. However, when participant's ages were available, this information was included in the relevant section. It is hoped that this format will enable an accessible and clear understanding of the current evidence for each issue. Throughout these sections, gaps in the Australian literature are identified. These sections are followed with a review of the literature related to the technical and behavioural measures employed by students, parents,

teachers and schools to mitigate the risks to cyber-safety. That section also includes information about the effectiveness of these methods in mitigating associated risks.

To the fullest extent possible, we have identified and reviewed the highest quality peer-review research evidence available. In addition, we have included the highest quality grey literature given the number of government agencies as well as not-for-profit organisations who have also conducted research. In most cases, we relied on the quality research literature in the first instance, especially when discussing the consequences associated with the risks outlined in the tender. However, for some issues (e.g., privacy, identity theft) where there is limited research literature available, we relied (in some parts, solely) on the grey literature.

SECTION 2

REVIEW OF AUSTRALIAN AND INTERNATIONAL LITERATURE ON CYBER-STALKING, GROOMING AND SEXUAL SOLICITATION

Section Summary

Cyber-stalking

- Exact prevalence rate in Australia is unknown.
- Estimates from the US, UK and Australia combined in**d**icate approximately 7% of people were subjected to cyber-stalking behaviours.

Online grooming / sexual solicitation

The majority of **non-incarcerated offenders** who sexually solicit minors are:

- Other adolescents (43% - 48%);
- Young adults between 18-21 years (20% - 30%), and
- Older adults (4% - 9%).

The majority of **incarcerated offenders** who sexually solicit minors are:

- 18-25 years of age (23%);
- 26-39 years of age (41%), and
- 40 + years of age (35%).

2.1 Overview

This section deals with possibly the most publicly debated, emotive and largely misunderstood risk associated with the Internet, namely the sexual stalking, grooming and solicitation of children and teenagers. This can, in part, be linked with media headlines and reports announcing, for example, "2,500 arrests in the US in a one year period for Internet crimes against minors" (Piazza, 2004) or "up to 20,000 attempts to access child

pornography being blocked daily in the UK" (BBC NEWS UK, 2004). In addition, statistics detailing the risky behaviours associated with the Internet can contribute to public fear associated with the Internet and related technologies.

For example, Garlik (a UK-based online identity security company) reported that 1 in 5 UK children regularly met Facebook "friends" – meetings which only 7% of parents of those who completed the questionnaire were aware. Reports such as this contribute to the public perception that the Internet is a dangerous environment where risky behaviours are commonplace. In the absence of other information, the statistic describing the number of offline meetings of online friends is potentially very concerning. However, it is important to recognise that very little is known about the quality of the methodology of the study from which these results was drawn; it was only reported that 500 people aged 8 – 15 years answered a number of questions as part of this study. In the absence of any demographic information, we are unable to make any inferences whatsoever about the generalisability of the data presented in this study. We are unable to arrive at any solid conclusions regarding the online or offline behaviours of those who participated in this study. Furthermore, the report indicates that students were meeting with "strangers". The assumption made is that these strangers were adults and, therefore, quite probably paedophiles. However, as before, this conclusion simply cannot be made based on the available methodological information (i.e., the methods used to collect and analyse the data). However, none of these concerns were addressed in any of the media releases that were identified as part of this review. Therefore, these reports may create highly inaccurate perceptions about the nature and consequences associated with online interactions and online safety and security. Although

some clearly have a vested interest in promoting online security, it is critical that research results disseminated to the public be based on methodologically strong studies.

Herein lays the problem. Studies on cyber-stalking and grooming are, relatively speaking, few and far between. Among the most commonly reported reasons are the numerous and varied ethical concerns that such research topics raise. Given the nature of online interaction and the topic of grooming, the assessment of these behaviours is practically impossible[3]. Despite being an area of inquiry that is, relatively speaking, sparsely populated with researchers, it probably generates the greatest amount of community concern.

> "This lack of research may be attributed to problems of gaining access to the population, reluctance of victims to reveal they were victimized, difficulty in determining the age of the parties, or other methodological difficulties. More research is required to understand the dynamics and complexities of minor-to-minor unwanted sexual solicitation and contact crimes."
>
> *ISTTF, 2008, Appendix C, p. 21*

Given that offline contact can be associated with prolonged grooming encounters – which can be considered the most serious contact risk that minors face from Internet related interactions – these fears may have some merit. Although as outlined previously, our goal throughout this review is to present an unbiased, objective and factual overview of the most

[3] For example, you could enter a chatroom and ask if efforts to groom children are being made, although a response is unlikely. However, once a child has been 'groomed' it is too late. Therefore, the rate of grooming as assessed in terms of actual meetings between offender and victim is likely to be an underestimation of the true rate of online grooming.

current literature; we are conscious that, as was noted in the IDology Inc (2008) response to the final report of the ISTTF (2008), even a small percentage can translate to a huge number of people. While keeping strictly to the research literature so as to avoid conjecture, personal opinion and other such factors, we endeavour not to lose sight of this fact.

The media often represent the stereotypical "online predator" as someone who uses the Internet to lure child victims into situations that will result in a sexual assault. Wolak, Finkelhor, Mitchell, and Ybarra (2008a) note that media reports over the years have described child sexual offenders as typically lurking in Internet venues popular with children and adolescents, using public information found on Social Networking Sites (SNS) to identify potential targets and deception to cover up their ages and sexual intentions. They supposedly entice unknowing victims into meetings or stalk and abduct them so that law enforcement has to deal with an increase in the number of Internet-based sex crimes of epidemic proportions. However, the authors note that "the reality about Internet-initiated sex crimes – those in which sex offenders meet juvenile victims online – is different, more complex, and serious but less archetypically frightening than the publicity about these crimes suggests" (p. 111 – 112). Of course, that is not to say that these acts are not harmful to victims – Mitchell and colleagues (2007a) demonstrated that those who were sexually solicited online were 3 times more likely to report depressive symptomatology, 2.6 times more likely to report substance use and 1.8 times more likely to report engaging in delinquent behaviours.

As much writing on this topic is probably conjecture and not necessarily evidence-based, we reviewed only the research literature that has been or is being peer reviewed. Many government agencies have also commented on this issue in particular and we believe that the voices of these experts should be acknowledged. However, as acts of cyber-stalking, grooming and sexual solicitation vary by country in terms of their legality, there is little to be gained from investigating the prevalence and risks associated with these acts in all countries. Therefore, while we aimed to include as many quality and relevant government reports as possible, we confined our review to just a few other countries. In the sections that follow, we present an overview of the Australian and international literature on cyber-stalking and online grooming.

2.2 Cyber-stalking

Cyber-stalking is a term used to describe the use of electronic forms of communication (e.g., e-mail, chat rooms, etc.) to repeatedly harass or threaten another person (Spence-Diehl, 2003). Cyber-stalking refers to a cluster of behaviours that include:

- seeking and compiling information on the victim in order to harass;
- threaten and intimidate the victim online or offline;
- repeated unsolicited e-mailing and Instant Messaging (IM);
- electronic sabotage such as spamming and sending viruses to the target;
- identity theft;
- subscribing the victim to services;
- purchasing goods and services in the victim's name;

- impersonating another online;
- tricking other Internet users into harassing or threatening a victim (e.g., by posting the victim's personal details on a bulletin board along with controversial invitations, such as engagement in bizarre sexual games like rape role-play), and
- sending or posting hostile material, misinformation and false messages (Burgess & Baker, 2002; Finn, 2004; McGrath & Casey, 2002; Spitzberg & Hoobler, 2002).

While a diverse set of behaviours can be used to cyber-stalk, some are more serious than others, as illustrated by a well-known case of cyber-stalking in the US. In that case, messages, which included the victim's address and contact phone number, were posted by a man (whose romantic advances had previously been rejected by the victim), which detailed the victim's (fake) rape fantasies. Not surprisingly, the victim received a number of calls and even had men come to her house in the middle of the night, banging on her door saying that they were there to rape her (Maharaj, 1999). More recently, there was a case in the United States where a husband allegedly advertised on a popular website and recruited another man to rape his wife[4].

Research on cyber-stalking is relatively new, thus, we do not yet have a full and complete understanding of these behaviours. Further, as with other topics in this review, the environment in which cyber-stalking primarily occurs (i.e., cyberspace) is constantly evolving making it difficult to map a comprehensive (and accurate) temporal framework. In an attempt to chart cyber-stalking development, Philips and Morrissey (2004) collated

[4] At the time of the writing, this case was being processed in the court system.

data from 827 cases of cyber-stalking that were reported on the Working to Halt Online Abuse website – an US-based self-help organisation. The authors reported that 43% of cyber-stalking episodes began by the victim being sent unwanted emails. However, it appears that the interaction (i.e., the first online meeting) began in chatrooms (13%), on instant messaging (11%), on websites (7%), or through online newsgroups (1%). Importantly, only 1% of cyber-stalking episodes began offline and transferred to online.

> "Cyberstalking can be simply an electronic precursor to real world behaviours."
>
> *Ogilvie, 2000, p. 3*

In the US the growing use of emails as a cyber-stalking tool has been depicted as "the changing face of stalking" (Buhi, Clayton, & Surrency, 2009, p. 425). Buhiet, et al. advised researchers to examine the relationship between stalking and technology, in particular SNS such as MySpace and Facebook. This advice was based on two-thirds of their participants reporting being stalked in ways other than traditionally described. Despite the variety of types of cyber-stalking behaviours outlined in Table 2.2.1, some have argued that cyber-stalking is analogous to offline stalking. However, one notable difference between offline and cyber-stalking is the lack of information regarding the prevalence of cyber-stalking. For example, Ogilvie (2000) noted that "we have absolutely no empirical research upon which to estimate the actual incidence of cyber-stalking and,

indeed, determining the magnitude (or not) of this crime is practically impossible" (p. 1 – 2). Bozin (2009) cautioned that Australia might follow in the footsteps of the US in relation to cyber-stalking crimes and legislation governing these acts. However, a Parliamentary inquiry on cyber-crime (2004) made no mention of cyber-stalking that we could find.

Table 2.2.1 *Types of cyber-stalking behaviours*

Type	Description
Direct Email	Similar to written communication, the stalker uses email to alarm, annoy and harass.
Remailers	Email sent through a third party where the headings are removed, making it virtually impossible to trace its origins (Lucks, 2001).
Spamming	Sending hundreds of email messages to a user (intended to "clog" their mailbox).
Instant Messaging	"Real time" communication sent directly from stalker to victim.
Chatrooms	"Real time" communication posted to a group of users. Fabricated information may be used to humiliate or shame the victim, thus encouraging other group members to harass, criticise, harm or ostracise the victim.
Bulletin boards	Similar to chat rooms, except messages are posted to a website, where they remain and others may view them at any time.
Third party/Proxy	Messages are posted to bulletin boards, chatrooms or listserves for the purpose of enlisting the aid of others to harass or harm the victim. The stalker may pose as the victim and make inflammatory remarks or describe personal (often sexual or violent) fantasies. By posting the victims' address or telephone, these methods frequently result in a shift to dangerous terrestrial stalking (i.e., offline stalking).
Computer stalking	Whenever the victim is connected to the Internet, the stalker may be able to access, monitor and manipulate the victim's computer (Ogilvie, 2000).
Websites "tributes"	Some stalkers have been bold enough to develop websites in "tribute" to their victims. Some of these provide a wealth of personal information about the victims or describe the stalker's fantasies and obsessions in relation to the victim.
Pager codes	The stalker may send threatening codes to the victim's pager. In ex-intimate partner stalking, these codes may have a special meaning known only to the victim (i.e., date of violent incident).
Personal data manipulation	Stalkers may access and manipulate victims' bank accounts, student registration, telephone account, email accounts, online purchasing, or other personal data available on the Internet.
Blackmail	Prior to the onset of stalking, the victim may have engaged in compromising communications or exchange of photographs with the stalker. These are later used for blackmail, threats or intimidation (e.g., a threat to share "flirtatious" communications with the victim's spouse).

Adapted from Spence-Diehl (2003).

2.2.1 Australian literature

It is important to note the paucity of evidence in this review of the Australian-based cyber-stalking research literature. There appears to be few researchers who have published research data on cyber-stalking and, to the best of our knowledge, what has been published to date is generally a review of work done elsewhere (usually in the US). This makes it practically impossible to estimate prevalence rates for these behaviours in Australia. Of course, that is not to say that these behaviours are so rare as to be unimportant. In fact, the Australian legal system has long been aware that cyber-stalking behaviours are harmful, distressing and can lead to more dangerous offline interactions. This is supported by the fact that cases of cyber-stalking have been prosecuted in Australian courts for many years. However, as with many areas of cybercrime, the legal system has difficulties with defining and categorising cyber-stalking. Maury (2004) cited the adjustments made by the State of Victoria in 2003 to existing legislation as an example of how a State can facilitate criminalising cyber-stalking.

Cyber-stalking can encompass behaviours ranging from stealing someone's identity to making online purchases to posting information online (usually false) about the victim's sexual interests often with contact details (e.g., email address). Ogilvie (2000), one of the few researchers in Australia to have published in the area of cyber-stalking, suggests that it is useful to classify cyber-stalking into three categories: (1) E-mail stalking, (2) Internet stalking, and (3) Computer stalking. E-mail stalking often takes the form of hateful, obscene or threatening email but can also include the victim being sent hundreds of spam emails designed to clog their email inbox. Internet stalking has been described as the most

worrying category. Ogilvie (2000) suggests that this type is of grave concern as it appears to be the most likely to move offline. For example, Laughren (2000) demonstrated that Internet stalking is most often accompanied by what are considered traditional stalking behaviours, such as threatening phone calls, vandalism of property, threatening mail and physical attacks. Finally, computer stalking describes those situations where the stalker hacks into the victim's computer using, for example, a Trojan horse virus (Bocij, Bocij, & McFarlane, 2003) in order to monitor and control their online activity.

As noted, we were unable to locate any study that estimated prevalence rates of cyber-stalking in Australia. A very recent report by Paul Mullen and colleagues (Purcell, Flower, & Mullen, 2009) provided some data which we can use to extrapolate prevalence rates. They examined stalking behaviours in adolescents (less than 18 years of age) focusing in particular on characteristics of the offence and the effectiveness of intervention orders. Of the 906 offences where applications for intervention orders were made, 11% were classified as cyber-stalking. In their study, cyber-stalking comprised harassment via instant messaging, email harassment and posting malicious content about the victim on websites.

It should be noted that 15% of the cases reviewed by Purcell and colleagues (2009) involved sending unwanted text messages, a method, which may in some ways be similar to other cyber-stalking behaviours. The authors noted that, in contrast to adult stalkers who often utilise a broad repertoire of behaviours including more covert forms of harassment, adolescent stalkers used more direct forms of contact such as unwanted approaches and phone calls. Therefore, it may be that, if these behaviours continue into adulthood, those

adolescent perpetrators may incorporate more Internet-based stalking behaviours. However, the generalisabilty of the results of this study is limited given that only adolescents and those cases where applications for intervention orders were made were included. Importantly, these limitations are likely to under-estimate the true prevalence rate of cyber-stalking in Australia.

One point worth noting is the relationship between bullying and stalking. Purcell, et al. (2009) noted evidence to suggest that, especially in the case of females, some stalking episodes were preceded by bullying interactions. As will be detailed in the section on cyber-bullying (Section 3), bullying using technology such as the Internet is growing.

2.2.2 International literature

International research provides us with a clearer picture of cyber-stalking prevalence rates although there is still limited research in this area. Early research provided proxy statistics for prevalence rates as cyber-stalking was not directly measured. For example, Fisher, Cullen, and Turner (2000) assessed stalking experiences in over 4000 female undergraduate students and reported that, of the 13.1% who indicated they had been stalked, 27.4% had received unwanted emails (the sixth most common stalking behaviour used). Bocij (2003) reported that about 30% of respondents (from primarily the US and UK) reported being cyber-stalked. However, those who responded to any of 11 different behaviours were deemed to have been cyber-stalked. This approach could result in an

over-estimation of the number of perpetrators of cyber-stalking, as it was not clear from the methodology if the behaviours must be completed by the same perpetrator. Alexy, Burgess, Baker, and Smoyak (2005) reported that 3.7% of students were subjected to stalking behaviours and that this group represented over 30% of all those who reported being stalked. However, as inclusion criteria were not provided for this study, the generalisability of these results to other undergraduate students is difficult to evaluate.

Further, the authors reported that the males in their study were more likely to have been cyber-stalked than were the females (although females were significantly more likely to be stalked offline). It should be noted that, while there are other studies that have been completed, the results are difficult to evaluate. For example, Spitzberg and Hoobler (2002, p. 86) reported "almost a third indicate some degree of computer-based harassment and obsessive pursuit" but fail to qualify that this rate includes all those who reported the behaviour occurred on only one occasion. Further, their computer-based harassment items include, for example, "pretending to be someone she or he wasn't" (p. 83). Clearly, this item is likely to over-inflate prevalence statistics (20% responded to it in the affirmative) but not as much as including one time acts as stalking.

Most recently, the work of Sheridan and Grant (2007) provides us with the clearest picture to date of the prevalence of cyber-stalking. Participants for this study were recruited online[5] and comprised UK (53.1%), US (36.2%), and Australian residents (10.7%). We did not include these data in the section on Australian literature, given that

[5] It is important to keep in mind that the method of data collection likely resulted in a biased sample and may have inflated, or deflated, prevalence statistics. Nonetheless, of all the research conducted to date examining cyberstalking, this is methodologically the strongest.

almost 90% were from the UK or US. Based on the 1051 responses analysed, the average age was 32.6 years and victims were predominately female (86.8%). Table 2.2.2 below details the demographic data for each of the four categories.

Table 2.2.2 *Sheridan and Grant (2007) demographic data for each stalking type*

Type of stalking	*N*	Mean age (SD)*	% Female	Primary occupations§
Purely online	42	37.6 (11.3)	81%	Professionals (31%) Students (16.7%) Disabled (11.9%) Homemaker (9.5%)
Cross-over	50	33.5 (10.5)	86.3%	Professionals (41.2%) Admin/clerical (17.6%) Students (9.8%) Unemployed (7.8%)
Proximal with online	50	29.8 (9.9)	84%	Professionals (40%) Admin/clerical (26%) Students (10%) Service industry (6%)
Purely offline	51	31.6 (11.0)	92%	Professionals (24%) Admin/clerical (20.5%) Students (11.8%) Service industry (7.6%)

** When the stalking began.*
§*Specific job titles were not provided.*

The authors examined four types of stalking: *purely online* (where no offline contact was made), *cross-over* (where victims were stalked purely online for a minimum of 4 weeks before offline stalking commenced), *proximal with online* (where the stalking was primarily of an offline nature but the victim received emails or had been harassed via the Internet in other ways), and *purely offline* (where no Internet stalking was experienced at

any time). It should be noted that the authors qualified that cyber-stalking occurred if: (1) the stalking originated online, and (2) the stalking remained solely online for a minimum of 4 weeks.

Overall, 47.5% reported being harassed via the Internet. When the cyber-stalking qualification (see above) was applied, only 7.2% of the sample was judged to have been cyber-stalked. When 23 personal (e.g., depression) and medical effects (e.g., nausea, headaches, or weight changes) of the four types of stalking were compared, the authors reported that none of the types differed. In other words, cyber-stalking (purely online or cross-over) were just as harmful to the victim as the other two types (proximal with online and purely offline) and the "threat does not have to be physical to cause significant short- and long-term damage" (Sheridan & Grant, 2007, p. 636).

> "…the cross-over group (who began by cyberstalking their victims for a minimum of 4 weeks before crossing over to physical harassment) engaged in the most extreme stalking behaviours and were the most physically dangerous."
>
> *Sheridan & Grant, 2007, p. 637*

In terms of the effects on others, the only statistically significant relationship was found between cyber involvement and a detrimental effect on a victim's relationship with their family. It is possible that this is related to the perpetrator sending emails or posting messages while pretending to be the victim. It is also of interest that the average age of those who reported being cyber-stalked only (purely online group) was greater than the

other 3 groups. The authors did not address this point so it is unlikely that the purely online group were significantly older. However, it is interesting when one considers that only 6.2% of victims reported having a number of interactions with the offender online before the cyber-stalking began. Therefore, approximately 94% of victims did not have any prior contact with the perpetrator of the cyber-stalking suggesting that they were randomly selected by the offender. Unfortunately, the authors did not provide any information regarding the Internet habits of those in the purely online group so it is not possible to ascertain if they were selected from chatrooms, SNS, or other methods (e.g., IM). Finally, in terms of additional factors of importance, Sheridan and Grant (2007) reported that cyber-stalking was less likely to be perpetrated by ex-partners and was more often engaged in by acquaintances or strangers. Further, those who were purely cyber-stalked reported that the police more often took their complaints seriously when compared with the other three groups. Although we do not know how accurately the results reflect the incidence and characteristics of cyber-stalking and the perpetrators in Australia, is safe to assume they are reasonably comparable given the relative homogeneity in the overall sample.

Reflecting the changing environment of the Internet and behaviours such as cyber-stalking, the authors report (p. 637) that the "highest proportion of male victims was targeted by online stalkers," and that although the result was not statistically significant "it was thought that female stalkers were particularly drawn to online harassment due to the associated absence of physical confrontation." The authors conclude that there appears to be sufficient evidence to suggest that those who engage in cyber-stalking behaviours are

not a separate subgroup of stalkers but that the Internet is used as another tool in the stalker's repertoire.

2.2.3 Summary

Overall, cyber-stalking constitutes a series of behaviours that include unwanted emails and malicious web posts about another person. Although Australian prevalence rates remain unclear, one study which included 10% Australian respondents reported that, of those who self-identified, the rate of purely online stalking is approximately 5% compared with 54% of purely offline stalking (Sheridan & Grant, 2007). Interestingly, when the two groups are compared (online versus offline), professionals appear to be over-represented in the purely online group, as do older respondents. This finding was not investigated by the authors but may relate to time spent online.

Furthermore, Sheridan and Grant (2007) reported that those who described themselves as "disabled" comprised 12% of the online only victim group (but were notably absent from other types of stalking categories) highlighting how the Internet "levels the playing field" in terms of potential risks and victims. This is further highlighted by the finding that the highest proportion of male victims was in the online categories. Although the general consensus in research circles is that cyber-stalking does not constitute a new form of stalking, clearly certain aspects of the Internet make this type of behaviour more attractive and more feasible for certain types of perpetrators.

"Although a new medium for communication is involved, the nonforcible sex crimes that predominate as offenses against youth online are not particularly new or uncommon."

Wolak, Finkelhor, Mitchell & Ybarra, 2008a, p. 113

2.3 Cyber grooming and sexual solicitation

NetAlert (2007) has defined grooming as "course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes". Grooming, as a set of behaviours, is not a new concept; it has long been known that child sex offenders engage in a variety of elaborate grooming and solicitation techniques in order to have sexual contact with children (e.g., see Lang & Frenzel, 1988). While offline techniques (e.g., offering to babysit) can increase the potential that the extra-familial child sex offender will be apprehended, the Internet has provided a number of additional buffers to avoid detection.

Bowker and Gray (2005) suggest that the Internet provides child sex offenders with four main reasons which are compelling enough to warrant using the Internet to try to initiate physical interactions. First, the Internet provides child sex offenders with anonymity so that the potential victim will be unaware if they are talking to a peer or a paedophile. Of course, the anonymity associated with the Internet also provides law enforcement officials with an opportunity to entrap those looking to engage in sexual interactions with minors. Second, using the Internet makes it feasible for child sex

offenders to groom multiple children simultaneously. Although not impossible, attempting this offline would be risky. Third, home computers make it possible to store huge catalogues of images and videos, which can be used to reinforce existing fantasies and develop new ones. This fact also serves law enforcement well in that the information stored on computers can provide them with sufficient evidence to ensure the offender is convicted. Fourth, as will be discussed throughout this review, the Internet has empowered people to become self-producers of materials, including images and videos making total regulation of content practically impossible.

Although little research has been conducted on the topic of grooming, a six-stage process of grooming (also called "cybersexploitation") has been described. The stages include: victim selection, friendship forming, relationship forming, risk assessment, exclusivity, and the sexual stage. O'Connell (2005) outlined a process whereby the offender forms a relationship with a minor with the first two stages concerned with building a relationship while assessing the potential of detection by the victim's (older) siblings or parents. The exclusivity stage introduces a greater level of connectedness (i.e., best friends) as well as beginning to engage the minor in more adult oriented conversation. At the sexual stage, much of the conversation can revolve around sex and many conversations revolve around masturbation. It is also at this stage that the idea of meeting is introduced. As outlined below, given the previous discussion about sex, most victims are fully aware that meeting the offender is for the purposes of a sexual encounter.

Overall, much has been written about online grooming (in the non-scientific, peer-reviewed literature). Indeed, were we to address all that has been written on the topic, this

section of the review alone would likely run for hundreds of pages. However, much that has been written has not been based on any empirical evidence as far as we can identify. Therefore, any strategies that are put into place to address online grooming (or any other cyber safety issue), and are based on inaccurate or insufficient evidence, are unlikely to be effective in enhancing the safety of those children and adolescents who use the Internet. For example, consider the following quote from Berson (2003, p. 9):

> "Grooming is also a deceptive process in which a child is unprepared to interpret cues which signal danger of risk. Predators are skilled at gaining the trust of a child before luring them into interactions. The process of grooming through the formation of a close bond creates a victim who is more likely to comply with sexual advances."

Although much of that paragraph may intuitively make sense, the assumptions that are made are only based, at best, on anecdotal evidence. For example, there have been numerous cases where the victim professed their love for the offender indicating the formation of a close bond (e.g., Wolak, et al., 2008). In order to obtain a clear picture of both those who groom and those who are subjected to grooming, it is necessary to, as much as is feasible, examine the characteristics of both groups. Other descriptive comments by Berson (2003) regarding cyber-predators (e.g., they "hide behind the protective cloak of anonymity, masking as 'one of the kids'", p. 10) have the potential to, for example, misdirect law enforcement efforts. Therefore, to ensure that efforts to reduce cyber risks (e.g., online grooming) are appropriately structured and targeted, it is important to rely on

the available evidence. Further, there is evidence indicating that 3.3% of offenders who view child pornography on the Internet (i.e., those with a circumscribed sexual interest in children) also communicate directly with children online (Laulik, Allam, & Sheridan, 2007).

The following section assesses the research and other literature describing online grooming. The first point to make is that the scientific literature on the topic of grooming is very sparse. Although technically "grooming" and "solicitation" are two different behaviours (with grooming referring to a more protracted set of behaviours that, over time, may result in a minor being solicited for sex), we argue that there is much to gain from including the literature on sexual solicitation in this section of the report. For example, Berson (2003) suggested that one of the functions of sexual solicitations by adults is to "groom" youth and coerce them into online or offline sexual encounters. Sexual solicitation has been defined as a type of online communication where "someone on the Internet tried to get [a minor] to talk about sex when they did not want to," an offender asked a minor to "do something sexual they did not want to," or other sexual overtures coming out of online relationships (Finkelhor, et al., 2000).

What follows is a review of the literature concerning online grooming and sexual solicitation. As noted, the research literature in this area is very limited (this is probably one of the most limited topics that we will cover in this review paper in terms of the empirical, peer-reviewed scientific literature). Clearly, there are many hurdles – some insurmountable – that are faced by researchers in this field and these hurdles have likely contributed to the limited evidence-based, scientific and peer reviewed work that we can

draw on. Given these limitations, we feel that addressing the issue from an Australian versus international perspective may not be useful.

2.3.1 A review of the online grooming and solicitation literature

In one of the only research studies to date to examine Internet-initiated sex crimes, Wolak and colleagues (2004) reported that the stereotype of the deceptive child sex offender who relies on lies and trickery to seduce minors is largely inaccurate. Although the vast majority of Internet-initiated sex crimes involve adult men using various Internet-based mediums of communication (e.g., email, chatrooms, instant messaging) to communicate and seduce minors, the majority of those minors are aware that they are conversing with an adult. Indeed, only 5% of those offenders pretended to be teenagers when they first met their potential victims online.

Further, most victims (in the US at least) are aware that, when they arrange to meet offline, they are doing so with the expectation of engaging in sexual activity. Consistent with this, Wolak, et al. reported that most victims profess to be in love with the offender with 73% meeting on multiple occasions. The end result of the nature of these interactions is that most US offenders are charged with, for example, statutory rape, a charge that applies to those cases where a victim is too young by law to consent to having sex with an adult and that the sexual interaction was deemed not to have been forced (Wolak, et al., 2008b).

To estimate the relative prevalence of Internet-initiated sex crimes in the US, Wolak and colleagues (2003, 2004) compared the number of arrests nationwide for charges of

statutory rape to the number of Internet-initiated sex crimes (95% of which were nonforcible). The authors reported that if the Internet and non-Internet initiated cases were combined; those cases where the relationship began online would comprise only 7% of the total. Consistent with this, Willard (2009) reported very low rates of Internet-initiated sexual contact between teenaged victims and adult perpetrators. Of the 183 case files that were reviewed[6], Willard reported that:

- 8 incidents (4%) involved actual teen victims with whom the Internet was used to form a relationship;
- There were only 12 reports (6%) of predators being deceptive about their age, and
- The majority (79%) of police stings, which resulted in offenders being arrested, occurred in chatrooms.

> "Despite the establishment of one or more public profiles on MySpace, there has apparently not been one successful sting operation initiated on MySpace in the more than two years during which these sting profiles have been in existence."
>
> *Willard, 2009, p. 3*

[6] Case files consisted solely of adjudicated cases in the State of Pennsylvania from March 21, 2005 until January 13, 2009. These represent reported cases only and may not be consistent with those cases that remain unreported.

Despite this low overall figure, Wolak, et al. (2008b) reported that the number of Internet-initiated cases has risen since 2000 as the Internet has become more prevalent and preferable as a communication tool. Despite the statistic reported at the beginning of this section, that 20% of youth Facebook users regularly meet strangers offline, a more methodologically sound study reported that in the US, the percentage of youth who subsequently meet offline is between 10 – 16% (Berrier, 2007; Berson & Berson, 2005; Pierce, 2006, 2007; Wolak, et al., 2006). Although still a sizeable number, these meetings are typically friendship-related, nonsexual, are formed between similar-aged youth and, importantly, are known to parents (Wolak, Mitchell, & Finkelhor, 2002). For example, Wolak, et al. (2006) reported that 73% of parents were aware of offline meetings and 75% of those parents accompanied their children to the meeting.

Wolak, Finkelhor, and Mitchell (2007), in response to comments on the second Youth Internet Safety Survey report (Wolak, Mitchell, & Finkelhor, 2006), presented the following caveats which were intended to clarify issues related to the prevalence rate of online solicitation.

- **Solicitations do not necessarily come from "online predators":** All online solicitations were of an unwanted sexual nature. However, many could have been from other youth as most of those solicited did not know the age of the person who solicited them.
- **Solicitations are not always intended to lure or are devious in nature:** Many solicitations are limited to brief questions or comments. Many messages were relatively crude, for example, one girl was asked what her bra size was.
- **Most solicitations are not viewed as serious or threatening:** Over 65% of youth reported that the solicitation did not upset or frighten them.
- **Nearly all youth handled unwanted solicitations easily and effectively:** Most youth responded to sexual solicitations by removing themselves from the situation, blocking the solicitor, leaving the web site or computer, telling the solicitor to stop, or confronted, warned or ignored them.

So, contrary to the Garlik study, it appears that, in the US at least, parents are aware of their children's offline meetings with online friends. It should be noted that there might be a cultural issue that explains the difference as estimates from other countries vary. For example, it has been reported that over 25% of New Zealand youth have met a person offline that they had only previously known online (Berson & Berson, 2005). We were unable to locate any data regarding the number of Australia youth who arrange offline meetings with online friends. However, there is no evidence to suggest that it is any higher than other Western countries. Given that the Garlik study may have been methodologically

flawed, we would estimate that the percentage of minors who arrange offline meetings with online friends to be in the region of 10 – 16% (i.e., similar to the US).

2.3.2 Victim characteristics

There are several factors, related to engaging in risky behaviours, which increase the potential for exposure to sexual solicitations or grooming interactions (Wolak, Finkelhor, & Mitchell, 2008b). These can be divided into four broad categories: *types of online interactions with unknown people; history of sexual or physical abuse; general patterns of risky behaviour; and being someone who is either homosexual or questioning their sexuality.* In terms of the *types of online interactions with unknown people*, those youth who share personal information (e.g., name, telephone number, pictures) to unknown people online or talk to strangers online about sex, are more likely to receive aggressive sexual solicitations that involve either actual or attempted offline contact (Mitchell, Finkelhor, & Wolak, 2007b). Recent evidence suggests that those youth who do interact and share information with strangers online are not typical of all youth Internet users (75% of whom do not interact with strangers; Wolak, et al., 2006; Ybarra, Mitchell, Finkelhor, & Wolak, 2007). Further, those who are at greatest risk of receiving aggressive sexual solicitations may be an even more select group – only 5% of those, who talked to a stranger online, discussed sex.

An additional risk factor for receiving sexual solicitations involves frequenting Internet chatrooms. The very nature of chatrooms (i.e., enabling immediate, direct communication) makes obscene language and sexual talk more likely, especially in those

chatrooms targeted at adolescents (Subrahmanyam, Smahel, & Greenfield, 2006). Wolak and colleagues (2003a) reported that most of the offenders who initiated sexual contact via the Internet met their victims in chatrooms thus indicating the heightened risk associated with these environments. Research from the Netherlands has demonstrated that youth who are lonely, shy, or lacking in social skills tend to interact with others in chatrooms to compensate for problems they have forming friendships offline (Peter, Valkenburg, & Schouten, 2005). Therefore, it seems that chatrooms are especially risky in terms of the potential for encountering a child sex offender.

Mitchell, Finkelhor and Wolak (2001) demonstrated that those with a *positive history of offline sexual or physical abuse* are more likely to receive online aggressive sexual solicitations. This may be based on an inability to critically assess and be more responsive to online sexual advances (Berliner & Elliott, 2002; Rogosch, Cicchetti, & Aber, 1995). However, it may also be related to a more general pattern of risk taking behaviour, a noted consequence of childhood trauma (Wolfe, Jaffe, & Crooks, 2006). It has been demonstrated that girls are considerably more at risk for sexual solicitation, comprising 70 – 75% of victims (Wolak, et al., 2004; 2006). Further, those females aged 14 – 17 years are in the highest risk category receiving the vast majority of solicitations. As will be discussed below, this is about the same age as the majority of perpetrators (who tend to be male) in contrast to the commonly held belief that the majority of perpetrators are older adults. Overall, approximately 4% of youth received distressing sexual solicitations (to which they reported being very upset or afraid) and 4% reported receiving

aggressive solicitations. Only 2% of youth reported that they received both distressing and aggressive solicitations (Wolak, et al., 2006).

Although sexual orientation was not directly assessed in their 2003 study, Wolak, et al. (2008) reported that there were many factors (e.g., male victims met offenders in gay-oriented chatrooms) in the male victim cases that suggested that the victims were either homosexual or questioning their sexuality. In relation to the consequences of being solicited, the majority of youth tends to deflect or ignore the comments (Rosen, Cheever, & Carrier, 2008). Typically, those sexually solicited were not overly traumatised or otherwise psychologically damaged by the interaction; 65 – 75% of young people aged 10 – 17 years who received sexual solicitations were "not particularly upset or frightened" (Wolak, et al., 2006, p. 20). However, 28% of young people who received sexual solicitations reported being very or extremely upset and 20% reported feeling very or extremely afraid. More aggressive solicitations resulted in young people feeling very or extremely upset (34%) or very or extremely afraid (28%). Finally, 25% of young people who received sexual solicitations reported "one or symptoms of stress, including staying away from the Internet or a particular part of it, being unable to stop thinking about the incident, feeling jumpy or irritable, and / or losing interest in things" (Wolak, et al., 2006, p. 20).

2.3.3 Offender characteristics

First, it is important to note that this section will not review either the literature regarding offline offenders (except in cases where comparison is informative) or the literature regarding online traffickers and/or consumers of child pornography. As noted in

Section 4 (exposure to illegal and inappropriate content), online child pornography represents an issue distinct from grooming. There is evidence that online offenders target adolescents as opposed to children (Lanning, 2002). For example, Wolak, et al. (2004) demonstrated that 99% of victims of Internet-initiated sex offences were 13 to 17 years of age (M = 14.46 years, SD = 0.14 years). The authors reported that none of the victims were under the age of 12 in contrast to the offline victims, a large proportion of whom are younger than 12 years (Finkelhor & Baron, 1986; Snyder, 2000). Further, research conducted in the US has provided some interesting insights regarding those people who solicit youth for sexual liaisons. For example, the majority of offenders were reported to be other adolescents (43 – 48%) or young adults between 18 – 21 years (20 – 30%) with less than 10% (4 – 9%) coming from older adults (Finkelhor, et al., 2000; Wolak, et al., 2006). Interestingly, data collected from US law enforcement records paint a somewhat different picture. In those cases, offenders were aged from 18 – 25 years (23%), 26 – 39 years (41%), and over 40 (35%) years of age (Wolak, Finkelhor, & Mitchell, 2004). Further, evidence from the same US study indicated that most offenders were male (99%), non-Hispanic white (81%) and communicated with the victim for 1 – 6 months (48%). Further, Wolak, et al. (2006) reported that the majority of those who solicited others for sex on the Internet were male (73%). Of those females who sexually solicited others, 64% were younger than 18 years and 34% were aged between 18 and 24 years. In addition, although most (86%) of those who solicited others for sex met first online, in 14% of cases the victim knew the identity of the perpetrator from offline encounters.

Wolak, et al. (2006) also reported that 31% of solicitations involved an attempt to arrange an offline meeting (what the authors call aggressive solicitations). In those cases involving attempted meetings, 26% of perpetrators were known to the victim (from offline encounters). Furthermore, only 2 cases were reported where online sexual solicitations resulted in sexual assault, an increase from zero cases five years previously (Finkelhor, et al., 2000).

> The most frequent consequences of aggressive online sexual solicitations involved:
> 1. Asking to meet a young person in person (75% of cases);
> 2. Calling a young person on the telephone (34% of cases);
> 3. Coming to the home of the a young person (18% of cases);
> 4. Giving a young person money, gifts, or other items (12% of cases);
> 5. Sending offline mail to a young person (9% of cases), and
> 6. Buying travel tickets for a young person (3% of cases).
>
> *Wolak, et al., 2006, p. 18*

Thus, there is evidence to suggest that online offenders are, contrary to public opinion, not paedophiles who, by definition, are sexually attracted to prepubescent children (American Psychiatric Association [APA], 2000). This distinction is important in terms of the identification of offenders and potential victims, assessment of victim-oriented risks, and the treatment / management of victims. That, of course, is not to say that there are not paedophiles that attempt to groom young children for the purposes of sexual contact. However, given that younger children do not tend to use the Internet for communication purposes (i.e., they don't usually frequent chatrooms) and are usually more supervised than

older children (Roberts, Foehr, & Rideout, 2005; Wang, Bianchi, & Raley, 2005), the risk of them interacting with a paedophile online is relatively small.

Finally, there is some indication that online offenders who solicited teenagers may differ somewhat from offenders who solicited law enforcement officers who were posing online as teenagers (Mitchell, et al., 2005). For example, those who solicited undercover investigators were more likely to be older and middle class (in terms of employment status and income). These offenders were less likely to have prior arrests for sexual or nonsexual offences but were equally as likely to be in possession of child pornography and report substance abuse problems.

SECTION 3

REVIEW OF AUSTRALIAN AND INTERNATIONAL LITERATURE ON CYBER-BULLYING

Summary section

- Prevalence rates of less than 10% in Australia have been reported.
- International prevalence rates as high as 52% have been reported.
- Currently, there is inconclusive evidence in relation to gender differences in engaging in cyber-bullying behaviours and being the victim of cyber-bullying behaviours.
- Although most (up to 82%) victims know the identity of the perpetrator, anonymity is an important factor in cyber-bullying behaviours.
- Engaging in cyber-bullying behaviours increases with age with UK estimates ranging from 8% in year 7 to 23% in years 10 – 11.

3.1 Overview

Given that the topic of cyber-bullying is so new, an initial overview of the concept of bullying is provided. Generally, (non cyber specific) bullying is defined as a type of repeated aggression that is intentionally carried out by one or more powerful individuals and targeted toward a single person who is not able to defend him or herself. Dan Olweus' early research in Norway identified a number of factors which he considered crucial when differentiating between aggression and bullying (e.g., Olweus, 1993a). For example, while aggression is generally a single act (e.g., punching someone), bullying is comprised of

repeated and sometimes varied acts (e.g., punching the same person on numerous occasions or threatening them if they don't hand over their lunch money).

Further, Olweus reasoned, bullying behaviours are characterised by an imbalance of power, thus ruling out aggression between two persons of equal power. The important factor in relation to power is that it is often viewed more in terms of the person who was doing the bullying rather than the person who was being bullied (i.e., the perpetrator had more power). Finally, bullying behaviours must be intentionally enacted to inflict some form of harm (that harm can be physical, psychological, social, etc.). Including intentionality in the definition excludes those acts that cause harm but are bereft of malice (e.g., a visit to the dentist). In almost all bullying research, these three components (repetition, power imbalance, intent) are used to distinguish this behaviour.

3.2 What is cyber-bullying?

To date, cyber-bullying has been somewhat difficult to define because, as Kowalski, Limber, and Agatston (2008) noted, the methods employed to engage in these behaviours are varied. For example, students can create personal online profiles where they might list classmates they do not like, or similarly they may take on anonymous, virtual personalities in Multi-User Domain (MUD) and massively multiplayer (MMOs) online game rooms to harass others. Alternatively, cyberbullying can take the form of enticing individuals to share secrets or photographs (emailed in confidence), that are then altered and sent to

unlimited audiences once relationships sour (Harmon, 2004). Other forms include sending mean or nasty messages using IM or postings on a SNS (e.g., MySpace), e-mail or mobile telephone, or sending embarrassing pictures to others (Smith, et al., 2008). One of the difficulties facing researchers in this area is whether listing disliked classmates on Facebook is the same as distributing a private IM conversation to the rest of the school and, if they differ, what is the most appropriate way to measure this difference?

To date, cyber-bullying has generally been defined as bullying in an electronic medium or bullying via technology. Most researchers have adopted Olweus' definition of bullying as an aggressive, intentional act or behaviour repeatedly carried out by one or more people who are more powerful than the victim. Consistent with this approach, Smith and colleagues (Smith, et al., 2008) defined cyber-bullying as "an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" (p. 376). There are four major components to this definition, namely, the act must be aggressive, intentional, repetitive, and with a power imbalance. Belsey (2004) defined cyber-bullying as "the use of information and communication technologies...to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others". Note the absence of a power imbalance suggesting that the nature of online power is such that Belsey does not consider it a crucial factor in cyber-bullying interactions.

More recently, it has been acknowledged that for research on cyber-bullying to proceed with uniformity it is necessary to identify the core components of these behaviours

(Dooley, Pyzalski, & Cross, in press). Vandebosch and van Cleemput (2008) interviewed focus groups, of youth aged 10 – 19 years, and asked them to reflect on their experiences with information and communication technology (ICT) and cyber-bullying. The authors noted three main components that comprise cyber-bullying: the behaviour must be intentional, repetitive, and characterised by a power imbalance – the same factors considered central to face-to-face bullying - suggesting that it is the behaviour not the medium that is important. Consistent with this, Kowalski, et al. (2008) suggested that cyber-bullying was merely the electronic form of traditional bullying rather than a separate phenomenon.

However, Dooley, et al. (in press) argued that, from a theoretical perspective, there may be factors and functions unique to the cyber environment that minimise the relative importance of the traditional cornerstones of bullying. Take, for example, the case of a child who had a single picture of them doctored (i.e., the picture was manipulated in some way) and posted on the Internet and the website address was distributed to most students in their school. The initial incident (taking the picture and posting it online) only occurred one time but the fact that most students at school saw the picture can, for all intents and purposes, repeatedly and significantly worsen the impact of the initial act. Consistent with this, Slonje and Smith (2008) suggest the problem with defining cyber-bullying by repetition is that a post may be a single act and often the victim may not be aware of the frequency of viewings.

An additional issue identified in the course of this report is the variation in the terminology used. For example, some maintain that "online harassment" more accurately describes repeated online aggression which also includes flaming (online fights between two people of equal power), impersonation, denigration, trickery, outing, and exclusion (Chisholm, 2006; Willard, 2005). Others have suggested that cyber-bullying is a repetitive set of behaviours while online harassment may comprise a single act (Burgess-Proctor, Patchin, & Hinduja, 2009; Hinduja & Patchin, 2009; Wolak, Mitchell, & Finkelhor, 2007). Ybarra, Espelage, and Mitchell (2007) suggested that the traditional definition of bullying may be too restrictive. They argued that, in cyber-bullying interactions, frequency may not be an important component when defining the interactions, as it may not accurately reflect most cyber-bullying incidences.

Bullying using technology is of increasing concern as access to technology becomes more widespread. Early research indicates that Australia is a global leader in SMS mobile phone text messaging, with mobile phones being the most common medium used for cyber-bullying among adolescents in Australia (Campbell & Gardner, 2005). For example, a study conducted by the Australian Psychological Society in 2004, indicated that 83% of Year 7 to 12 students had a mobile phone, with 61% using their phone at least once per day (2004). Data also indicates that SMS mobile phone text messaging in Australia has increased exponentially to about 500 million SMS messages sent each month in 2004, compared to 10 million per month in 2000 (Lee, 2005). Today the figure is likely to be significantly higher. As with mobile phone technology, Internet use in Australia is increasing. For example, in 2007-2008, 67% of Australian households had Internet access

up from 16% in 1998 (Australian Bureau of Statistics, 2009). Further, wireless connections increased from 481,000 in December 2007 to 1,462,000 in December 2008. It has been predicted that, with this rise in Internet access, cyber-bullying will rise. In a study with students in Brisbane, the majority felt that the incidence of cyber-bullying was growing (Campbell & Gardner, 2005).

3.2.1 Prevalence of cyber-bullying in Australia

To date, several cyber-bullying prevalence studies have been conducted in Australia. Most recently, Cross and colleagues (Cross, Shaw, Hearn, Epstein, Monks, Lester, et al., 2009) examined covert bullying (including cyber-bullying) in approximately 7,500 primary and secondary school students from all over Australia[7]. Students were asked if they had experienced (or engaged in) bullying behaviours such as being sent nasty text messages or emails, or having mean or rude comments posted on SNS. The authors reported that rates of being bullied using technology ranged from 4.9% in Year 4 to 7.8% in Year 9. Prevalence rates were higher for females (7.7% versus 5.7% for males), non-Government schools (8.4% versus 5.7% for Government schools), and non-metropolitan schools (7.3% versus 6.4% for metropolitan schools). The overall rate of being bullied using technology was 6.6%.

[7] The Australian Covert Bullying Prevalence Study report can be found at http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx

Similarly, engaging in bullying behaviours using technology ranged from 1.2% in Year 4 to 5.6% in Year 9. Prevalence rates were higher for males (3.8% versus 3.3% for females), non-Government schools (6.4% versus 2.0% for Government schools), and non-metropolitan schools (4.4% versus 3.2% for metropolitan schools). The overall rate of engaging in bullying behaviours using technology was 3.5%. A survey of 2,027 eleven and twelve year olds attending Western Australian Catholic schools found that almost 10% had been sent hurtful messages on the Internet during the past school term, with the figure being as high as 12.5% among girls (Epstein, 2006).

In addition, Lodge and Frydenberg (2007) assessed the reported incidence of cyber-bullying in 652 young people aged 11 – 17 years who attended two independent and three state co-educational government schools in the Melbourne metropolitan region. The authors reported that 21% of students reported, "that they had been the victims of cyber-bullying during the academic year" (p. 48). Of those students who reported experiencing cyber-bullying behaviours, 30% received "nasty messages from peers via e-mail or SMS, several times a term of more often" (p. 49). Lodge and Frydenberg also reported that "girls attending independent schools report[ed] higher mean scores for victimisation that uses information and communication technologies than boys attending independent schools, and girls and boys attending state schools" which they suggested was a function of both income (higher income associated with increased potential to use a mobile phone) and use of technology (with girls more often using mobile phones to communicate with friends in addition to sending a significantly larger number of SMS messages per week than boys; Australian Psychological Society, 2004). It is important to note that there are some

limitations associated with this study including a non-generalisable sample, the use of a non-standardised measure of cyber-bullying, and the measure only contained two items assessing cyber-bullying.

An additional Australian-based study addressed exposure to cyber-bullying (among other cyber-safety risks) in 709 students across Years 8 – 10 from four different high schools in the Australian Capital Territory (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006). The authors used a number of measures to assess various aspects of cyber-safety (e.g., use of filtering software) and reported that 36.9% of males and 36.7% of females reported experienced bullying. Although these prevalence rates appear to be quite large, it is important to note that only one item was used to assessed bullying (and not cyber-bullying) and therefore we are unable to interpret these scores in a meaningful way. Further, given the participant characteristics outlined in the paper, it is unlikely if the scores reported are an accurate reflection of the current level of cyber-bullying.

Finally, a study of 22 Australian students[8] aged 11 – 12 years reported that "bullying occurred during school-based and home-based interactions and that many of the students who bullied at school were also likely to bully online. Both boys and girls instigated cyber-bullying although the boys were far more aggressive in their interactions and bullied each other online more than the girls did" (Maher, 2008, p. 56). However, this conclusion was based purely on a series of observations, field notes, interviews, and discussions with teachers and recordings of online interactions with a small sample of

[8] The students were all from Sydney, Australia.

students. No information was provided about the students so it is not possible to have confidence that the results of this study are generalisable to all other 11 – 12 year olds in Australia.

3.2.2 Prevalence of cyber-bullying outside Australia

To date, much of the research on cyber-bullying has been conducted in the US and the UK. However, demonstrating that these bullying behaviours are not culturally determined, research has also been conducted in various other countries such as Turkey, Estonia, Iceland, Sweden and Ireland. It is important to notice the variance in prevalence rates reported in the literature (see Table 3.2.1). This is relatively common when there is a lack of consensus in relation to the definition of a construct (i.e., differing definitions can result in different measurement instruments – one instrument asks questions about repetition whereas another does not – which can affect the reported prevalence rate).

Raskauskas and Stoltz (2007) reported that close to 50% of American adolescents aged 13 to 18 were cyber-bullied. Reporting similarly high rates, Burgess-Proctor, Patchin, and Hinduja (2009) reported that 31.3% of American girls reported being the victim of cyber-bullying perpetrated by a friend from school, while 36.4% reported being the victim of cyber-bullying by someone else from school. In contrast, Kowalski and Limber (2007) reported that approximately 11% of American youth in grades 6, 7 and 8 were cyber-bullied. Li (2008) found that 55% of Canadian students, aged 12 to 15, reported being

victims of cyberbullying, and 65% of Chinese students, aged 11 to 14, reported that they had been cyber-bullied. Further, Kowalski & Limber (2007) reported that 22% of UK students aged 11 to 16 years indicated they had been cyber-bullied. Despite the variance in prevalence rates, Australian and international research has demonstrated that cyber-bullying is a growing area of concern (Cross, et al., 2009; Hinduja & Patchin, 2006; Li, 2007b; Wolak, et al., 2007).

Table 3.2.1 *Prevalence rates for cyber-bullying and cyber-victimisation by European country*

Form of risk encountered by children and median response across countries researched	Incidence by European country Note: Percentages refer to online teenagers unless otherwise stated
Aggressive contact (child as participant) *…Been bullied/harassed/stalked* The approximate median response is 15 – 20%	Poland: 52% Estonia: 31% of 6-14 year olds Italy: 21% of 7-11 year olds and 18% of 12-19 year olds UK: 20% of 11-19 year olds Ireland: 19% of 9-16 year olds Norway: 16% Sweden: 16% of 9-16 year olds Iceland: 15% of 9-16 year olds Belgium: 10%
Aggressive conduct (child as actor) *…sent bullying/harassing messages* The approximate median response is 12%	Belgium: 18% Norway: 14% Denmark: 10% UK: 10% Ireland: 8%

Hasebrink, Livingstone, and Haddon (2008), Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. London: EU Kids Online (Deliverable D3.2).

In addition to prevalence rates, variable rates have also been reported in terms of the medium used to engage in cyber-bullying behaviours. For example, a recent Canadian study demonstrated that 23% of middle school students were bullied via e-mail, 35% were bullied via chatrooms, and 41% were bullied via mobile phone (Li, 2007a). Further, a Swedish study reported that of lower secondary students (12 to 15 years) bullied in the last 2 – 3 months, 4.8% were bullied via text message, 9% via e-mail, 6.7% by a phone call, and 8.6% using a picture/video clip (Slonje & Smith, 2008). Slonje and Smith (2008) also reported that students (aged 15 – 20 years) rated bullying behaviours using text message or e-mail as having less of an impact than face-to-face bullying, while bullying behaviours enacted using phones had similar levels of impact. Finally, and consistent with others (e.g., Smith, et al., 2008), bullying using picture/video technology was considered by students to have a greater impact than face-to-face bullying.

3.3 Gender differences in cyber-bullying

Face-to-face bullying has predominately been reported in males with fewer females engaging in bullying behaviours (Olweus, 1993b). However, data from the limited cyber-bullying research conducted suggests that gender difference patterns in face-to-face and cyber-bullying are not consistent. For example, the difference in the rate of engaging in cyber-bullying behaviours and experiencing cyber-bullying (i.e., being victimised) between males and females is not as large as has been demonstrated in face-to-face bullying research. Hinduja and Patchin (2007, 2008a, 2008b) and Topçu, et al. (2008) found no

statistically significant gender differences in the rate of engagement in cyber-bullying behaviours. Similarly, research in the US and Canada demonstrated similar rates for males and females in the rates of engaging in bullying and harassing behaviours (Li, 2007a; Wolak, et al., 2007; Ybarra, et al., 2006).

Although the reason for gender differences between face-to-face and cyber-bullying is unclear, one possibility relates to the environment within which cyber-bullying operates. For example, it has been demonstrated that females tend to engage in more indirect forms (compared to direct) of aggression and bullying such as rumour spreading and gossiping – often called relational aggression (Osterman, et al., 1998). It may be that the Internet and mobile phone technology lend themselves to these types of indirect aggression or bullying behaviours as they can be enacted without being in the presence of the victim. Others have suggested that girls who engage in relational aggression also engage in cyber-bullying behaviours to demean and exclude others from their peer groups through verbal gossip and threatening (Berson, 2003; Subrahmanyam, et al., 2006). Boys are more likely to use cyber-bullying behaviours to impose sexual harassment (Shariff & Gouin, 2005) through the use of confrontational language in homophobic bullying of male peers and sexual harassment of females (Chisholm, 2006; Subrahmanyam, et al., 2006).

The other gender issue in cyber-bullying research relates to victim profiles. Here again, the literature is somewhat unclear. For example, some studies have reported that females are more likely than males to be the victim of cyber-bullying (Kowalski & Limber, 2007; Li, 2007a; Slonje & Smith, 2008) while others have failed to find a gender difference

(Li, 2006a; Patchin & Hinduja, 2006; Smith, et al., 2008; Williams & Guerre, 2007). The reason for this inconsistency is unclear and further research is necessary before a conclusive profile of victims of cyber-bullying behaviours can be constructed.

3.4 Anonymity

One of the most important differences between cyber-bullying and face-to-face bullying is that the former may afford the perpetrator anonymity. As with cyber-related behaviours, there does not appear to be consensus on this question. For example, some reported that 41% of Canadian victims and 57% of US victims did not know the identity of the perpetrator of the cyber-bullying behaviours (Li, 2005; Wolak, et al., 2007). However, Hinduja and Patchin (2009) demonstrated that 82% of US victims of cyber-bullying behaviours were aware of the identity of the perpetrator and 41% of these were friends or former friends. Similarly, Juvoen and Gross (2008) reported 73% of respondents were "pretty sure" or "totally sure" of the identity of the perpetrator. There are several possible explanations for the differences in the rates of knowing the identity of the perpetrator. For example, the medium used to engage in cyber-bullying behaviours could account for the different rates, as victims may be more aware of the identity of the perpetrator if nasty messages are sent via email versus text message. Alternatively, the approach used to assess victim knowledge could impact on scores if participants were asked "*do* you know who sent you mean and nasty messages?" versus "*did* you know who sent you mean and nasty messages?" with the former asking if victims are *currently aware* and the latter asking if

they were *aware at the time*. Nonetheless, using technology to engage in bullying behaviours may afford some level of anonymity.

The lack of knowledge of the identity of a perpetrator of bullying behaviours can be problematic for victims as it can result in feelings of fear and anxiety that generalise to offline environments and social interactions (Kowalski & Limber, 2007). An interesting corollary of the anonymity afforded by ICT is that it has provided an opportunity to engage in behaviours online that would not be engaged in offline. For example, those who might not have felt in a position to bully or aggress against others in the schoolyard can now engage in extensive cyber-bullying behaviours using various strategies such e-mail, SMS, SNS, and IM to name but a few. Consistent with this, Ybarra and Mitchell (2004b) demonstrated that many students reported engaging in behaviours online they would not necessarily engage in offline.

> "There is some evidence in this study (and a lot of anecdotal evidence) of instances of bullying and misbehaviour [in Australian students] having occurred using MySpace where schools have already been forced to take action. Children are accessing the websites not only outside school hours but also during classroom time, despite efforts to restrict website access and activities."
>
> *De Souza & Dick, 2008, p. 154*

3.5 Cyber- versus face-to-face bullying behaviours

The relationship between online and offline bullying is, to date, unclear although there does appear to be some overlap. For example, Ybarra and Mitchell (2004a) reported that 56% of online aggressor/targets reported being the target of offline bullying, while 49% are aggressor-only and 44% are victim-only. This suggests that youth who are not involved in traditional bullying, may be involved in cyber-bullying. These findings are consistent with Ybarra and Mitchell (2007b) who reported that those who engaged in harassing behaviours online were significantly more likely to report offline victimisation. Ybarra and Mitchell (2004a) suggested that people who engaged in harassing behaviours online might be acting in retaliation to bullying experienced offline.

It has also been suggested that young people who were exposed to cyber-bullying behaviours had often been victimised offline, that online perpetrators had often also bullied others offline, but that many of those who were victims of bullying or engaged in bullying behaviours offline did not engage in or experience similar behaviours online (Raskauskas & Stoltz, 2007; Smith, et al., 2007). Li (2007a) found almost 30% of those who engaged in offline bullying behaviours also engaged in online bullying behaviours. Similarly, others have reported that more than a third of children who reported experiencing cyber-bullying also reported being bullied at school (Beran & Li, 2007; Erdur-Baker, under review). Thus, there is evidence suggesting an overlap between cyber-bullying behaviours and offline, face-to-face bullying behaviours. However, the nature of the overlap between online and offline bullying behaviours is unclear making it somewhat difficult to distinguish between

the processes involved in incidences of engaging in both online and offline bullying behaviours versus incidences of engaging only in online bullying behaviours. Williams and Guerre (2007) reported that there are common causal pathways with verbal, physical, and Internet perpetration of bullying behaviours.

3.6 Age and cyber-bullying

To date, the relationship between age and engaging in cyberbullying behaviours has been consistently reported. Ybarra and Mitchell (2004b) found that those who engaged in cyber-bullying behaviours were more likely to attend high school than middle school. Similarly, Smith, et al. (2008) demonstrated that older students were more likely to report ever engaging in cyber-bullying behaviours with rates of 8% in Year 7, 12% in Years 8 – 9 and 23% in Years 10 – 11. Smith, et al., (2008) also reported a similar age related trend for the victimisation of cyber-bullying behaviours with rates of 14% in Year 7, 19% in Years 8 – 9, and 26% in Years 10 – 11. The age-related differences may be related to the relationship between age and technology use. For example, Juvoenen and Gross (2008) reported that 15 – 17 year olds were significantly more frequent users of email, profile sites, blogs, and cell phones than were 12 – 14 year olds. Further, when compared to the younger age group, respondents aged 15 – 17 years were also significantly more likely to have more than 3 years' experience using the Internet.

Consistently, Kowalski and Limber (2007) reported that victimisation rates increased each year for students in Years 6 to 8. Although there is limited data on older adults, there is preliminary evidence suggesting that the relationship between age and cyber-bullying follows an inverse U pattern where rates start out low, increase until about the mid-teenage years and then begin to decrease over time. For example, Slonje and Smith (2008) reported that 17.6% of lower secondary students (aged 12 – 15 years) had been cyber-bullied compared to 3.3% of older secondary school students and college students (aged 15 – 20 years). The incidence and nature of cyber-bullying in adults are relatively unknown but there does appear to be some emerging interest in cyber-bullying behaviours enacted in the workplace (e.g., .

SECTION 4

REVIEW OF AUSTRALIAN AND INTERNATIONAL LITERATURE ON EXPOSURE TO INAPPROPRIATE AND ILLEGAL CONTENT

Summary section

- Exposure to illegal and inappropriate content has been described as being of great concern to parents.
- Australian youth are at risk of being exposed to Internet-based pornography. Prevalence rates of exposure to online pornography in Australia are:
  - **84% of boys** and **60% of girls** accidentally exposed.
  - **38% of boys** and **2% of girls** deliberately exposed.
- Images of extreme paraphilic behaviour (e.g., bestiality, coprophilia) are not easily found but can be located if actively sought out.
- Although Australian-based research is limited, evidence from overseas suggests that exposure to pornography at a young age is associated with specific negative outcomes.
- While the effect of media violence (especially in video games) on aggressive thoughts, feelings and physiological reactions is well established, little is known about the effect of Internet or mobile telephone based violent media.

4.1 Overview

It has been reported that parents are more concerned about exposure to illegal and inappropriate content on the Internet than any other form of media (Aisbett, 2001). Parental concerns are based on issues such as the relative lack of regulation of material

posted online as well as the easy access to inappropriate content. Despite the potentially limitless list of topics that could be considered "inappropriate", most research that has been conducted in this area addresses either exposure to pornography[9] (intentional or accidental) and media violence (covering movies, music, and images). Importantly, although Internet content in Australia is governed by the Broadcasting Services Act (1992; see box below), the variety and speed with which content is uploaded (in addition to the fact that much of the pornographic content originates from overseas) makes it very difficult to regulate all online content. Our extensive search of the scientific and non-scientific literature also revealed a small number of studies that focused on hate groups and content describing or depicting self-harm. However, it should be noted that there is very limited information from Australian-based research studies on exposure to pornography, media violence, hate groups, or self-harm content.

[9] There exists ongoing debate in the literature regarding the use of the term *pornography* with some researchers arguing that the descriptor *sexually explicit material* is more appropriate. We do not believe that it is useful to enter into this debate in this report and, for clarity, will use the term *pornography*.

Under the Broadcasting Services Act 1992, the following categories of online content are prohibited (www.acma.gov.au/WEB/STANDARD/pc=PC_90102):

- Any online content that is classified RC* or X 18+* by the Classification Board (formerly the Office of Film and Literature Classification). This includes real depictions of actual sexual activity, child pornography, depictions of bestiality, material containing excessive violence or sexual violence, detailed instruction in crime, violence or drug use, and/or material that advocates the doing of a terrorist act.
- Content which is classified R 18+* and not subject to a restricted access system that prevents access by children. This includes depictions of simulated sexual activity, material containing strong, realistic violence and other material dealing with intense adult themes.
- Content which is classified MA 15+*, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system. This includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse language, and other material that is strong in impact.

* Classifications are based on criteria outlined in the *Classification (Publications, Films and Computer Games) Act 1995*, ***National Classification Code*** and the ***Guidelines for the Classification of Films and Computer Games 2005***.

Finally, an issue that is yet to be discussed in any great depth (but for which reports in the media are becoming more frequent) relates to the production of illegal and often pornographic material. Several cases that have been brought to US courts provide evidence that some youth are not only consumers but also producers of pornography. For example, a case that is currently being addressed in the court system in the US state of New Jersey relates to the arrest of a 14-year-old girl for production, possession and distribution of child

pornography[10]. The charges stem from pictures that she uploaded to her MySpace page. The nude pictures posted were of the girl herself and she reportedly posted them for her boyfriend to view. Although only a small number of cases involving minors taking nude self-portraits and posting them online (or distributing them using other means) have appeared in the media, they do highlight that for cyber-safety many issues are pertinent.

4.2 Exposure to pornography

Internet-based pornography is big business with retail sales of Internet-based pornography growing 13.6%, between 2005 and 2006, to reach almost $3 billion US dollars (Edelman, 2009). Although still surpassed by sales and rentals of pornographic videos (totalling $3.6 billion US dollars), this figure does not fully describe the scope of Internet pornography. For example, Doran (2008) estimated that, on average, only 20% of Internet pornography consumers paid for any online content suggesting that the annual revenue from Internet pornography could be as high $15 billion if every consumer paid for the content they viewed. Further, a small number of oft-cited studies have examined the extent to which pornography exists on the Internet as well as other World Wide Web applications, such as Usenet (e.g., Rimm, 1995; Mehta, 2001; Mehta & Plaza, 1997). Although Rimm's study – which involved the examination of 917,410 pornographic images – has been widely criticised on methodological grounds (e.g., Thomas, 1996; Wallace & Mangan, 1996), Mehta's more recent work (2001) demonstrated that although the majority of pornographic

[10] This case was being processed in the New Jersey courts at the time of the writing of this report.

images available online are very graphic (but not considered disturbing or sexually bizarre), there remains a smaller percentage of images that are highly paraphilic, depicting images of coprophilia and urophilia (0.7%), bestiality (3.1%), and necrophilia (0.2%).

Given the very low percentage of these more graphic images, we will not address them in this review focusing instead on the content that youth are most likely to encounter online. Similarly, although it is not unheard of that youth are exposed to child pornography on the Internet, the limited research evidence on this topic means that a useful presentation of this issue is not feasible. Furthermore, given the underground nature of online groups that trade in child pornography (Taylor & Quayle, 2003), it is likely that these images will only be viewed by those who actively seek them out (in contrast to unintentional exposure). Nonetheless, as Colleen Bryant of the Australian Institute of Criminology recently noted (2009, p. 3), "online content is often unregulated and therefore can include sexual violence and other sexual content that is illegal in Australia."

Unfortunately, the quantification of online content is, with current technology, practically impossible and we do not have a full understanding of the extent to which violent sexual material is available online. What follows is a presentation of the literature describing Australian and international research on exposure to online pornography but does not specifically address violent pornography. Only a brief discussion of the effects of exposure to violent pornography will be presented, however, as there are several limitations with this research that warrant cautious interpretation of results.

4.2.1 Australian literature

Although Flood (in press) noted that children and youth are routinely exposed to Internet-based pornography he has pointed out that "until recently there [has] not been a single Australian study that [focuses] on the prevalence of [pornography] exposure and assesses its likely impact" (2007, p. 45). Despite Flood's proviso, the Australian-based literature on the topic of pornography exposure is still sparse comprising a small number of studies. Along with Clive Hamilton, Flood examined exposure to pornography by youth in two Australian cities (Sydney and Melbourne). Two hundred participants (100 boys and 100 girls) aged between 16 and 17 years were contacted via telephone and asked a series of questions about their exposure to pornography both online and offline (Table 4.2.1 below). It should be noted that their studies (Flood, 2007; Flood & Hamilton, 2003) provided only very limited information regarding participant demographics (e.g., 50% had part- or full-time jobs and 86% were at school) as well as being comprised of a sample which is unlikely to be representative of the national youth population (i.e., the survey participants were restricted to Sydney and Melbourne only).

Table 4.2.1 *Percentage of Australian youth (16-17 years old) exposed to pornography*

	X-rated video (%)		Internet – accidental (%)		Internet – deliberate (%)	
	Boys	Girls	Boys	Girls	Boys	Girls
Total	**73**	**11**	**84**	**60**	**38**	**2**
Every week	5	0	24	7	4	0
Every 3 to 4 weeks	16	0	22	6	7	0
Every 2 to 3 months	11	0	11	11	11	0
Less often	40	11	27	36	16	2

Adapted from Flood and Hamilton (2003).

Although the results of this study should be interpreted cautiously, the data reported by Flood and colleagues is promising in that it provides a snapshot of exposure to pornography as reported by some Australian youth. Flood and Hamilton (2007) reported that more teenagers viewed pornography via video and Digital Versatile Disc (DVD) than online. This is consistent with an adult-based study[11] reported by McKee, et al. (2008) who demonstrated that, in relation to medium of consumption, adult users of pornography more often used videos than the Internet.

While Flood and Hamilton (2003) reported that 38% of males and 2% of females intentionally viewed pornography on the Internet, many more (84% of males and 60% of

[11] Although exact ages were not recorded, more than 33% were in the 26-35 year age range.

females) reported accidental exposure. Although the rates differ, these results support previous research in that it is apparent that Australian youth are being accidentally exposed to pornography on the Internet. For example, in the only two other studies that were identified, Aisbett (2001) reported that about 50% of 11 – 17 year olds (boys and girls living in a house with an Internet connection) reported seeing something on the Internet that was offensive. Similarly, NetRatings Australia (2005) reported that, in Internet connected households, 38% of children (boys and girls) reported accidentally accessing a website, that their parents would prefer them not to see, one or more times.

As with the earlier Australian studies described above, caution must be exercised when interpreting these results. For example, in the Aisbett study, pornographic material was *most often*, but not always, described as offensive. Clearly then it is not the case that offensive material is *always* considered pornographic. Similarly, of those websites that parents did not want children to see, only 45% contained nudity or pornography. Therefore, although it appears that Australian youth are being exposed to Internet-based pornography (accidentally and deliberately), the true rate of exposure is unknown. In a personal communication, Dr Michael Flood reported that the estimates reported in his work (i.e., accidental exposure rates of 84% in boys and 60% in girls; deliberate exposure rates of 38% in boys and 2% in girls) are best considered "at least" estimates in that he argues that the rate is only higher than reported – due to the sensitive nature of the topic it is expected that not all those who deliberately viewed pornographic content online would admit to doing so.

A recent Australian based study noted that, with the exception of those aged 66 or older, each subsequent generation reported first viewing pornographic materials earlier than the generation before (McKee, Albury, & Lumby, 2008). Couple this with the increase in the number of sexually explicit websites over the past 10 years and it is reasonable to conclude that Australian youth are at risk of being, and are being, exposed (intentionally or otherwise) to sexually explicit material. Flood and Hamilton (2003) note that this fact alone may not be as troublesome as the nature of the material online especially given that online content is often more diverse and incorporates a large amount of self-produced materials which can be very different from other more commercially oriented material (Bryant, 2009).

To date, no Australian-based research has been conducted examining the *effects* of pornography. Despite this, much has been written about the harmful effects of Internet (and other) pornography, which is based on personal opinion and religious beliefs. For example, Roslyn Phillips, a research officer from the Festival of Light Australia (a Christian Ministry) argues that the most compelling evidence that pornographic and violent images change a viewer's behaviour is that it is "common sense". Others have proffered anecdotal evidence suggesting that the increase in sexually abusive behaviour perpetrated by children can be directly linked to the availability of Internet pornography (Murray, 2006). The distinct lack of Australian-specific evidence concerning the effect of pornography exposure makes it difficult to say what impact it is having on Australian youth.

In a recent study conducted by researchers at the University of Canberra (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006) 92.5% of male and 61.3% of female year 8 – 10 students reported exposure to Internet pornography. The authors did not contextualise 'exposure' so it is unclear if the figure reported is comprised of those who were exposed deliberately (i.e., intended exposure), accidentally, or a combination of both. Importantly, the authors reported an association between exposure and frequency of use with those who use the Internet more being exposed to more pornography. Finally, a study conducted by the Australian Broadcasting Authority (2001) demonstrated that 47% of youth aged 11 – 17 years of age reported being exposed to online material they considered "offensive and disgusting" such as pornography, violence and nudity. However, as with others, it was unclear if the exposure was deliberate or accidental and the figure reported also included non-pornographic material.

Flood (2007) noted that there exists sufficient evidence (from overseas studies) to argue that exposure to pornography has four primary effects. First, greater exposure to sexualised images (this includes all types of non-sexually explicit images, music, and television programs) is associated with more liberal sexual attitudes, greater factual knowledge and an increased belief in peers' sexual activity although this is not specific either to the Internet or to pornography. Second, younger children may be shocked, disturbed or upset by premature or unwelcome exposure although there is evidence that only a small percentage (less than 10%) of youth report this (Wolak, et al., 2006). Third, images that are outside the cultural norms (e.g., coprophilia, urophilia or bestiality) may be particularly distressing. Although this is likely to be the case, there is evidence suggesting

that images such as these are far less common than more 'mainstream' pornographic images (Mehta, 2001).

Finally, Flood (2007) highlighted strong evidence demonstrating that males who are frequent users of particularly violent pornography may evidence strong beliefs supporting sexual aggression in addition to a greater propensity toward sexual violence. This last point represents one of the most important and debated topics in pornography research. There is compelling evidence that the greatest negative effects (behavioural and psychological) are associated with violent pornography (e.g., Malamuth, Addison, & Koss, 2000). Despite a far greater diversity of pornographic content (including self-produced content) being available on the Internet (Bryant, 2009), the majority of research to date (especially in relation to children and adolescents) has addressed 'mainstream' and not violent pornography. Therefore, the evidence for the harmful effects of violent pornography does not *directly* translate to non-violent material.

4.2.2 International literature

In comparison to the Australian-based literature, a relatively large body of research has been completed in the US, as well as in European (e.g., The Netherlands) and Asian (e.g., Taiwan) countries. As would be expected, varying prevalence rates for exposure to pornography has been identified across the countries studied. In the US, Wolak, et al. (2006) found that about 42% of youth reported either deliberate or accidental exposure or

both an increase from the 2000 prevalence rates (Mitchell, et al., 2007a). In relation to the intentional viewing of online pornography, 19 – 21% of US minors (under the age of 18 years) indicated that they deliberately visited a pornographic website (Wolak, et al., 2006). Interestingly, an earlier study reported that 21% of seventh to tenth grade students (13 – 16 years of age) had visited a pornographic website for more than 3 minutes in the previous 30 days (Stahl & Fritz, 1999) suggesting that this age bracket may be when most intentional exposure to pornography occurs.

Ybarra and Mitchell (2005) concluded that, independent of medium of exposure, those who intentionally view pornography were more likely to report delinquent behaviour and substance use in the previous 12 months. However, those who viewed online pornography were more likely to endorse symptoms of depression as well as lower levels of emotional bonding with parents or caregivers. Whether those clinical symptoms are a cause or an effect of viewing Internet pornography is unclear. Finally, Braun-Courville and Rojas (in press) found that adolescents exposed to sexually explicit websites were more likely to have multiple lifetime sexual partners, to have had more than one sexual partner in the last 3 months, to have used alcohol or other substances at last sexual encounter, and to have engaged in anal sex. Further, adolescents who visited pornographic websites displayed higher sexual permissiveness scores compared with those who have never been exposed.

Unintentional (or unwanted) exposure to pornography was recorded for 34% of US 10 – 17 year olds (Wolak, et al., 2006), an increase from previous years where only 25%

reported viewing unwanted pornographic images in the previous 12 months (Mitchell, Finkelhor, & Wolak, 2003). Mitchell, et al. (2007) reported that 44% of US 16 – 17 year olds had been accidentally exposed to pornography while a study by the Kaiser Family Foundation (2001) put this figure closer to 70% (compared to 84% of Australian males and 60% of Australian females). Although the content of the pornographic material that youth were exposed to was not described, only a small percentage (9%) reported being "very or extremely upset" by the exposure (Wolak, et al., 2007b). Cameron and colleagues (Cameron, Salazar, Bernhardt, Burgess-Whitman, Wingood, & et al., 2005) found from web-based focus groups that a number of teenagers who participated described incidences of unintentional exposure occurred after a misleading URL was followed. Finally, in addition to being somewhat distressing for some, exposure to Internet pornography has been associated with engaging in certain sex behaviours, such as oral sex (Kraus & Russell, 2008). This may be related to Internet use, however, it appears that the practice of oral sex has been increasing over the past 15 years (Francoeur, 2004) making it difficult to determine the extent of the influence (if any) of the Internet.

Outside of the USA, Peter and Valkenburg (2006) reported that 71% of Dutch male adolescents actively sought out online sexual material compared to 40% of Dutch female adolescents. Parental control was not associated with not being exposed to pornography suggesting that the youth in this study were viewing pornography independent of whether they were being monitored. However, this was measured using a single item ("My parents know when I am surfing the Internet) and is unlikely to accurately measure "monitoring". Further, the authors acknowledge that this result may reflect the relatively liberal approach

to pornography in The Netherlands where youth may not feel that they must hide the websites they have been viewing from their parents.

One of the most interesting findings reported by Peter and Valkenburg (2006) was that those with faster Internet connections were more likely to expose themselves to pornography than were adolescents with slower Internet connections. It may be that those youth using dial-up connection speeds either did not have the patience to wait for images to download or were concerned about being caught and less likely to risk the time it takes to download Internet pornography using dial-up connection speeds. Consistent with the idea of not wanting to get caught, the amount of time spent online was unrelated to exposure, suggesting that those who view pornography may be specifically logging on to the Internet for this sole reason. Further, Peter and Valkenburg reported that adolescents with a high need for sensation, who were dissatisfied (in general) and who were more interested in sex were all more likely to view pornography online.

Recently, Sabina, Wolak, and Finkelhor (2008) found that among 563 US adolescents, 93% of boys and 62% of girls were exposed to Internet pornography before the age of 18 years. The authors reported that boys were more likely than girls to view online pornography (consistent with every other study in every other country) as well as more extreme images (e.g., rape, child pornography). Further, Livingstone and Bober (2005) reported that 57% of UK 9 – 19 year olds have been exposed to pornography online, and of these youth 38% had seen it via pop-up adverts, 36% had accidentally stumbled onto a pornographic website, 25% had received unsolicited pornographic material by e-mail or IM

and 10% had intentionally accessed this explicit material. Table 4.2.2 below presents prevalence rates for exposure to "unwanted sexual material" by European country.

Table 4.2.2 *Prevalence rates for viewing pornographic or unwelcome sexual content by European county*

Form of risk encountered by children and median response across countries researched	Incidence by European country Note: Percentages refer to online teenagers unless otherwise stated
Sexual content (child as recipient): *…Seen pornographic or unwelcome sexual content* The approximate median response is 40%	Poland: 80% UK: 57% of 9-19 year olds Iceland: 54% of 9-16 year olds Austria: 50% of 10-15 year olds, 60% of 11-18 year olds Norway: 47% of 9-16 year olds The Netherlands: 46% of 13-18 year olds (71% in males, 40% in females) Belgium: up to 40% of 9-12 year olds Ireland: 37% of 9-16 year olds Sweden: 37% of 13-16 year olds France: up to 33% of 12-17 year olds Denmark: 29% of 9-16 year olds Italy: up to 25% of 7-11 year olds

Adapted from Hasebrink, Livingstone, and Haddon (2007).

As can be seen, prevalence rates of between 25% and 80% were reported across a number of European studies. It should be noted that the criterion "seen pornographic or unwelcome sexual content" combines both deliberate and accidental exposure. Further, little information is available that might explain some of the very high rates, for example, in

Poland[12]. Hence, it appears that exposure to pornography occurs more often in a small number of European countries than in Australia. Importantly, as noted earlier, the nature of the pornography being viewed is unknown making it somewhat difficult to compare across both countries as well as studies.

Estimates of exposure to pornography in Asian countries are less clear and far less studied. In Taiwan, for example, approximately 38% of adolescents have had been exposed to Internet pornography (Lo & Wei, 2005). Previous estimates were somewhat higher (44%; Lo & Wei, 2002). However, in Cambodia, estimates of Internet-based pornography exposure were substantially lower at 5.3% (Child Welfare Group, 2003). This rate underestimates the true incidence of youth pornography exposure and is likely based on the relative lack of Internet access. Consistent with this, pornography was much more often viewed in either video (36.8%) or magazine (33.3%) formats.

In one of the very few studies to have examined the longitudinal effects of exposure to pornography, Brown and L'Engle (2009) reported that exposure to pornography for males predicted less progressive gender role attitudes, more permissive sexual norms, sexual harassment perpetrations and having oral sex and sexual intercourse two years after the initial survey. For females, early exposure predicted subsequently less progressive gender role attitudes as well as having oral sex and sexual intercourse. Although this study gives a clear picture of the effect of earlier exposure to sexually explicit material, the results combine both online and offline exposure (although the authors reported that using a

[12] Although the high prevalence rate in Poland may be related to a lack of parental control over Internet use (Zboralski, Orzechowska, Talarowska, Darmosz, Janiak, et al., 2009)

computer to view pornography was the most common medium for males and second most common medium for females – with X-rated movies being more common). Across all forms of media (i.e., music, television, Internet), those youth who were exposed to more sexual content were more likely to be sexually active and to anticipate future sexual activity (Pardun, L'Engle, & Brown, 2005).

4.2.3 Summary

Overall, in terms of exposure to online pornography, it appears that reported prevalence rates for Australian youth are greater than some countries (e.g., the USA) but less than others (e.g., Poland). It has been suggested that European countries reported higher rates of exposure to pornography than the USA as European cultures tend to have a more relaxed and open view about sex and pornography (e.g., Peter & Valkenburg, 2008). McKee, et al. (2008) reported that younger people appear to be consuming more Internet-based pornography than older adults. Other research indicates that younger youth are exposed to pornography more in an offline context (e.g., movies or magazines) than older youth. This developmental trend (i.e., from offline to online to offline exposure and/or consumption of pornography) raises a number of interesting issues. First, from an Australian perspective, given that the sale of X-rated videos and DVDs is illegal except in the Australian Capital Territory (ACT) and the Northern Territory (NT; although it is not illegal for those over 18 years to purchase the videos and/or DVDs), one has to ask how and where minors are obtaining non-Internet based pornographic material? It may be, as others

have suggested, that they are being given magazines or movies by older siblings or friends. It is also plausible that they are viewing their parents' pornography. Regardless, it appears that, consistent with non-Australian research, younger youth are more likely to encounter pornography offline in the form of movies or magazines (e.g., Pardun, 2005; Ybarra & Mitchell, 2005).

In contrast, older youth appear to be more likely to encounter pornography online. However, the developmental relationship between age of exposure and medium of consumption is unclear. For example, it is not possible to say if viewing pornographic magazines results in increased curiosity about sexually explicit material and greater subsequent intentional exposure to online pornography. It is also feasible that those who view pornographic magazines at an early age may be disgusted and upset by it and comprise those do not intentionally seek out pornographic material online. Further, it is also feasible that while lack of awareness, skill, or opportunity presents barriers to viewing pornography material online for younger children, these are easier to overcome for older youth. These are questions that longitudinal research studies can answer. However, the moral and ethical implications of researching exposure to pornography in children and youth mean that it is unlikely that a thorough understanding of the developmental implications of exposure will be obtained.

An important caveat to the research literature described above is the lack of consensus regarding both the nature of exposure (intentional or accidental) as well as the medium in which the exposure occurred. For example, most studies fail to ask participants

to specify what they were doing when the exposure occurred. This is important as it has been suggested that there is variability in the likelihood of exposure. For example, Greenwood (2004, p.742) testified, to the US Congressional Committee on Government Reform on March 13, 2003, that peer-to-peer file-sharing networks tend to be used specifically for the "exclusive purpose of downloading music [and] exposure to pornography on these networks is most often inadvertent." In fact, the staff report that elicited Greenwood's response, had previously reported that "nearly six million video, image, and other files identified as "xxx," "porn," or "sex" were available for downloading on just one popular peer-to-peer network in a recent two-day period" (Committee on Government Reform, 2003, p. 1). The name of that network was Kazaa and, at a random time during that two-day period, there were over 4.3 million concurrent users (i.e., users who were simultaneously logged onto the network).

Other avenues whereby unintentional exposure can occur include:

1. Mirror sites: pornographic websites where the name of the site mirrors better-known websites. These sites were very popular until the 2003 Truth in Domains Name Act was passed by President George Bush making it a criminal act to construct a website with an address that was designed to mislead children and youth and increase the potential of exposure to pornography content[13]. In 2003 John Zuccarini was arrested and jailed for 2 ½ years for owning the websites www.Teltubbies.com

[13] The Act was allegedly brought on by the presence of www.whitehouse.com which was a pornographic website very similar to www.whitehouse.gov, the website of the President of the US.

and www.Bobthebiulder.com (after popular children's characters, the Teletubbies and Bob the Builder), which have since been shut down.

2. Misleading domain names / spelling errors: For example, mistyping www.betscape.com (instead of www.netscape.com) will open a gambling websites. The National Center for Missing & Exploited Children reported that the number of misleading domain names increased from 842 in 2005 to 2101 in 2006.

3. Misuse of brand names: Searching for www.amazon.com will display a link to www.amazon-cum.com.

4. Keyword searches: Searching for toys, dollhouses, girls, or boys can result in links to pornographic websites being displayed. This can also occur when searching for video game characters and cartoon characters (e.g., Pokemon or Dora the Explorer).

Importantly, we do not know if (or what) there are any pre-morbid differences between those who are exposed on the Internet versus those who are exposed while using peer-to-peer applications. Further, we do not know if the pornographic material that youth are exposed to while using the Internet is qualitatively different than the material on file-sharing applications. This limits our conclusions regarding the effects of exposure to Internet-based pornography.

4.3 Violent media

Media violence is by no means a new phenomenon; violent movies have been available for over 75 years and violent television for over 50 years (Huesmann, 2007). Similarly, the opinion that violent media is harmful is not a recent one going back at least to the early 20th century (Kirsch, 2006). Despite the relatively lengthy history of media violence, research examining the relationship between media violence and the Internet (as well as other forms of technology such as mobile telephones) is practically non-existent. Importantly, the role of violent media on the Internet is still largely overlooked. Further, the video filming and sharing capabilities of mobile telephones mean that videos of fights can be quickly and easily distributed to a wide audience.

It should be noted that the specific relationship between media violence and later aggressive and violent behaviours is still debated. Although some authors (e.g., Ferguson, 2007) have highlighted a variety of methodological limitations (e.g., publication bias) that may compromise particular research studies, several meta-analytic reviews have demonstrated statistically significant positive relationship between exposure to violent media and aggressive behaviour, thoughts and emotions, as well as physiological arousal (Anderson & Bushman, 2001). Further, when compared with correlational studies, studies that undertook the challenging task of experimentally manipulating conditions reported stronger effects in the relationship between violent media and these variables (Anderson, 2004). Support for the adverse effects of exposure to violent media is also provided by studies demonstrating that, with prolonged exposure, psychological and physiological

reactivity to violence content diminishes over time, a phenomenon called desensitization (e.g., Fanti, Vanman, Henrich, & Avraamides, 2009).

Although the experimental manipulation of variables causally related to behaviour is difficult, Polman, et al. (2008) reported that children who actively played a violent video game were rated by observers (blind to exposure condition) as acting more aggressively than children who passively watched the same violent video game. Overall, the evidence supporting a link between exposure to violence and later aggression is strong enough that the APA (2000) issued a resolution to "advocate for the reduction of all violence in videogames and interactive media marketed to children and youth." This resolution is supported by comparative studies which indicate the relative strength of the association between media violence and undesirable behavioural indicators (Fig 4.3.1).

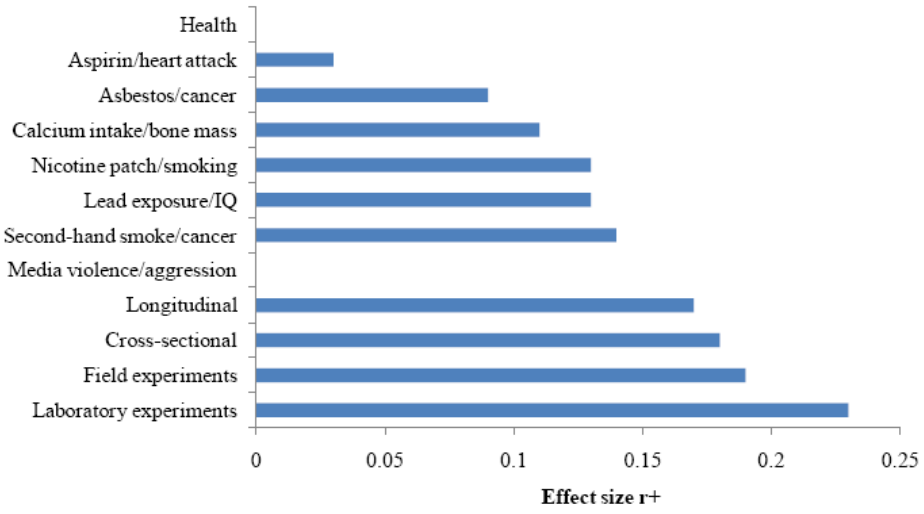

Figure 4.3.1 Overall effect size coefficients between various toxins and health status compared to media violence experiments. Adapted from Gentile, Saleem, & Anderson (2007).

4.3.1 Australian literature

Our examination of the scientific and non-scientific literature revealed few studies (Australian-based or international) that specifically addressed media violence exposure on the Internet. Nonetheless, the relationship between media and violence has long been recognised with early interest discussing the impact of print (e.g., Clarke, 1990) and video media (e.g., Wilson & Nugent, 1987). More recently, a report in The Age newspaper noted that exposure to violent media on the Internet is one of the factors related to a recent increase in youth perpetrated violent crime and has been linked to an 18% increase in the number of adolescents linked with criminal activity from 2005 to 2006 (Russell, 2008). It

is important to note that, despite this seemingly strong relationship, this information is purely anecdotal and no research evidence was provided to support the claim that Internet-based media violence has directly caused an increase in adolescent criminal activity.

The Australian Psychological Society (2000), in a formal position paper, noted that high levels of exposure to violent media was occurring through electronic media. Other groups, such as the Royal Australasian College of Physicians (2004), called for more research to investigate the developmental effects of media technologies and content on children. Although a number of Australian government reports have been prepared on the topic (Sheehan, 1997), little formal experimental research has been conducted. Therefore, given the lack of Australian-specific research, a discussion of the international literature is appropriate.

4.3.2 International literature

The issue of Internet-based violence has, of late, become a vibrant topic in both research and public policy circles. However, practically no experimental studies have been completed investigating the extent of violent content on the Internet. The primary feature of Internet-based violent material is that much of it depicts real people engaging in real acts of aggression. This phenomenon means that the experimental literature, focused mainly on video game violence, has not kept up with type of media that youth are being exposed to. The presentation of violent media on the Internet was highlighted with the leaking and

uploading of video footage showing the execution of Wall Street Journal reporter Daniel Pearl in February 2002. The video, which is still easily available online, shows Pearl being decapitated in very graphic detail. At the time, much of the public debate centred on his death and little was said about the availability of such graphic and disturbing video.

With the exception of the medium of Hollywood-produced horror movies, this level of graphically violent media remained largely unavailable to the general public until the advent of the Internet. Although this is an exceptional circumstance, it is clear that consumers now have access to much more, and increasingly realistic, violent media. The most striking difference between Internet-based violent media and others forms of media relates to the realism of the information available online, a point that has received little attention to date. To gain an estimate of the extent of aggressive and violent content available on the Internet, the first two authors of this report (Dooley & Cross), as part of a pilot study currently underway at ECU, conducted a content survey in August 2008, using the three major internet search engines Google, AltaVista and Yahoo!. The following search terms were used: fight, street fight, school fight, aggression and violence. Table 4.3.1 below presents the number of hits for each term across the search engines used.

Table 4.3.1 *Number of website hits* containing aggression/violence related terms*

Search term	Google hits	AltaVista hits	Yahoo! Hits
Fight	350	1.02 billion	993
Street fight	8.3	288	288
School fight	10.1	395	389
Aggression	22.6	64.1	63.2
Violence	157	540	522

** Website hits are in millions except where noted. In addition, the above data do not solely represent those websites with violent content and can include, for example, anti-violence sites.*

It is clear, given the above, that there is a large amount of violence-related content on the Internet. For example, some websites are dedicated to the macabre and contain graphic pictures of victims of violence (e.g., murder victims and accidental death victims). Others are purely dedicated to the portrayal, glorification and distribution of violent videos depicting real fights. One such website actively promotes and encourages its users to upload videos and it hosts many videos of schoolyard fights and sexually explicit pornography.

This presents an interesting issue in relation to youth as participants – a point raised in the ISTTF report which noted that "some degree of production by minors of violent content is likely, but no studies have specifically looked in depth at minors viewing or creating violent movies online, probably due to the relatively early stage of the adoption of

video sites" (2008, p. 32). A search of videos uploaded to YouTube (a popular video-sharing website[14]) as part of the pilot study mentioned above, revealed a large number of videos with very graphic violent content. Using the search term "fight" on YouTube generated links to millions of videos. Similarly, searching for "street fight" linked to over 300,000 videos[15]. A large proportion of these videos contain unedited footage of real fights (which appear to be filmed using mobile telephones and handheld video recorders) and some of the videos have been viewed millions of times. In addition, there are many hundreds of thousands of video clips on YouTube that contain sexually provocative (although most are not sexually explicit) content and many of these contain disguised links to pornographic websites[16].

European studies have revealed some extremely high prevalence rates for viewing violent media on the Internet (see Table 4.3.2 below). For example, 90% of 10 – 20 year old SNS users in Ireland reported seeing violent or hateful content online. It is unclear if this group of Irish SNS users is a distinct group in relation to their time online or their online viewing habits. Most other countries, where this type of content risk has been examined, reported prevalence rates closer to 40% with the overall median response being 32% across all studies and countries (Hasebrink, et al., 2008). In the UK the rate is marginally lower than the median level at 31%.

[14] Importantly, while pornographic or sexually explicit material is not permitted on YouTube, graphic movies of real fighting are easily available. Despite not being permitted, explicit pornographic material is available on YouTube.
[15] This number was current as of 20 July, 2009.
[16] Disguised links refer to links that are created using a smaller website address that does not contain the name of the original website (e.g., using TinyURL the website http://www.minister.dbcde.gov.au becomes http://tinyurl.com/o7spcx). Many of these links on YouTube direct users to pornographic websites.

Table 4.3.2 *Prevalence rates in a selection of European countries for observing violent or hateful content*

Form of risk encountered by children and median response across countries researched	Incidence by European country Note: Percentages refer to online teenagers unless otherwise stated
Aggressive content (child as recipient): *…seen violent or hateful content* The approximate median response is 32%	Ireland: 90% of 10-20 year olds (SNS users) Poland: 51% of 12-17 year olds Belgium: up to 40% of 9-12 year olds The Netherlands: 39% of 13-18 year olds Denmark: 35% of 9-16 year olds Iceland: 35% of 9-16 year olds France: up to 33% of 12-17 year olds UK: 31% of 9-19 year olds Norway:29% of 9-16 year olds Germany: 29% of 12-19 year olds Sweden: 26% of 9-16 year olds Italy: up to 25% of 7-11 year olds Austria: 15% of 10-15 year olds

Adapted from Hasebrink et al. (2008).

4.3.3 Summary

Overall, there is strong evidence from non-Internet studies that exposure to violent media (often in the form of video games) is related to an increase in aggressive thoughts, feelings and emotions as well as physiological reactivity. The relationship between exposure to violent media and aggression appears to be well established. However, it is clear both from expert commentary and ongoing research at the Child Health Promotion Research Centre at ECU that the violent material easily available on the Internet (e.g., on YouTube) is qualitatively different from what is available in other forms of media (e.g., video games). Again, the capability to upload self-produced videos to sites such as

YouTube fundamentally changes the nature of the content that is available. No longer are youth restricted to stylised Hollywood-esque fight scenes as videos of school yard fights, bar brawls, gang shoot-outs and bike gang attacks, as well as a teenage girls being badly beaten by a gang of rival girls, can be viewed online. Despite this, much research needs to be completed to obtain a clear understanding of the impact of Internet violence.

4.4 Other Problematic Content

Additional problematic content that youth may encounter on the Internet includes hate groups and content depicting or describing self-harm and suicide. However, very little research has been conducted on these topics, especially in relation to the latter content.

4.4.1 Hate groups

Although the research literature is sparse, it has been noted that the "World Wide Web has allowed marginalized extremist groups with messages of hate to have a more visible and accessible public platform" (Leets, 2001, p. 287). Leets noted that after the Oklahoma City bombing in 1995 there was one hate website which increased to 2800 by 2001. In 2004, the Southern Poverty Law Center reported that there were 497 hate sites in the previous year (2004) suggesting either varying criteria used to define a "hate website" or a significant reduction in the number of sites in operation (which is unlikely). Schafer

(2002), in a content analysis of 132 extremist sites, concluded that many of the sites were designed to facilitate discussion and interaction between members. Building on this work, Gerstenfeld, Grant, and Chiang (2003), reported that the majority of sites they reviewed contained links to external websites, approximately half contained information presented in multimedia and half contained racist symbols. Of greatest concern, was that the authors found many websites (some of which are no longer available) which contained webpages specifically for children and youth (some of the material on these pages included games, music, "history" lessons, as well as some home-schooling curricula). As evidence of this, the authors described a video game, called *Ethnic Cleansing*, which was freely available to download and play[17].

Further, current website figures may underestimate the extent of online hate given the emergence of hate group SNS. Chau and Xu (2007) argued that the Web has enabled hate groups (e.g., the Ku Klux Klan) to reach more people than ever before and this is especially the case given the recent use of Weblogs (Blogs) to spread hate messages. Of particular concern, argued Chau and Xu, is that "young people, the major group of bloggers, are more likely to be affected and even 'brainwashed' by ideas propagated through the Web as a global medium. Hatred and extremism ideas could easily be embedded into their minds to make them become members of these hate groups or even conduct hate crimes" (p. 58). We were unable to find any objective research evidence to support this claim.

[17] A search revealed that, at the time of writing this report, the game is still available for purchase from the producers website.

In relation to the prevalence of viewing a hate website, Okrent (1999) found that 25% of US teenagers surveyed had seen a website that contained information about hate groups. Another small scale US-based study reported that chat participants had a 19% chance of exposure to negative racial or ethnic comments when the interaction was monitored and a 59% chance when it was unmonitored (Tynes, Reynolds, & Greenfield, 2004). Despite these findings, it is difficult, with any great confidence, to describe the extent, nature, or impact of Internet-based hate websites.

4.4.2 Content describing or depicting self-harm

A final category of Internet content deemed inappropriate includes those websites that promote, describe and graphically depict self-harm. As noted by Shade (2003), these sites cause tremendous public outcry as they clearly encourage youth to engage in some, if not all, of the practices outlined in their various webpages. However, to date, little has been written about Internet-based self-harm information (Moyer, Haberstroh, & Marbach, 2008). It is clear that, in relation to self-harm, there are many varied online formats, for example, passive Websites, more active bulletin board and group discussions, interactive chat rooms and the visual realities of the cybercafés and cyber pubs (Adler & Adler, 2007a). These resources are fluid, changing constantly, being replaced quickly, and waxing and waning in popularity. Although it is unclear how users move from one resource to another, there is a suggestion that word of a new resource quickly spreads through the self-harming community (Adler & Adler, 2007b).

However, as was the case in relation to the hate group websites, there is a paucity of research literature addressing the prevalence and impact of these online resources. A few studies have examined the relationship between the Internet and self-harm. In the only prevalence study we found, Whitlock and colleagues (2006) identified over 400 self-harm bulletin boards where information on the most effective techniques for self-harming was shared. Further, the average age of users (which were predominately female) was between 16 and 23 years of age with the majority approximately 18 years. The authors noted that, despite the presence of technique requests or posts (6.2%), the majority of posts on the bulletin boards offered informal support for others (28.3%) with a further 19.5% discussing motivations and triggers. Whitlock, et al. note that much of the content in the bulletin boards may expose adolescents to a subculture that normalises self-harming behaviour – a concern shared by others (e.g., Rodham, Gavin, & Miles, 2007). Furthermore, it has been reported that the potential damage that these websites can promote is of concern as the youth who are engaging in self-harming behaviours is more likely to have concurrent mental health issues, a positive history of abuse and a poor relationship with parents (Mitchell & Ybarra, 2007).

Similarly, it is likely that those youth who are visiting the anorexia and bulimia websites are likely to have some existing issues in their attitude to food. As noted, the research in this area is non-existent and accessing these sites and their users may be further hindered when efforts to control and regulate this content pushed the sites underground. Now, it is more commonplace that sites will describe themselves as "pro-ana" or "pro-mia" and never specifically mention anorexia or bulimia. Again, we are severely limited in the

conclusions that can be made due to the distinct lack of research (and non-research) literature on being exposed to hate or self-harm sites.

SECTION 5

REVIEW OF AUSTRALIAN AND INTERNATIONAL LITERATURE ON THE PROMOTION OF INAPPROPRIATE SOCIAL AND HEALTH BEHAVIOURS

Summary section

Internet addiction

- An Australian study demonstrated that there was no evidence to suggest an association between the amount of time spent online and symptoms of depression, anxiety or social fearfulness.
- A number of international studies have associated excessive Internet use with symptoms of depression, social phobia, hostility, as well as problems with the family, in school, with physical health and personal finances.

Self-harm / suicide

- Many websites and bulletin boards openly discuss self-harm and suicide techniques.
- Most of those who visit self-harm / suicide websites are females approximately 20 years old.

Anorexia

- Exposure to anorexia promoting websites resulted in increased negative affect, lower self-esteem and lower appearance-related self-efficacy.

Drugs / cigarettes

- The promotion of illicit drugs is commonly found on the Internet.
- Over 93% of attempts to purchase cigarettes were made without proof of age verification required.

5.1 Overview

As with other topics in this review, the promotion of inappropriate social and health behaviours on the Internet potentially covers a limitless range of issues. However, our review of the literature has revealed that there are a number of issues of concern to youth, parents and community members. Initially, our review will address an emerging phenomenon, namely Internet addiction. This issue is fast becoming recognised as a potentially major social and health consequence of the Internet (although the empirical literature is limited). Further, we will address additional literature that relate to the promotion of *self-harm / suicide*, *eating disorders* (e.g., anorexia nervosa), *illicit drug use* and *cigarette use*. Finally, we will address a number of more general *physical* (e.g., technology related neck and back pain) and *social health* (e.g., social bonding) issues. It should be noted that although the explicit literature regarding the social health implications of the Internet is limited, there is sufficient evidence from other areas of cyber risk research to interpret the existence of general social problems. Given the limited Australian and international-based research on the issues outlined above, the available literature will be reviewed accordingly by issue.

5.2 Internet addiction

There continues to be much debate regarding Internet addiction (IA) in terms of the nature of the construct and whether it exists as a diagnosable addiction in a similar vein as

other types of addictions (e.g., gambling addiction). Diagnostic criteria conceptualise problematic Internet use (or IA) as an impulse control disorder where "an individual experiences rising tension or arousal before Internet use and a sense of relief or pleasure after completion of the behaviour" (Shapira, Lessing, Goldsmith, Szabo, Lazoritz, & et al., 2003). IA is generally considered to be comprised of the following: maladaptive preoccupation with Internet use; the use of the Internet for periods of time longer than planned; using the Internet or the preoccupation with its use causing clinically significant distress or impairment in social, occupational, or other important areas of functioning and excessive Internet use that does not occur exclusively during periods of hypomania or mania and is not better accounted for by other Axis 1 disorders (APA, 2004). It is believed that the criteria need to be both broad enough to capture problematic Internet users for systematic study but not so broad as to ignore other known psychiatric disorders that may account for the patient's symptomatology. Tables 5.2.1 and 5.2.2 below list the first- and second-order (primary and secondary) constructs associated with IA[18].

[18] These tables have been adapted from Douglas et al. (2008).

Table 5.2.1 *First-order Internet addiction constructs*

Construct	Theme	Theme description
Antecedents	Internet experience	Years using the Internet, the length of time spent online. Environments where participants reported using the Internet: college labs, work places.
	Social factors	Being alone, loneliness.
Pull factors	Sociability	Ease of social interaction, facilitation of exchange of ideas.
	Addictive applications	Applications available on the Internet that enhance the entertainment and social value.
	Internet ubiquity	The Internet's ubiquity combined with the ease of access and the availability of information. Use of the Internet in place of other media to communicate with the world.
	Compulsion activities	Cyber-sex/porn, and -relationships, gambling, etc.
Push factors	Interplay of virtual and real self	Choosing an online identity completely different from reality, or compensating for shortcomings of reality.
	Escapism	Individuals who tend to suffer from an inferiority complex and lack confidence.
	Psychological needs/motivations	Diversions from loneliness and boredom, stress release, relaxation, discharging anger and frustration.
Negative effects	Impacts	Five main areas with significant impact on individual's lives are: academic, relationship/personal, financial, occupational and physical. Positive impacts include self-identification, closer relationships with friends, bonding with the world.
	Symptoms	Considers the various symptoms of IA: preference for computer over family and friends, thinking about being online, feeling moody when not using the Internet, etc.
	Pathological tendencies	Including: endless computer upgrades, changing sleep patterns, etc.
Control strategies	Self-regulation	Attempts made by individuals to control the habitual use of the Internet, as well as any behaviour resulting from this control: shopping, reading, visiting friends, other.
	Coping activities	Renewed interest in pursuing real-life day-to-day activities.

Table 5.2.2 *Second-order Internet addiction constructs*

Construct	Theme	Theme description
Profile	Internet addict profile	Candidate appears to have little or no social life and/or self-confidence in addition to denying there is a problem.
Antecedents	Internet experience	Relatively new users of the Internet may be at a higher risk for developing addictive patterns than others.
	Social factors	Individuals who feel misunderstood and lonely may use virtual relations to seek out feelings of comfort and community.
Pull factors	Internet as replacement for other media	An increase in the dependence on the Internet for communication.
	Addictive applications	The Internet itself is not addictive; rather it is the prevalence of applications, such as chat, email, games, and gambling that increases an individual's likelihood of becoming addicted.
	Internet features	Five key features of the Internet include: affordability, counteraction of depression or other medical conditions, communication efficacy, ease of use, and anonymity.
Deviant behaviours	Online offending behaviours	Downloading, trading, production of child pornography, commission of a contact offence, internet seduction of children among others.
	Areas of Internet dysfunction	Four key areas for Internet dysfunction include deceptive behaviour, cyber-affairs affecting real relationships, subjective escape and sociability for extremely shy individuals.
Negative effects	Impact of Internet use	Heavy Internet use may not result in negative effects if online friendship is a part of overall friendship patterns.
	Consequences of Internet abuse	Real life leisure time activities are replaced by maladaptive behaviour towards the Internet.
Control strategies	Self-regulation	Productive use of the Internet possibly involving self-regulating practices.
	Coping activities	Coping activities appeared to be transitional, essentially only helping participants pass time until their next log in.
	Internet addiction education	Getting students to become aware of appropriate and productive use of the Internet is an important task.
	Treatment	There is a need for the development of effective treatment protocols to handle the increase in IA.

Many parents, teachers and practitioners are concerned about young people using the Internet excessively; however, conjecture exists within the literature as to what constitutes problematic Internet use. Addictive use of the Internet has no official name and is not classified as a disorder, and there are no clearly defined features to diagnose such a disturbance (Zboralski, et al., 2009). In recent years, psychological literature has found that individuals who exhibit problematic Internet use often also suffer from other psychiatric disorders (e.g., Yen, et al., 2007).

Young (1999a, b) argued that IA is a broad term covering a variety of behaviours and impulse control problems that can be categorised into five main areas:

1. Cyber-sexual addiction: Compulsive use of adult websites for cyber-sex and cyber-pornography;
2. Cyber-relationship addiction: Over-involvement in online relationships;
3. Net compulsions: Obsessive online gambling, shopping or day-trading;
4. Information overload: Compulsive web surfing or database searches, and
5. Computer addiction: Obsessive computer game playing (e.g., Doom, Solitaire, etc.

Other research has suggested that excessive Internet use shares some characteristics of substance abuse (e.g., Brian &Wiemer-Hastings, 2005). It has also been suggested that

problematic Internet use may be a similar construct to pathological gambling (Mitchell, et al., 2005). Evidence from China has demonstrated that adolescents with IA were more likely to have engaged in aggressive behaviours in the previous 12 months (Ko, Yen, Liu, Huang, & Yen, in press). Even if Internet use is harmful to an individual, it is not yet clear whether this signifies a separate disorder entity or is a manifestation of an underlying mental health problem.

Prevalence of problematic Internet use has been studied in many countries and among many cohorts. For example, Kaltiala-Heino, Lintonen and Rimpela (2004) conducted a study involving 7,292 Finnish children aged 12 – 18 years to assess the prevalence of features consistent with harmful use of the Internet. While prevalence rates were much lower (less than 2%) than in previous studies, some adolescents anecdotally reported using the Internet in ways comparable to other addictive disorders. Prevalence rates as high as 61% have been reported, depending on the type of inventory scales used to determine such rates (Mitchell, Becker-Blease, & Finkelhor, 2005).

> "...it would seem premature at this stage to use one label for the concept [of Internet addiction], as most of the studies conducted in the field so far have presented varying degrees of differences and conflicting results."
>
> *Widyant & Griffiths, 2006, p.48*

Variance in prevalence rates of IA has been reported and probably depends on how this disorder is conceptualised. For example, Young (1996) developed a questionnaire based on the Diagnostic and Statistical Manual of Mental Disorders (4th edition; APA, 2004), which modified criteria for pathological gambling to provide a screening instrument for problematic Internet use. Of the 396 US college student participants, 2% experienced academic and relationship difficulties and 15% experienced mild occupational and physical difficulties as a result of excessive Internet use. Yao-Guo, et al. (2006) surveyed 476 Chinese junior high school students and found that about 11% suffered from Internet addiction and, when compared to their peers, reported more emotional and personality problems. Prevalence rates of up to 25% have been reported in Poland (Zboralski, et al., 2009) – although upon closer examination, this prevalence rate includes both those students who reported "abusing the computer and Internet" as well as those who were "in danger of the problem". Neither category was described in sufficient detail to enable a discussion of their accuracy.

Research conducted in Australia examined the psychological consequences of Internet use in undergraduate university students (Campbell, Cumming, & Hughes, 2006). An online study was conducted with 188 participants who rated themselves as regular users of the Internet[19]. Participants reported that they used the Internet as a vehicle for expanding social networks and consequently enhancing the chance of meaningful relationships, self-confidence, social abilities, and social support. No evidence was provided indicating a

[19] Given the mode of data collection, it is feasible that this sample was biased and, thus, not generalisable to the general public.

relationship between the amount of time spent online and symptoms of depression, anxiety, or social fearfulness. While those who primarily used the Internet for online chat, reported that it was psychologically beneficial to them, they also opined that frequent Internet users are lonely and that the Internet can be addictive.

Recently, Yen, et al. (2007) examined the association between IA and depression, Attention Deficit / Hyperactivity Disorder (ADHD), social phobia, and hostility for adolescents. A total of 2,114 Taiwanese students aged 15 to 23 years (Mean age = 16.3 years) participated in the research. Self-report questionnaires were completed and based on their responses, it was found that adolescents with Internet addiction had higher ADHD symptoms[20], as well as symptoms of depression, social phobia, and hostility. However, hostility was associated with IA only in males. Yen, et al. concluded that online gaming was the best predictor of IA, and that effective evaluation and treatment for symptoms of ADHD and depression were required for adolescents with IA. Yen, et al. further concluded that male adolescents with high hostility required more attention in preventive strategies and therapeutic interventions for Internet addiction. In another Taiwan-based study, Tsai and Lin (2003) interviewed 10 high school students (8 male, 2 female; all were 16 – 17 years of age) who scored in the highest range on the self-report Internet Addiction Scale for High School Students in Taiwan. The authors reported that "almost all of the interviewed adolescents once tried to withdraw from the Internet but then felt depressed and the withdrawal was usually not successful" (p. 650). Further, significant levels of impairment

[20] This is not to be confused with a formal diagnosis of ADHD but **refers to symptoms of inattentiveness, hyperactivity and impulsivity**. The authors did not report the breakdown of symptoms.

in the following areas: school, family, health and finance were reported. For example, students reported spending more time online than anticipated which negatively impacted on their academic performance. An interesting finding of this study was that many of the students (specific number unknown) reported that they were addicted to the social interaction afforded by the Internet.

> "Many of the adolescents in this study were addicted by the messages and activity on the Internet, but not by the Internet as a medium per se."
>
> *Tsai & Lin, 2003, p.651*

Jang, Wang and Choi (2008) investigated the independent factors associated with addiction to the Internet, particularly psychiatric symptoms. They conducted a study with 912, 7^{th} – 12^{th} grade students (Mean age = 13.9 years) in four high schools in Seoul, South Korea and demonstrated that 3.7% of junior high school students and 5.1% of senior high school students reported being addicted to the Internet. The authors also demonstrated that symptoms of obsessive-compulsion and depression were significantly correlated with Internet addiction. Jang, et al. reported that male gender was independently associated with the transition from intermittent addiction to Internet addiction. Therefore, as has been suggested by others (e.g., Zboralski, et al., 2009), pathological Internet usage appears to be

an issue more commonly observed in boys. The underlying process involved in males compared to females is, however, unclear.

Problematic Internet use has not only been correlated with psychiatric symptoms, but also with factors associated with other types of maladaptive behaviours. For example, it has been suggested that dysfunctional family structure is correlated with problematic Internet use (Ko, Yen, Yen, Lin, & Yang, 2007; Park, Kim, & Cho, 2008; Zboralski, et al., 2009). Park, et al. (2008) examined factors associated with excessive Internet use in middle and high school students in South Korea. Of the 903 returned self-administered questionnaires, 11.9% were classified as Internet addicted. Risk factors of family violence (e.g., marital violence and parent-to-child violence) were found to be strongly associated with Internet addiction. Interestingly, conversation time with parents was not associated with Internet addiction, suggesting that the quality of a relationship between parents and youths is more important than the quantity of time spent together and that the quality of the relationship may have more significant influences on adolescent negative behaviours. An unexpected finding of the research, and in contrast to previous findings (e.g., Jang, et al., 2008), was that gender was not significantly related to Internet addiction.

Individual personal characteristics have also been researched in relation to problematic Internet use. For example, Chou and Hsiao (2000) investigated excessive Internet usage among college students in Taiwan. Among participants who reported excessive Internet usage, self-reported communication associated with the Internet was the most powerful predictor of problematic Internet use, followed by sex satisfaction. These

authors also reported that addicted users of the Internet rated the impact towards study and daily life routines (e.g., meals, sleep, appointments and classes) more negatively than their non-addicted counterparts. Furthermore, it has been demonstrated that excessive Internet use has been associated with sleep deprivation (Brian & Weimer-Hastings, 2005; Punamaki, et al., 2007).

Another Taiwanese study that examined individual characteristics associated with problematic Internet use among adolescents (16 –24 years of age; $n = 416$) focused specifically on the relationship between Internet addiction and online gaming (Wan & Chiou, 2007). The authors demonstrated that adolescent players who exhibited addictive characteristics also displayed higher intrinsic motivation than extrinsic motivation (i.e., they were more motivated by internal factors) suggesting that those who demonstrated the most addictive behavioural patterns were not primarily motivated by overt aspects of the game (e.g., winning points or stages).

Douglas, et al. (2008), in a recent synthesis of the qualitative research literature on Internet addiction, reported that the:

1. Main antecedents of Internet addiction include:
   - Feelings of isolation, loneliness, low self-confidence and self-esteem.
2. Main symptoms of Internet addiction include:
   - Excessive time spent online, denial that the problem exists, moodiness and irritation when offline.
3. Negative effects of over-engagement with the Internet are multiple and include developing problems in any of the following areas
   - Scholastic, occupational, interpersonal, financial, or physical.

One of the few longitudinal studies conducted (involving 2,790 online gamers), demonstrated that a player's internal reasons for playing influenced the development of problematic usage, but that these effects were overshadowed by the importance of self-regulation in managing both the timing and amount of play (Seay & Kraut, 2007). Further, the authors demonstrated that the level of self-regulatory activity was important in enabling online gamers to avoid negative outcomes such as problematic use.

Gambling is another aspect of online gaming that has been shown to be associated with problematic Internet use among adolescents. In their review Griffiths and Wood (2000) suggested that the Internet is an easily accessible forum for gambling by young people and the authors argued that underage gambling is a serious issue that needs to be addressed. The authors noted that there are distinct similarities between online gaming and gambling in relation to the processes involved in their development and maintenance in

particular as they relate to behavioural outcomes. Griffiths and Wood (2000, p. 213) reported that these outcomes include:

> …stealing money to play arcade games (Keepers, 1990; Klein, 1984), stealing money to buy new games cartridges (Griffiths & Hunt, 1998), engaging in minor delinquent acts (Kestenbaum & Weinstein, 1985), using lunch money to play (McClure & Mears, 1984), truancy in order to play (Keepers, 1990; Griffiths & Hunt, 1998), not doing homework/getting poor grades (Griffiths & Hunt, 1998; Phillips, et al., 1995), sacrificing social activities to play (Egli & Meyers, 1984; Griffiths & Hunt, 1998), irritability and annoyance when unable to play (Griffiths & Hunt, 1998; Rutkowska & Carlton, 1994), playing longer than intended (Griffiths & Hunt, 1995, 1998; Phillips, et al., 1995) and an increase in self reported levels of aggression (Griffiths & Hunt, 1995, 1998). In a related review of the literature, Brown (2006) suggested reasons for the increase in online gambling: popular media; comfort level with technology; twenty-four hours a day, seven days a week access; anonymity, and access to credit. It should be noted that the reasons mentioned above are not specific to youth.

> "Before heralding a new disorder labelled an addiction, it is imperative that the first step taken is to provide empirical data that supports the presence of the salient features of an addictive disorder. In this regard, given that neuroadaptation involving [brain] reward circuitry plays a central role in the chronic maintenance of licit and illicit substance dependency, it is incumbent on researchers to demonstrate similar alterations in brain chemistry in excessive Internet users."
>
> *Blaszczynski, 2006, p. 8*

5.3 Self-harm/suicide

A review of self-injury Internet message boards was conducted by Whitlock, Powers and Eckenrode (2006) to investigate the role of message boards in disseminating information about self-injurious practices. The authors examined the prevalence and nature of the message boards and their users, as well as the specific content areas raised for discussion. Of the 406 message boards identified, 10 were chosen for content analysis. Members of the discussion boards described themselves as mostly female between 12 and 20 years. Findings indicated that interactions between members tended to normalise and encourage self-injurious behaviour and add potentially lethal behaviours to the repertoire of established adolescent self-injurers and those exploring identity options. Whitlock, Powers and Eckenrode concluded that access to a virtual subculture of like-minded others may expose and reinforce the behaviour for a large number of youth.

There is much disagreement as to whether these discussion groups increase or decrease self-harming behaviour despite the large number of groups available. One of the most important studies on self-harm on the Internet was conducted in Australia; Murray and Fox (2006) investigated both positive and negative aspects of membership to a self-harm discussion group. Participants (n = 102) were recruited via postings to a self-harm Internet discussion group, with the majority of respondents being female. The mean age of participants was 21.4 years while the mean age at which respondents had begun self-harming was 13.6 years.

Participants completed a web-based questionnaire and content analysis was conducted on the data. While findings indicated that the majority of participants viewed the discussion group as having positive effects, for some there was a negative impact. Specifically, 11% of respondents indicated they had learnt and enacted more severe methods of self-harm and also felt less of a need to stop self-harming as a consequence of exposure to the group.

Suicide, the most extreme outcome related to self-injurious behaviour, has generally escaped the censorship of electronic communication. A handful of reported cases have linked Internet use with suicide attempts, but it is unclear if there are additional unreported cases (Borzekowski, 2006). Pro-suicide websites include in their content, accounts of completed suicides, information on suicide methods, academic research on suicide and interactive discussion (Baume, Rolfe, & Clinton, 1998). The impact of suicide on subsequent suicides (i.e., copy-cat cases) was greatest among adolescents (Schmidtke & Schaller, 2000). With this in mind, Baume, Rolfe and Clinton (1998) investigated how suicide fatalities influenced the behaviours of vulnerable adolescents who expressed suicidal ideation in cyberspace. The authors described the effect of suicide modelling, a term used to describe the effect of inducing more completed suicides as people model the behaviours of icons or peers who have taken their lives, and suggested that this was a major source of information for young people on the Internet. Suicide notes were also found to be abundant on pro-suicide websites, which give users of these websites a sense of the frame of mind of individuals who choose to take their own life. Of grave concern is that clustering of suicides have been known to occur, suggesting an imitation or copycat effect

that occurs following media coverage or contact with a suicide. Therefore, there is potential for suicide related information found on the Internet to influence the state of mind of a young person who is experiencing suicidal thoughts and, because of the interactive communication component, to do so more strongly than the print media, television and films.

> "…it was suggested that young people are more likely to be influenced by the internet to commit suicide than older people. This is because young people have a higher incidence of risk-taking behavior, co-morbid substance abuse, and depressive disorder. Adolescents without social support may be particularly vulnerable because of the high suicide rate in this age group."
>
> *Alao, Soderberg, Pohl, & Alao, 2006, p. 490*

Illustrating how suicide websites can potentially trigger suicidal behaviour in predisposed adolescents, Becker, et al. (2004) described a case study of a 17-year-old female who visited suicide websites, where she researched reliable suicide methods, contacted an anonymous user and purchased substances to be used for suicide. It was reported that she had got the idea of using suicide as a problem-solving strategy only through the Internet. Becker, et al. concluded that youths with dependent, insecure, frightened and evasive traits might especially be at risk, as well as those who cannot express their worries, fears and sadness to a parent and thus look for guidance on the Internet. As a result of the promotion of suicide and suicide methods on the Internet,

widespread concern exists as well as calls for mandated legal control of such sites. Recent developments in Europe and Australia have noted jurisdictional complexity as an obstacle to effective application (Mishara & Weisstub, 2007). Public concern about the vulnerability of Australian youth recently gave rise to the enactment of amendments to the Australian Criminal Code, which criminalised any Internet activity that intentionally related (directly or indirectly) to the incitement of suicide (Commonwealth of Australia, 2004). Further, under existing Australian law, any Internet site that actively promotes or instructs in methods of violence (including self-harm and suicide) are considered prohibited content under the Broadcasting Services Act (1992) and, thus, would be classified RC (Refused Classification) under the National Classification Scheme (see www.classification.gov.au).

> "Eliciting a careful and sensitive internet history as part of routine psychiatric history taking may prove invaluable in assessing young people at risk of self-harm and suicide and in uncovering other aspects of psychopathology associated with excessive or unhelpful internet use."
>
> *Cooney & Morris, 2009, p. 185*

5.4 Anorexia

Pro-ana websites refer to websites that glorify anorexia nervosa as a way of life; they advocate anorexic behaviour should be understood not as a disease but rather a special lifestyle and an outstanding achievement (Grunwald, Wesemann, & Rall, 2008). In recent years, the number of pro-ana websites has grown (Shade, 2003). A number of studies have been conducted to explore the content and impact of pro-anorexic websites and have demonstrated that, typically, most pro-ana websites include a forum for discussion, links to chatrooms, a gallery (which usually feature fashion photographs of thin models), and links to other websites (usually pro-ana support sites, but in few cases recovery and health sites) (Shade, 2003). Interestingly, Chesley, et al. (2003) concluded in their investigation of pro-ana websites that compared to pro-recovery sites, pro-ana websites were generally much better organised and more comprehensive, which may be seen as an attempt to heighten the appeal of the website.

Pro-ana websites have also been examined in terms of their support for those with anorexia nervosa. In one of the few published, peer-reviewed studies to date, Fox, Ward and O'Rourke (2005) explored the types of support that individuals perceived through pro-ana websites and the facilitation of the disease that occurs from such perceived support. The authors proposed an anti-recovery perspective on the disease by suggesting that pro-ana websites safely encouraged the management of a dangerous lifestyle. Ethnographic and interview data were collected from participants in the *Anagrrl* website and online

forum. As with other studies, the majority of participants were female and ranged from 17 – 20 years of age (those most often frequenting pro-ana websites).

Perceptions of support included a safe and positive place to share experiences free from the prejudices of society, which facilitated normalisation of the disease through communication. Tips and tricks on anorexic behaviours are provided and individuals can place photos of themselves on these websites. This type of support is perceived to provide *thinspiration* – a term used by many pro-ana websites as a form of encouragement to remain underweight. Fox, et al. (2005) concluded that pro-ana websites provide individuals experiencing anorexia nervosa with routines and rituals that are considered extreme and risky. Further, pro-ana websites normalise, control, justify and legitimise anorexia behaviours through the sharing of information, risk management and support.

The impact of viewing pro-ana websites was investigated by Bardone-Cone and Cass (2007) in one of the few methodologically rigorous studies available addressing this topic. A comprehensive study was conducted which examined the effects of viewing a pro-ana website by asking participants to view either a construction of a prototypic pro-ana website or one of two comparison websites related to female fashion or home decor. Female undergraduates (n = 235) were randomly assigned to either the pro-ana condition or the fashion condition. Those who were exposed to the pro-ana material reported significantly more negative affect, lower self-esteem and lower appearance related self-efficacy than those who viewed a comparison website. Bardone-Cone and Cass concluded

that pro-ana websites are a troubling influence on certain individuals, especially those who are searching for, and forming self-identity.

To determine the impact of eating disorder websites on those currently suffering from the illness, Keski-Rahkonen and Tozzi (2005) investigated whether viewing anorexia nervosa recovery support group websites impeded recovery from anorexia nervosa. An exploratory Internet-based study was conducted to address the recovery process in eating disorder sufferers. Utilising qualitative methodology, messages (n = 685) posted in a Finnish-language eating disorder discussion group were analysed for the context of word recovery. Results suggested that the beneficial role of Internet support groups in the process of recovery may be limited to the early stages of recovery and that active participation delayed recovery in the last stages of change. The authors concluded that in the later stages of treatment, patients should be encouraged to leave discussion groups and to reach out for other activities.

5.5 Drugs and cigarettes

Pelling (2004) argued that the Internet has the potential to influence the attitudes of children and adolescents regarding substance use and may also be able to influence the ability of youth to gain access to illicit substances. As such, the US Department of Justice (USDOJ; 2002) has been investigating this influence. The following discussion about illicit substance use will focus primarily on the promotion of illicit drug and cigarette

consumption on the Internet in adolescents. This is largely because an extensive search of the literature did not reveal any quality research regarding the promotion of underage alcohol consumption on the Internet.

The facilitation of drug-use appears to be the most common drug-related activity on the Internet. Information about drug use, drug production and wholesale quantities and suppliers can be easily accessed on the Internet (USDOJ, 2002). According to the USDOJ (2002) marijuana is the most common drug promoted on the Internet, followed by Methylenedioxymethamphetamine (MDMA; common name *ecstasy*), d-lysergic acid diethylamide (LSD; common name *acid*) and gamma-Hydroxybutyric acid (GHB; common name *Liquid Ecstasy*). Many of the websites that are dedicated to drug use glamorise drug use while others implicitly promote drug use and experimentation (USDOJ, 2001).

With amphetamine use (such as *ecstasy*) such a public concern, an assessment of the quantification of online availability and portrayal of amphetamine-class prescription stimulants was conducted by Schepis, Marlowe and Forman (2008), with a focus on those medications commonly prescribed to and abused by adolescents. These consist of central nervous system stimulants, which are medications indicated for the treatment of ADHD, sleep disorders and obesity. The authors conducted a web search to assess the frequency of websites offering to sell controlled stimulants or websites that directly linked to retail sites. The findings suggested that multiple websites offer to sell controlled stimulants without requiring a valid prescription and that retail sites used legitimising images (e.g., individuals in laboratory coats) and written claims of legality for their activities. Based on their

developing reasoning skills, adolescents may be more vulnerable to such claims. It should be noted that pro-use websites did appear in the searches, although with a much smaller frequency. Schepis, et al. (2008) concluded that the extent to which youth are obtaining these drugs via the Internet remains unclear, but clinicians must be aware of the potential for abuse. Further, although it is clear that illicit drugs can be obtained via the Internet, it is unclear who is actually purchasing them.

The emergence and growth of Internet cigarette sales has concerned policymakers and tobacco control advocates because, as has been suggested, the Internet has the potential to undermine years of progress in restricting tobacco advertising and promotion, and reducing youth access to tobacco (Ribisl, Kim, & Williams, 2002; Ribisl, Williams, & Kim, 2003). Cigarettes are easily accessible via the Internet and a recent study found that minors could successfully receive cigarettes, through credit card and money order purchases, without ever having their age verified (Ribisl, et al., 2003). Ribisl, et al. (2002), who were the first to publish empirical research characterising web-sites selling cigarettes in the United States, conducted a cross-sectional study to determine the proportion of Internet cigarette vendors who would sell cigarettes to minors. Adolescents (n = 4) aged 11 to 15 years of age made 83 attempts to purchase cigarettes via Internet vendors in the US[21]. Of these attempts, 93.6% of credit card and 88.9% of money order purchases were successfully received without proof of age verification required. Other estimates of successful purchases by adolescents resulting in cigarettes being obtained using Internet-based

[21] This is a relatively small sample both of attempts to purchase as well as of the adolescent participants who were attempting to make the purchases.

vendors (without verification of age required) ranged between 71% and 76% (Bryant, Cody, & Murphy, 2002; Jensen, Hickman, & Landrine, 2004). Clearly, by failing to conduct adequate age verification[22], the growing number of websites selling tobacco products makes it easier and cheaper for children and adolescents to purchase cigarettes (Campaign for Tobacco-Free Kids, 2005). However, as with illicit drugs, knowing that adolescents *can* purchase cigarettes over the Internet does not automatically tell us if they *are* purchasing them.

We located one quality study that may offer some insight on who is purchasing cigarettes via the Internet. To address this, Unger, Rohrbach and Ribisl (2001) examined the prevalence of attempts to purchase cigarettes via the Internet amongst adolescent smokers by assessing the behaviours of 17,181 tenth and twelfth grade students residing in California, US. Among youth under 18 years of age who described themselves as current smokers (n = 1,689), only 2.2% reported attempting to purchase cigarettes on the Internet. This suggests that among those youth who classify themselves as smokers, the vast majority were still obtaining their cigarettes offline. More recently, a study by Fix, et al. (2006) assessed trends of youth cigarette purchasing behaviour on the Internet. A longitudinal design was employed to determine the trends of ninth grade students (n = 7,019) in New York (students surveyed in 2001 and 2005) with data aggregated to examine trends in youth smoking behaviour. The authors reported that students surveyed in 2005 were 2.6 times more likely than those surveyed in 2001 to have purchased cigarettes over the Internet. The characteristics associated with a greater likelihood of attempting to

[22] The use of age verification technology is discussed in Section 7.6.

purchase cigarettes on the Internet were younger age, male sex, frequent smoking, and low perceived access from other sources.

Several studies have conducted content analyses to assess the accessibility and appeal to youth of cigarette marketing sites on the Internet[23] (Hong & Cody, 2002; Malone & Bero, 2000; Ribisl, 2003; Ribisl, et al., 2002). All studies found that images of young, attractive individuals were frequently associated with smoking, thus, portraying smoking as a glamorous, sexy, and popular lifestyle to youths. Most tobacco sites were found to be e-commerce sites with many selling a range of products, including lighters, music and art. Many websites were also found to be closely related to the sites young people frequent, such as, shopping, hobbies and recreation by featuring pictures of celebrity smokers, providing information about smoking in movies as well as providing advice to teenage smokers. Overall, it has been suggested that tobacco-marketing websites may be particularly effective in encouraging smoking uptake in young adults and use sophisticated and successful strategies to engage users in the product (Freeman & Chapman, 2009).

Many SNS have also been shown to provide brand naming of tobacco products (Freeman & Chapman, 2008); for example, a search on Facebook of 'Marlboro cigarettes' revealed 82 related interest groups[24]. This raises the issue of individuals creating interest groups not explicitly for advertising purposes but that still represent products thus implicitly advertising them. The website YouTube has also been implicated in the implicit

[23] Websites were identified using a common Internet search engine and searching using smoking-related keywords.

[24] On 2 May, 2009, we searched Facebook using the search term "Marlboro cigarettes" which resulted in 190 groups being displayed. Some groups had only one member while others had hundreds.

advertising of tobacco products with content analyses identifying numerous video clips that glamorise smoking, for example, one playlist is titled "favourite smoking movies" (Freeman & Chapman, 2007; Turtle, 2007). Finally, in a review of state laws governing Internet delivery sales of cigarettes in the United States, it was reported that recent growth of delivery sales of tobacco products via Internet vendors has prompted states in the US to implement new regulations focused on preventing youth access (Chriqui, et al., 2008). Vendors operating overseas, whose practices are difficult to regulate, present an additional threat to tobacco control (Knowles, Wanke, & Kawachi, 2004). To the best of our knowledge, Australian state laws are yet to implement such policies to reduce the potential of the Internet as an avenue for the purchase of tobacco products by minors.

5.6 Physical Health

There is little Australian or international research investigating inappropriate general physical health behaviours of adolescents and children on the Internet. A US-based study conducted by Jacobs and Baker (2002) investigated the ergonomic design of workstations and musculoskeletal well being of a sample of 12 year old students. The authors reported that ergonomics relating to young people and workstation setup was neglected, that furniture was often inadequate and there were issues relating to keyboard and monitor placement, as well as the fact that children's heels may not touch the floor when using adult sized chairs. These factors can all lead to musculoskeletal problems, especially in relation to an increased amount of time spent using a computer (Jacobs &

Baker, 2002). A similar study investigated how the use of computers, the Internet, and mobile phones are related to neck and shoulder pain and lower back pain (Hakala, Rimpela, Saarni, & Salminen, 2006). A self-report questionnaire was conducted on 14 –18 year old (*n*=6,003) students in Finland. Participants reported that the amount of time spent using computers and mobile phones was related to neck, shoulder and lower back pain. Hakala, et al. concluded that increased computer-related activities and mobile phone use represent independent risk factors for neck, shoulder and lower back pain.

An Australian study examined sedentary behaviours, including technology use, in relation to obesity in 11–14 year old youth (Burke, et al., 2006). However, this study did not find a significant direct relationship between obesity and technology use (Burke, et al., 2006). Interestingly, a Finnish study reported that computer use was significantly related to obesity in 16-year-old girls but not in 14- and 18-year-old girls (Kautianen, Koivusilta, Lintonen, Virtanen, & Rimpela, 2005). The nature of this relationship between age, obesity and technology use is, however, unclear.

5.7 Social health

As Internet use is an isolating activity, studies have researched the social consequences of such an activity (Mesch, 2008; Wolak, et al., 2003). It has also been suggested that excessive use of the Internet by youth exacerbates the anti-social behaviours investigated by these studies (Gennaro & Dutton, 2007). Mesch (2008) explored social

characteristics of frequent Israeli adolescent (13 – 18 years of age) consumers by assessing the difference in the social development between Internet users and non-users. Internet users demonstrated lower self-control resulting from a low quality of social bonding (i.e., less commitment to their families, fewer pro-social attitudes and lower attachment to school than their peers who did not use the Internet). Finally, results from an unpublished thesis demonstrated that potentially problematic attitudes and behaviours regarding amount of time online had a significant association with psychosocial adjustment (Windham, 2008).

SECTION 6

REVIEW OF AUSTRALIAN AND INTERNATIONAL LITERATURE ON BREACHES OF PRIVACY, IDENTITY THEFT, AND ONLINE SECURITY

Summary section

Privacy

- Over 92% of Australian young people feel that privacy is very important.
- More than 40% of Australian young people have had pictures posted online without their permission.
- Many young people share private information online due to peer pressure.

Identity theft

- Approximately 3% of Australians over the age of 15 years were victims of identity fraud and theft in 2007 alone.

6.1 Overview

Breaches of privacy, identity theft and online security are issues, which have emerged as greater numbers of youth interact on the Internet. With the Internet acting, in effect, as an extension of the social world of young people, particularly those who utilise SNS to establish and conduct relationships often on a daily basis. Linked with increased Internet use are the increased risks associated with the disclosure and solicitation of personal information, which, once made available on the Internet, can become freely

available to all other users. Research in this area is in its infancy as early attempts are made to understand the factors associated with young people's use of technology and the associated breaches of privacy, identity theft and online security. In addition, early attempts are being made to understand the associated impact that education programs, parental and environmental influences have on the choices young people make in relation to their personal information. Importantly, issues of privacy retention have been addressed in the sections in this report describing cyber-bullying as well as cyber-stalking, grooming and sexual solicitation and will not, for the sake of brevity, be repeated in this section. What follows is a review of the literature and major government reports (Australian and international) related to the issues surrounding breaches of privacy and identity theft.

6.2 Breaches of Privacy

The Internet can be an attractive environment for children and adolescents (as well as adults), but may facilitate an individual's privacy being compromised (Berson & Berson, 2006a; Descy, 2006; Youn, 2008b). An unpublished report[25] prepared by the United Nations Youth Association South Australian Division, Flinders Law Students Association, and the Adelaide University Law Students' Society presented survey data describing the attitudes of young people to privacy issues. Although little is known about the demographic information of those who participated, the majority were aged 15 – 25

[25] This report was a joint submission to the Australia Law Reform Commission report on privacy in Australia (2008).

(77.8%), resided in Adelaide (73.0%) and were tertiary students enrolled at Flinders University (64.3%). Most respondents considered privacy to be important (38.1%) or very important (54.4%) with almost all considering it to be a right of all humans (95.5%). Although there are a number of limitations with the data presented in this survey, it is noteworthy that 67% of those who responded felt that their privacy had been breached at some time. The specific privacy breaches were not addressed although 40.6% reported that photographs or videos that identified them were posted online without their permission. The majority (29.1%) of those who did something in response reported complaining to the individual, body or organisation that made the breach while 9% of people did nothing. Of interest, 77.6% of those who completed the survey considered technology a strong (26.2%) or significant (51.4%) threat to their privacy.

An interesting issue raised and addressed in this report relates to the publication of personal information on SNS, which may violate the privacy of others through comments, photographs and videos published without consent especially in those cases where people are identified without their consent (Australian Law Reform Commission, 2008). De Souza and Dick (2008), in a paper addressing Australian children's information disclosure on MySpace, reported that 25.9% of teenagers visited the social networking site at least once a day and that most of those children did not believe that their information was safe on the site. In addition, participants revealed that they tend to reveal personal information in response to peer pressure.

There are many reasons why young people do not feel that their personal information is safe on SNS. For example, they may be aware of how easy it can be to obtain the personal information of another, which would affect their attitudes concerning the security of their own information. Further, the limitations (and lack thereof) of private information on SNS may be unclear to some users. Consistent with this, it has been demonstrated that minors younger than 14 years of age did not appear to fully understand the significance of personal information disclosure on MySpace, but all users who value their personal privacy were less likely to disclose highly personal information (De Souza & Dick, 2008). A report from the PEW Internet and American Life Project stated that 55% of American teens have online profiles (Lenhart & Madden, 2007) with about 25% of those under the age of 18 (Hinduja & Patchin, 2008b). Further, evidence from the National Cyber Security Alliance (n.d., cited in Model Criminal Law Officers' Committee, 2008) demonstrated that 74% of SNS users reveal personal information, such as e-mail address, name and birthday.

Online social networking has advantages for young people such as being a forum for self expression, discussing difficult matters without a face to face confrontation, finding like-minded others, new experiences, and having fun (Brennan, 2006; Lenhart & Madden, 2007). It has been suggested that some of these positive aspects (e.g., being able to discuss difficult matters without a face-to-face interaction; sense of privacy) increase the likelihood of sharing personal and private information (Berson & Berson, 2006b; Brennan, 2006; Huffaker, 2006). Information that would be exchanged gradually in a face-to-face environment is often posted online to many 'friends' at a time (Lenhart & Madden, 2007).

Once this information is posted online, is becomes public, and may be used to piece together details of the person and impinge on their right to privacy. Consistent with this, Gross and Acquisiti (2005) argue that the personal information that children and adolescents make available on SNS can be used to determine the social security number of the child, and so provide an avenue for loss of privacy as well as identity theft (Gross & Acquisiti, 2005; Wales, 2003).

Several studies have attempted to understand the factors associated with children's disclosure of personal information so that interventions aimed at protecting the privacy of children online can be developed. These studies discuss the use of technical and behavioural protection[26] such as filters, location of computers, self regulation of online industries, school-based education, knowledge, attitudes, behaviours of young people, and parental influence as being important in regulating privacy protection when online (Hinduja & Patchin, 2008b; Moscardelli & Divine, 2007; Rosen, Cheever, & Carrier, 2008; Williams & Merten, 2008; Youn, 2008a).

Finally, a report by the Office of the Privacy Commissioner (OPC) indicated that Australian youth are more likely to provide personal details to receive a reward or discount, with 18 – 24 year olds being the group most at risk, than older Australians (2007). Among this group the trend within Australia evidences a reduction of disclosure for a discount down from 54% to 39% since 2004, however 18% of 18 – 24 year olds report they would still provide personal information for a prize (Office of the Privacy Commissioner, 2007).

[26] Much of these technical and behavioural measures will be discussed in section 8.

Further, the OPC survey reported concern about providing personal information over the Internet with a four-fold increase in the number of Australian young people reporting they were 'more or as concerned' about providing information over the internet that they were two years ago (OPC, 2007). Interestingly, 58% of young people respondents aged 18 – 24 years also reported they were more likely to provide false information when online[27] to protect their privacy.

In recent years legislation has been developed in various countries to address privacy issues for minors. This, in turn, has led to an enhanced focus on the impact of online privacy of children which resulted in an increased number of websites with a privacy policy compliant with the Children's Online Privacy Protection Act (COPPA; which addresses the collection, use, and storage of personal information of children under the age of 13 when provided to commercial web sites and other online services), which was both prominent on the website and easily accessible (Center for Media Education, 2001; US Federal Trade Commission, 1998; 2002). Despite the availability of privacy policies on websites commonly used by minors, Turow (2001) demonstrated that university students had difficulty understanding the privacy policies on children's websites because they were too wordy or vague, and the language was too complex to absorb in a short time. Hence, if university students have difficulty deciphering the privacy policy it is unlikely that minors will have a full understanding of their privacy rights when using a particular SNS.

[27] Note: Providing incorrect information was a more viable solution rather than not going online.

Several issues are raised by the suggestion that minors are presented with privacy policies that are, for the most part, beyond their comprehension. For example, the employment of sophisticated methods of data collection and solicitation utilised by children's websites can pave the way for a breach of privacy. Marketing approaches include online techniques such as quizzes, registration forms for clubs, competition entry forms, coupons, digital postcards, loyalty programs, catalogues and the like, as well as offering rewards such as free phone calls or cash, for obtaining such information (Berson & Berson, 2006a; Cai & Gantz, 2000; Lewandowski, 2003; Lwin, et al., 2008; Moscardelli & Divine, 2007). These approaches are based on the apparent inability of children and adolescents to comprehend the value of their private information coupled with the attraction of a reward. However, evidence from the promotion of cigarettes on the Internet suggests that strategies that involve competitions, quizzes and rewards are tactics that are effective with young adults as well as teenagers (e.g., Freeman & Chapman, 2009).

Once personal information has been provided online, there is the potential that it will be disseminated to other groups or merged into a personal profile, and that the subsequent use of that information may constitute a privacy breach (Berson & Berson, 2006a; Lewandowski, 2003; Lwin, et al., 2008). Parental involvement and mediation in online activities are cited as important in helping children understand and navigate their possibly risky Internet experiences (Cai & Gantz, 2000; Lwin, et al., 2008). A PEW Internet & American Life Project study states that 85% of parents of teens, who use the Internet regularly have rules about the types of personal information they can put on the Internet (Lenhart & Madden, 2007). Finally, there are some interesting trends in relation to

who is using strategies to protect their privacy online. For example, female adolescents are more likely than males to undertake privacy protecting behaviours (Lenhart & Madden, 2007; Moscardelli & Divine, 2007). Further, teens appear to be restricting access to their information using behavioural methods, such as providing inaccurate or incomplete information (Lenhart & Madden, 2007; Moscardelli & Divine, 2007), whereas younger children are more reliant on technical means (i.e., Internet filtering software) as well as parental monitoring to provide protection (Lenhart& Madden, 2007; Rosen, et al., 2008).

6.3 Identity Theft

Identity theft is a phenomenon generally considered to be unknown prior to 1995 (AUSTRAC, 2004). Although the exact reason is unknown, the emergence of this type of fraud may be linked to the ability to discover information using the Internet – WebCrawler, the first full-text Internet search engine went live in 1994 – reducing the reliance on non-technical means (i.e., to steal credit cards from wallets or mailboxes). Several studies have observed that the incidence, extent and cost of identity crime are increasing in a number of countries, including Australia. This has been attributed to numerous factors, including:

- The rise in high-speed information flows;
- Globalisation;

- The increased use of remote communications rather than traditional face-to-face interactions;
- The ease with which documents can be forged using high-tech methods, and
- The widespread collection and dissemination of data about individuals by private sector and other organisations, which provides opportunities for easier access to personal information.

A great amount of information on individuals and other entities is readily available and accessible on the Internet. Recent survey data presented by the online security company Unisys indicated that many Australians are not vigilant in protecting the privacy of their online personal information. However, 62% of the Australians who participated in the survey reported being very or extremely concerned about unauthorised access to or misuse this information. There are several ways in which online identity and personal information can be accessed. The most well known is by sending fake emails (often called *phishing*) to entice people to enter personal information (usually bank account information) into a fake website (set up to look like the real website). Other techniques include using key logging software as well as stealing personal information from computer databases held by government organisations and financial institutions (Model Criminal Law Officers' Committee, 2008).

The Australian Bureau of Statistics (2008) estimated that approximately 3% of Australians over the age of 15 were victims of identity fraud and theft in 2007 alone.

Interestingly, the rate of identity fraud and theft was stable from age 15 to 55+ years of age (Figure 6.3.1).

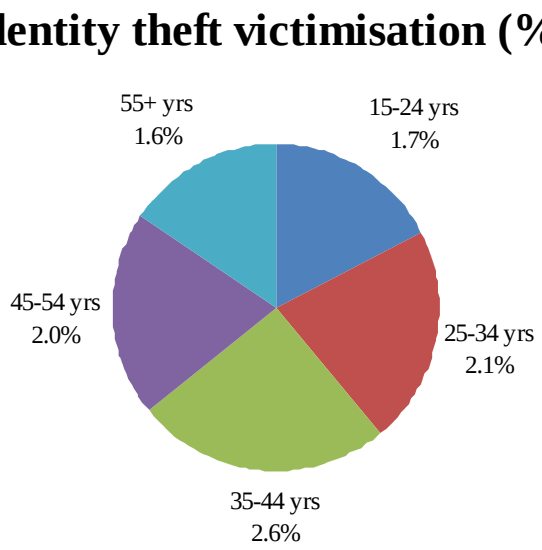

Figure 6.3.1 Percentage of Australian who were victims of identity fraud and theft in 20**0**7[28]

In contrast, a recent report by the Australian Institute of Criminology highlighted age as a factor in identity-related crimes (AIC, 2008). The AIC reported that 9% of participants (n > 1,500) reported being a victim of identity fraud and theft while a further

[28] Adapted from Australian Bureau of Statistics (2008). *Personal fraud Australia.* ABS cat. No. 4528.0. Available at www.abs.gov.au/ausstats/abs@.nsf/cat/4528.0

17% personally knew a victim. Those aged 34 – 49 years were most likely to have been a victim (12%), while those aged under 24 years were the least likely (2%; Figure 6.3.2).

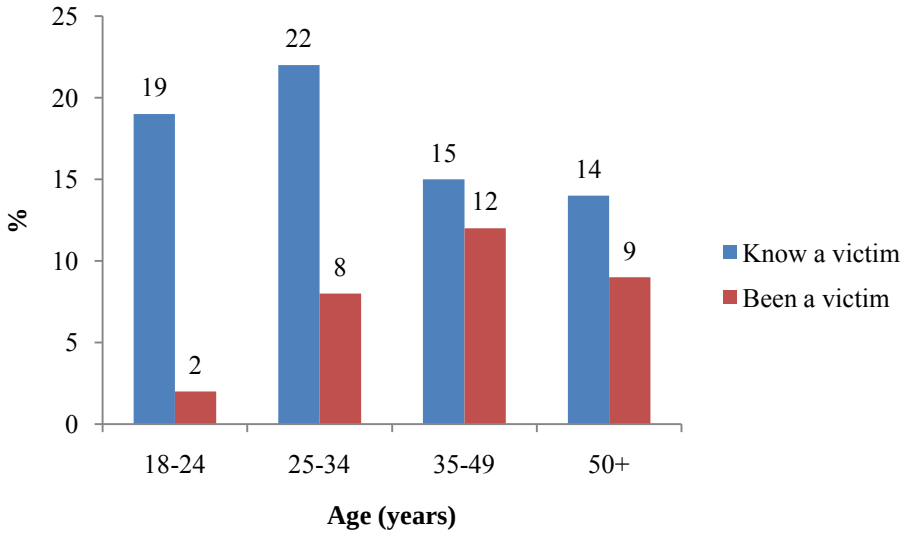

Figure 6.3.2 Rate of identity fraud and theft crimes by age in Australia in 2007[29]

Further, the AIC reported that participants with an annual household income greater than $100,000 were most likely both to have been a victim themselves (11%), and to have known a victim (21%), with the likelihood of knowing a victim increasing with household income up to $100,000. Overall, the level of community concern regarding identity fraud and theft incidents was high, with the majority of respondents (60%) saying they were concerned or very concerned. Finally, 45% of those who responded to the survey

[29] Adapted from Wallis Consulting Group (2007).

considered that using the Internet and online banking or purchasing were the most likely ways in which IFT would occur.

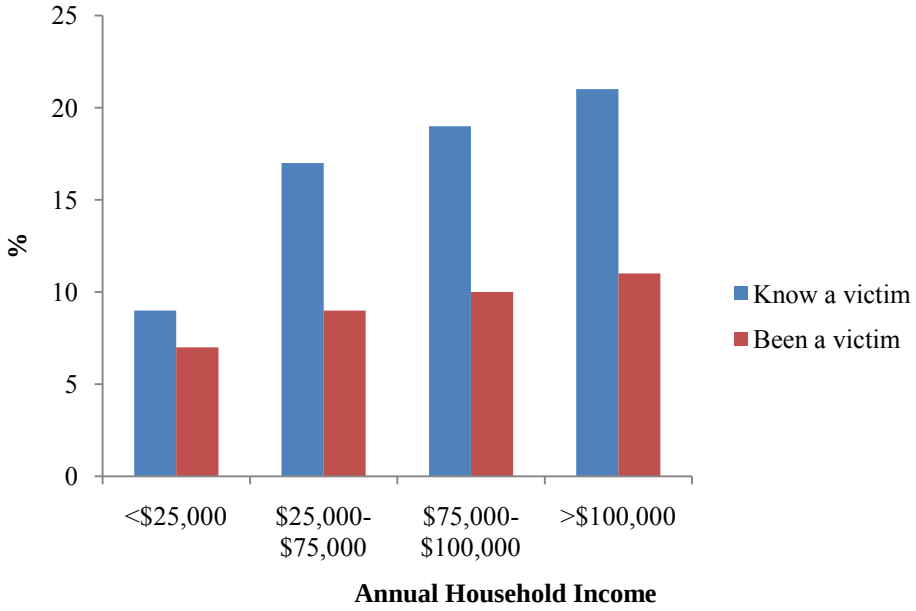

Figure 6.3.3 Rate of identity fraud and theft crimes by annual household income in Australia in 2007[30]

The annual cost of identity fraud is very difficult to estimate. For example, in a report on identity fraud to the Australian Attorney-General's Department, Main and Robson (2001) constructed an equation to estimate the annual cost of identity-related fraud based on the cost of crime estimated from annual Gross Domestic Profit (GDP). The authors reasoned that if estimates of fraud were used to "represent the best measure of financial

[30] Adapted from Wallis Consulting Group (2007).

crime currently available, and it is agreed that most financial crime is identity related, then it (the figure of 28%[31]) can be used to derive an estimate of the cost of identity-related fraud" (p. 4).

The equation is:

*Cost of identity fraud = Australian GDP ($billion) * Cost of Crime Estimated (%)*

** Proportion of Crime which is Identity-related (%).*

Using 1996 figures, the Main and Robson equation produced in an estimate for the cost of identity-related fraud of in excess of $4 billion per annum. Given that the GDP for 2008 was $825 billion, crime costs were an estimated 4.1% of GDP and fraud comprised 40% of the annual cost of crime, a recent estimate of the cost of identity-related fraud approximates $13.5 billion. This is in stark contrast to an estimate for 2001 – 2002 of $1.1 billion proposed in a 2003 report generated by the Securities Industry Research Centre of Asia–Pacific (Cuganesan & Lacey, 2003). Although neither figure can be confirmed, the latter is more in line with estimates from countries other than the US. For example in the US, there were 8 million victims of identity fraud in 2007 resulting in $49.3 billion dollars worth of loss (Javelin Strategy, 2007). Similarly, the cost associated with identity fraud in the UK from 2004 – 2007 totalled GBP£1.7 billion (an estimated AUD$3.5 billion; CIFAS, 2004). Finally, identity fraud in Canada during 2002 totalled CAN$2.5 billion (AUD $2.8 billion; Public Safety and Emergency Preparedness Canada, 2002).

[31] The 28% estimate was based on 1996 figures. The Australian Institute of Criminology (report available from http://www.aic.gov.au/publications/cfi/cfi169.html) reported that fraud and related offences comprised 40% of the cost of all crime (the next highest being 10% for burglary offences).

Interestingly, a US based survey reported that only a small percentage of identity fraud occurred over the Internet, with most cases still involving traditional offline channels. In contrast, a Australian-based study revealed that Internet-related activities were considered the most common reason why identity theft occurred (followed by losing or having identification card, wallet, passport or some other type of official document of verification stolen and using or losing sight of a credit card) demonstrating that the public perception regarding the risks associated with the Internet does not match with the actual statistics – offline behaviours are more prevalent. Further, the time spent by victims in resolving identity fraud cases increased from 33 hours in 2003 to 40 hours in 2006 suggesting that the theft was more complex and difficult to resolve. Although the reason for this increase in resolution time is unclear, evidence from the UK indicates that deceased fraud (i.e., stealing the identity of deceased persons) has become more popular in recent times and, in 2006, was costing approximately GBP£250 million each year (CIFAS, 2004[32]). It should also be noted that it is possible that the seven-hour difference in resolution time between 2003 and 2006 is the result of a sampling bias and does not represent a statistically "meaningful" difference.

In most international literature, identity theft is mentioned in passing with the focus on privacy issues. There is little specific data relating to identity theft and young people, however a large body of work is available on identity theft in general. With each personal disclosure; however, the young person loses more control over their personally identifying

[32] CIFAS, Decreased Frauds – Research results – December, 2004. Available at: www.cifas.org.uk/reports_deceased_fraud.asp

information, which can then be used for fraudulent financial gain (Lewandowski, 2003). In 2006, the US Federal Trade Commission recorded 1,498 reports of identity theft from young persons up to 18 years of age, equating to 2% of total identity thefts reported in that year (Youn, 2008a). Often the identity theft is not discovered until the young person is older, with the main ways being:

- Denial of credit or loans, such as college tuition loans;
- Rejection of new bank account request;
- Refusal of a drivers licence;
- Rejection of connection requests by phone or utility companies;
- Receipt of bills, summons and collection notices;
- Serving of an arrest warrant, and
- Rejection of employment applications for no apparent reason (Identity Theft Resource Centre, 2007).

SECTION 7

DRIFTING BEHAVIOURS

Summary section

- No studies were identified that specifically addressed drifting behaviours.
- Most outcomes studies are not designed to draw conclusions about the nature (or existence) of drifting.
- It is suggested that there are many external and internal factors that are likely to underlie seeking out increasingly explicit or paraphilic content. Further, progressing to viewing more explicit or illegal content would be expected in a minority of cases – cases which are not likely to be characteristic of or consistent with the average Internet user.

7.1 Overview

This report presents a review of the Australian and international research literature on risks to cyber-safety. One of the risks outlined in the tender document (DCON/08/93) referred to "drifting" behaviours. As noted in the tender document, drifting is a term that has been used to refer to the viewing of inappropriate images leading to unhealthy curiosity about and tolerance for images of greater concern (e.g., child abuse). Based on our review of the literature, it appears that drifting is conceptually different to the other risks mentioned. Therefore, this section will address the concept of drifting and present a heuristic framework, which can be used to conceptualise the impact of exposure to positive

and negative material via the Internet as well as the role of social and psychological influences. Given the dearth of literature in this area, this section differs from previous sections in that little research literature is reviewed. Rather, this section presents a more theoretical discussion of the concept of drifting behaviours.

> "Certainly, users have different social and psychological needs that motivate their choices. These needs compel people to seek information or enter into communication, and they have expectations about what they will gain from such activity. Owing to these motives and expectations people select particular media channels, sources and content. Different people will use the same channels, sources, and content for quite diverse reasons and with contrasting expectations."
>
> *Mesch, 2009, p. 604*

7.2 Drifting behaviours

Our review of the literature did not reveal any research studies that specifically addressed "drifting" behaviours, namely, the progression from early exposure to age inappropriate content to later tolerance and curiosity for content that is of even greater concern. We speculate that the dearth of publications addressing this topic is because drifting is generally addressed as an implication of research findings related to Internet risks rather than distinct issue separate from the others reviewed in this report. In addition,

not all of the risks described in previous sections (e.g., grooming, cyber-stalking) have been examined in longitudinal research studies making it impossible to explicitly describe the long-term direct effects of these early experiences.

Further, research on the long-term outcomes of early exposure has not shed much light on the nature of drifting (at least in terms of how the concept is generally described). For example, much has been written about the short- and long-term effects of exposure to pornography. Evidence for "drifting" in relation to exposure to pornography would be found if there were differences in the type or amount of content, consumed by those who were exposed at a young age compared to those who were not exposed. Some have reported that adolescents exposed to sexually explicit websites were more likely to report having multiple lifetime sexual partners, having more than one sexual partner in the last 3 months, and having engaged in anal sex when compared to those not exposed (Braun-Courville & Rojas, in press). Furthermore, early exposure to pornography has been associated with sexual permissiveness, sexual activity at a younger age, acceptance of negative attitudes towards women and sexual aggression (Barak, Fisher, Belfry, & Lashambe, 1999; Greenfield, 2004; Lo & Wei, 2002; Malamuth & Impett, 2001). However, these differences in attitudes and practices are more accurately considered outcomes and do not necessarily provide support for the argument that exposure results in an increased interest or desire to view material considered increasingly inappropriate.

As was discussed in the relevant sections in the report, there is evidence to indicate that the effects of early exposure to illegal or inappropriate content, or to certain types of

negative social contact (e.g., cyber-stalking), have been associated with negative consequences. However, there is a notable lack of evidence demonstrating the relationship between long-term effects of exposure and increasingly deviant interests. Therefore, it is not feasible to definitely comment on, for example, the level of exposure that may result in unhealthy curiosity and interest in images considered to be more extreme (e.g., child pornography). Therefore, while there appears to be some evidence that early exposure to pornography is associated with varied sexual practices, there is no research evidence that early exposure to pornography is associated with intentional seeking out child pornography or images of an especially paraphilic nature (e.g., coprophilia or bestiality).

Further, there is evidence that prolonged exposure to violent media can result in emotional desensitization (i.e., a numbing or blunting of emotional reactions to events which would typically illicit a strong response) as well as cognitive desensitization (i.e., evident when the belief that violence is uncommon becomes the belief that violence is mundane and inevitable). For example, Molitor and Hirsch (1994) demonstrated that viewing violent content resulted in increased tolerance for violent behaviour. More recently, Funk, Baldacci, Pasold, and Baumgardner (2004) reported that exposure to violent media was associated with lower empathy and higher pro-violence attitudes; results which they argued could be interpreted as indicative of desensitization. So, while there is an indication that exposure to certain types of risks has been associated with the attenuation of a cognitive or emotional response to a stimulus, we were unable to locate any evidence suggesting that the resultant attenuation or modification in a person's attitude or belief was associated with an interest in more deviant stimuli. It is feasible that those who actively

seek out more deviant content represent a discrete sub-group of users. Consistently, it has recently been suggested that adolescents who use the Internet for pornography consumption "may represent a different and particular non-normative group among the adolescent population" (Mesch, 2009, p. 615). This is a very important finding as it suggests the existence of pre-existing individual factors (e.g., interest) that may underlie the active seeking of certain types of content online, such as pornography.

After an extensive review of the literature, we were unable to locate any articles or reports that explicitly discussed the concept of drifting. Furthermore, there does not appear to be a comprehensive understanding of the relationship between exposure and long-term effects in relation to actively seeking out more deviant content. In various sections of this review, we described studies that report very high rates of exposure to certain cyber-safety risks in young people (e.g., up to 85% in the case of accidental exposure to online pornography). Despite these high prevalence rates, we were unable to locate any sound evidence demonstrating that the majority of these young people develop an unhealthy interest in more deviant images or content in adulthood. Support for the hypothesis that there exists a sub-group of Internet users who have pre-existing paraphilic interests is evidenced by relatively small number of offenders apprehended on child pornography charges (Australian Institute of Criminology, 2009). That is, of all those individuals who viewed (intentionally or otherwise) pornography, it appears to be the case that relatively few view child pornography. Furthermore, as Mesch (2009) suggested, it is likely that the motivations of those young people who use the Internet for pornography consumption differ from those young people who have viewed pornography online accidentally.

Therefore, it is possible that those young people who deliberately accessed pornography online as part of a diverse pattern of accessing and downloading information (i.e., downloading pornography was not the *sole* reason for using the Internet) differ from those young people who primarily use the Internet for pornography consumption. In essence, it may be that those who are most at risk for "drifting" represent a specific subgroup of Internet users, but relatively little is known about them.

Figure 7.2.1 presents a heuristic that can be used when considering the effects of young people's exposure to harmful content and contact on the Internet. Clearly, there is positive and negative content available on the Internet[33]. The extent of influence from positive or negative content could be argued to be a function of both time spent online (i.e., number of hours) and exposure (i.e., the nature of the content that is viewed). Therefore, the more time spent online the greater the potential for exposure to age inappropriate content. It is important to note that time spent online and exposure are factors that would be expected to operate through environmental and social factors (i.e., time online and content exposure would vary according to accessibility and peer group or friend interests or influence). For example, low levels of emotional bonding with parents or caregivers are associated intentional viewing of pornographic content online (Ybarra & Mitchell, 2005). Further, some individual factors (e.g., age, gender) are likely to influence the effects of exposure to both positive and negative content. However, for most of the issues addressed

[33] We acknowledge that the descriptors "positive" and "negative" may mean different things to different people.

in this review of evidence, the specific nature of those factors is unclear as most are identified ad hoc.

In the heuristic presented below, it is suggested that the effects of positive and negative content and contact essentially mirror each other. It is important to note that we are not suggesting that the long-term effects of exposure are simplistic and discrete; it is presented in this format solely for illustration. Of course, how online (and offline) information is processed in relation to past experiences, internal attitudes and expectations as well as external feedback would be expected to have a significant influence on the drifting process. However, the overall approach outlined in the heuristic is that exposure to age-inappropriate content potentially results in a range of negative outcomes. For example, exposure to positive content would be expected to result in positive knowledge acquisition, which would further enhance and promote positive skill sets (i.e., protecting privacy online and not engaging in "risky" online behaviours). This would increase the likelihood of positive interactions, which would in turn, promote the development of positive social interaction skills, resulting in healthy development. It is likely that these factors are inter-related such that healthy development would increase the likelihood of seeking out positive content and positive interactions.

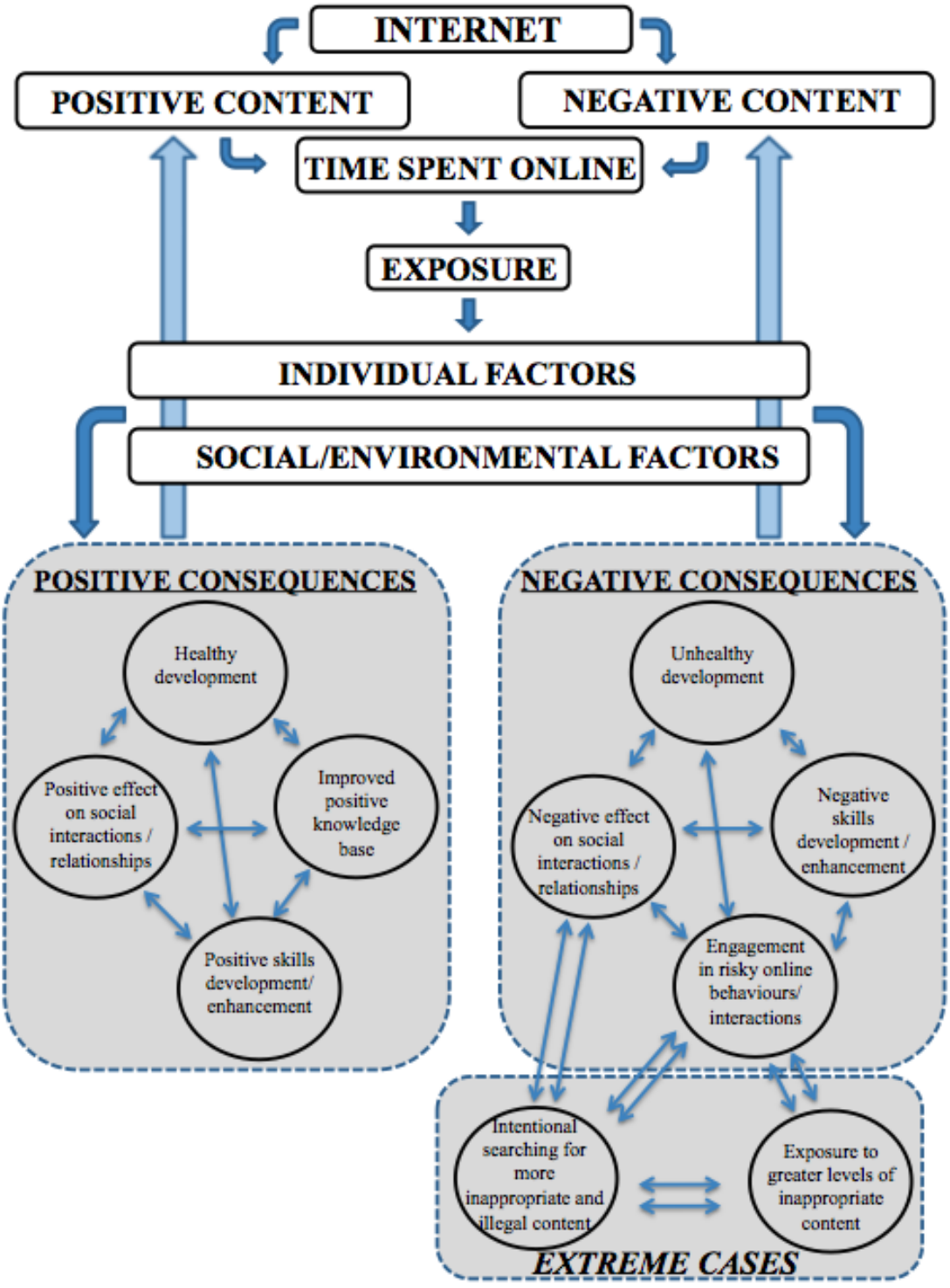

Figure 7.2.1 Effects of exposure to positive and negative Internet content and contact

In relation to exposure to negative content and contact, the reverse would be expected. For example, viewing sexually explicit images has been associated with the development of negative attitudes about sex. Frequenting websites and related online areas (e.g., chatrooms, etc.) that contain age-inappropriate content may increase the potential for engaging in negative and risky online behaviours (through the development of negative attitudes). In contrast to exposure to positive content, this would be expected to have a negative effect on social interactions ultimately leading to unhealthy development. It should be noted that exposure to negative and harmful content and contact would likely increase the potential of developing an unhealthy or more deviant interest in harmful content as well as a greater potential for harmful contacts. However, this is not to suggest that developing and engaging in increasingly inappropriate and unhealthy behaviours is based on exposure alone. Here again, the individual and socio-environmental factors have a significant role to play in the intentional consumption of more inappropriate content.

Importantly, in relation to the heuristic below, drifting would be anticipated to occur in a relatively small number of cases. These are the cases where, as Mesch (2009) suggested, the Internet is being used for a specific and deviant purpose (e.g., to view pornography). Coupled with pre-existing interests, these individuals actively seek out more deviant content or engage in increasingly risky behaviours. Given the paucity of research on this topic, it is difficult to comment on whether this is a phenomenon unique to or exacerbated by the availability of content online. Although, as previously noted, there is evidence that exposure to age-inappropriate content has been associated with negative attitudes and behaviours; the process of escalation to increasingly deviant content is

unknown. However, it is likely that consumption of more deviant content can have a negative impact on social relationships.

Finally, an important component of the heuristic is the influence that exposure to positive and negative content has on seeking out additional positive or negative online content. We suggest that the manner in which exposure to positive and negative online content is processed by the individual (internally and in the context of social or environmental factors) can affect the likelihood of future exposure to positive or negative content. For example, if an individual exposed to negative online content has a strong negative reaction (i.e., is disgusted by what they saw), they might be less likely to view similar content in the future. Therefore, exposure to positive or negative online content is not likely to result in only positive or negative outcome. It is more likely that, for an individual user of the Internet, there are positive and negative consequences associated with exposure to positive and negative content. In this way, it would be more likely that an individual user intentionally accesses and is exposed to subsequent negative content if their reaction to the initial content was not overwhelmingly negative. However, it is important to note that this is speculative and, to our knowledge, has not been addressed in any research study to date.

SECTION 8

REVIEW OF AUSTRALIAN AND INTERNATIONAL LITERATURE ON TECHNICAL AND BEHAVIOURAL MEASURES USED BY CHILDREN, PARENTS AND TEACHERS TO MITIGATE CYBER-SAFETY RISKS

Section Summary

- Similar levels of Internet filter use in households around the world:
  - 20 – 35% of households in Australia use Internet filters,
  - 33% of households in US use Internet filters, and
  - 28% of households in Europe use Internet filters.
- Trust is the most common reason Australian parents do not use Internet filters.
- Discrepancy between parents and children in terms of the existence of household rules governing Internet usage.
- Many education-based programs address cyber-bullying but **very few** are evidence-based.
- Technological advances in the area of text analysis have shown promise in enhancing safety from cyber-stalking/grooming encounters.

8.1 Overview

There are many technical and behavioural measures that have been employed to mitigate the risks associated with online activity. Other reviews (e.g., the Australian Communications and Media Authority [ACMA] report published in February 2008,

provides a comprehensive overview of Internet filtering technologies and other measures for promoting online safety) have focused on the development and mechanisms of the commonly used technical measures developed to enhance cyber-safety. These measures will be briefly discussed in this section, however, there is very limited information regarding the efficacy of most of the technical measures available (e.g., biometrics).

Most of the measures employed by students, parents, teachers and schools fall into two main categories: filtering and education. Given the lack of information regarding the efficacy of other technical measures in reducing cyber-safety risks, we will present only the available research literature related to filtering and education approaches. A brief overview on text analysis and additional approaches will be presented. It should be noted that the tender document (DCON/08/93) requested that measures, which parents, students, teachers, and the general community can and might use, be reviewed. Given that the potential resources that these groups *might* use is potentially limitless in that it could refer to resources that are currently under development and not actually available to the public, we deliberately interpreted "might" to refer to those resources that are already or almost available to the various user groups.

In relation to the latter, we suggest that there is little to be gained by a discussion of those resources that are not currently available. Given that research on cyber-safety is rapidly increasing, it is likely that resources will be modified as more is learned about cyber-safety risks. Currently, there is limited information about the effectiveness of a number of measures used to mitigate cyber-safety risks. For example, many of the cyber-

safety educational programs have yet to be empirically tested. As a direct comparison between measures to mitigate cyber-safety risks is unlikely to reveal important and useful information, we will present our review of measures used to mitigate cyber-safety risks separately. The technical and behavioural measures that have primarily been employed by students, parents, teachers and schools to mitigate cyber-safety risks will be presented in four categories:

1. Filtering, monitoring and auditing measures;
2. Educational approaches;
3. Text analysis, and
4. Other.

8.2 Filtering, monitoring, and auditing measures

Internet filtering software emerged in the 1990s as concerns about access to inappropriate material on the Internet grew. This report is not intended to provide an overview of the technology of Internet filters[34]. Rather, our focus is on the relationship between filtering technology and risks associated with the user. Furthermore, we focus on the use and effectiveness of filters from the perspective of the end user (i.e., the person who

[34] As of the preparation of this report, ACMA had produced two reports addressing developments in Internet filtering technologies which provide a thorough and extensive overview of filtering technology. We suggest that it is more useful for this report to focus on the use (and non-use) of filters as it relates to cyber-safety risks.

is potentially at risk) as opposed to the type of filter (e.g., Internet Service Provider [ISP] or user level). Given the focus of this report, we believe it is more useful to examine the reasons why families do or do not use filter technology. However, it should be noted that ISPs in many European countries use filter technology to specifically block child pornography (Collins, Love, Landfeldt, & Coroneos, 2008).

Overall, there are two basic strategies involved in identifying material to be filtered:

1. Index filtering – this approach essentially places content on a "good" or "bad" list based on if they are listed on a pre-determined index. This approach is often based on a whitelist or a blacklist. Whitelist-based filtering permits user access only to those websites that appear on a preapproved list. This strategy is primarily used to filter content for young children. Conversely, blacklists permits access to all Internet content with the exception of those that are classified as inappropriate or illegal. An additional strategy uses category indexes where content is classified according to subject categories (e.g., gambling, pornography, social networking).
2. Analysis filtering – once content is examined, it is found to meet an established set of criteria that are used to determine the acceptability of content. Among the methods that are used in this approach are key word filtering, profile filtering and image analysis filtering. Key word filtering involves looking for words that might indicate that the site contains content that has been classified as inappropriate. Profile filtering involves categorising content by comparing its characteristics (e.g., format or word usage) to other content previously classified as inappropriate.

Finally, image analysis filtering involves the examination of images for large amounts of skin tone, which is used to determine if the image involves nudity.

> "At present, most filters deal with communications risks by completely blocking access, rather than filtering the content of applications that permit high levels of interactivity, such as social networking sites, IM and chat."
>
> *ACMA, 2008, p. 30*

The filtering strategies outlined above essentially attempt to prevent a user from accessing material according to a pre-determined set of criteria. Monitoring and auditing approaches are designed to provide a record documenting activity after it occurs. Recently, in Australia, there has been a great deal of discussion focused on freedom of speech and censorship issues in relation to the use of ISP filters. It should be noted that this review will not address censorship or freedom of speech issues in this section on Internet filters. As noted above, the focus of this report is on cyber-safety risks and strategies to mitigate those specific risks. As with other sections in this review, we will limit our discussion to the scientific and quality non-scientific literature regarding filtering, monitoring and auditing measures.

There are a number of different types of software filtering tools available and a review of each is beyond the scope of this report. However, filters are available to do the following (GetNetWise, 2008):

1. **Filter sexually explicit graphic descriptions or images:** These tools block most sexually explicit material on the Internet. In addition, this category can be expanded to include other types of inappropriate content such as violent, racist or drug-related content. For example, the Australian Library and Information Association (2007) reported that Internet filters were used to block the following: pornography, violence, hate websites, web-based e-mail, commercial content, gambling websites, illegal content, online games and instant messaging.

2. **Monitor online activities:** These tools allow parents and caregivers the ability to monitor online activities through a variety of methods. These tools can also be used to inform parents and caregivers (and schools) about online activity by recording the addresses of websites visited.

3. **Limit the amount of time spent online:** These tools can limit the amount of time spent online. Some tools allow parents to block out times of the day when the child can or cannot go online.

4. **Block personal information from being posted or emailed:** These tools prevent a child from giving strangers their personal information (e.g., name, home address, etc.) while they are online.

5. **Browsers for kids:** These are Web browsers that serve as a gateway between your computer and the Internet. Browsers for kids generally filter sexual or otherwise inappropriate words or images. They are often designed to be easier for kids to use.

> One recent example of this is the recently developed and launched website, Kideo Player (2009). It consists of a selection of randomly presented short clip videos that have been selected from the video clips available on YouTube. The website authors report that Kideo Player is a way of accessing the educational and age-appropriate content on YouTube and, as each video is actually viewed and chosen by the website authors themselves (as opposed to being chosen by keyword search), the site is safe even for young children. The website is designed to be simple, videos are accessed by pressing the spacebar and are generated randomly so if a child does not like the video showing they can hit the spacebar to move onto the next video.

The ISTTF report (2008, Appendix D, p. 11) suggested that there are limitations associated with filtering technology indicating that, "filtering software can be easily circumvented or disabled by computer-savvy users, completely eliminating their effectiveness. Frequently, parents or guardians are notified in such cases, which is beneficial. In any case, parents, guardians, and other caregivers should simply be alert to the potential for circumvention."

8.3 Use of Internet filters

Despite the large number of filters available for little or no cost, it seems that the general uptake of these software safety tools is rather limited. A report prepared for the Australian Broadcasting Authority (now ACMA) demonstrated that, in 2005, filter use in Australia was relatively uncommon. For example, 35% of parents reported using software

filters with 29% using filtering software on a regular basis and 6% on an occasional basis (NetRatings, 2005). More recent Australian estimates put Internet filter usage levels considerably lower at approximately 20% (Fleming, et al., 2006). In the US, 33% of parents report using some type of filtering or blocking software - despite 84% of parents reporting being extremely concerned about exposure to sexual material on the Internet (Mitchell, et al., 2005). Furthermore, Mitchell and colleagues reported that parents were more likely to use Internet filters if they had younger children (10 – 15 years of age), had a high level of concern about exposure to sexual material on the Internet, had more extensive knowledge of their child's online activities, had low trust in their child's responsible Internet use and if their child used America Online. Reported rates across Europe range from 71% in the UK to less than 2% in Slovenia with an overall rate of 28% (see Table 8.3.1).

Table 8.3.1 *Reported rates of Internet filtering / blocking software in Europe*

	Filtering/blocking tools		
	At home (%)	At school (%)	Other (%)
All EU countries	27.6	30.8	8.0
UK	46.2	71.0	4.2
Ireland	35.2	43.4	2.8
Germany	29.8	21.5	5.0
Netherlands	28.0	31.6	0.8
Spain	25.6	14.4	4.4
France	25.4	26.6	10.2
Austria	21.8	17.7	9.5
Cyprus	20.7	20.7	0.0
Belgium	20.6	9.8	6.7
Italy	20.2	10.6	6.7
Sweden	19.9	26.5	0.9
Poland	18.8	30.0	21.3
Denmark	18.4	20.3	1.9
Greece	11.9	22.0	13.6
Czech Republic	10.1	20.7	21.8
Portugal	8.7	20.7	10.9
Estonia	7.0	11.3	10.2
Bulgaria	6.6	8.8	7.7
Slovenia	5.1	1.9	17.2

Hasebrink, Livingstone, and Haddon (2008). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London: EU Kids Online (Deliverable D3.2).

Livingstone and Helsper (2008) reported that 34% of parents indicated that the main reason Internet filters were used was to block access to pornographic websites. Among the other reasons parents gave for Internet filter use were to block junk mail (20%), chat rooms (13%), adverts (12%), instant messaging (4%) and e-mail (4%). In addition, those families with younger children, as well as those families classified as being of high socioeconomic status, reported having more general rules and regulations concerning Internet use. Parents reported rules concerning the amount of time spent online (53%), as well as using strategies

such as talking to their child about Internet use (64%), watching their child online (46%), being nearby when child is online (34%), checking which sites children visited (30%), checking e-mail accounts (17%) and sitting with their child while online (16%).

> "Parents have a preference for social over technical forms of mediation, preferring active co-use over technical restrictions, interaction restrictions, and monitoring practices."
>
> *Livingstone & Helsper, 2008, p. 596*

8.4 How effective are Internet filters?

Some have suggested that filters may not be an appropriate strategy for protecting young people from exposure to illegal and inappropriate content. For example, some have suggested (e.g., Kranich, 2004) that filters underblock some material (i.e., they do not block 100% of pornographic websites), they overblock some material (i.e., they block access to non-pornographic sexual material), or they fail to block some websites at all (e.g., English language-based filters will not block pornographic material that is written in a different language). Richardson and colleagues (Richardson, Resnick, Hansen, Derry, & Rideout, 2002) investigated the extent to which health related information was blocked using seven different filters that were intended to block pornographic material. The authors demonstrated that at the least restrictive setting, only 1.4% of health-related information

was blocked (see Figure 8.4.1). However, an additional 10% of content related to sexuality was blocked (e.g., content describing safe sex or condom use). At this level, approximately 87% of pornographic material was blocked. At moderately restrictive settings, 5% of health information and 90% of pornographic material was blocked. Finally, at the most restrictive settings, 24% of health information and 91% of pornographic material was blocked. The authors concluded "filtering software set to block pornography will not necessarily have a serious impact on access to general health information" (p. 2891).

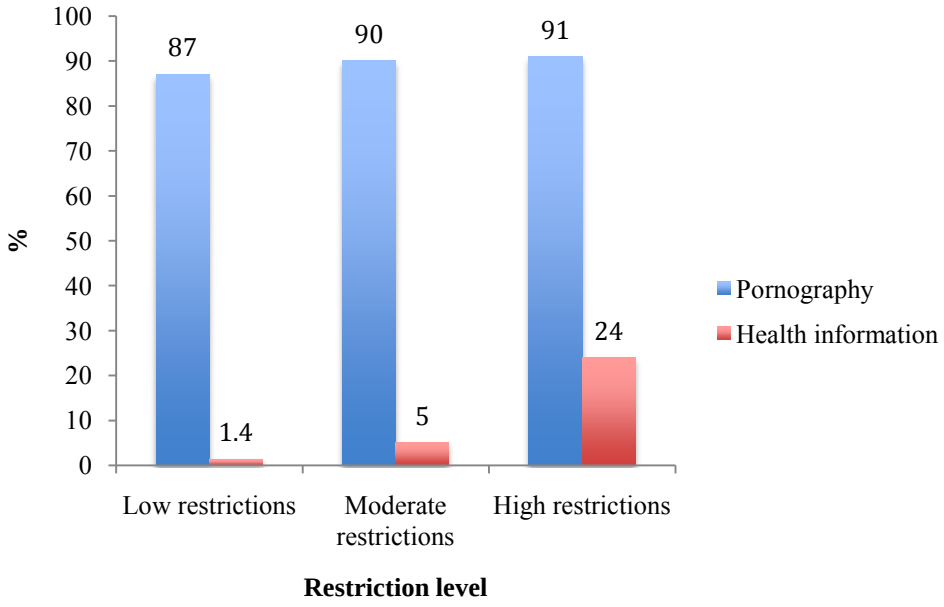

Figure 8.4.1 Percentage of pornographic and health information blocked by Internet filters

A study conducted on behalf of the COPA Commission (Hunter, 2000) investigated the effectiveness of four filters in blocking content that was classified objectionable

(nudity, violence, sex, offensive language). Hunter demonstrated that there was considerable variation in terms of how much objectionable content was not blocked compared to how much non-objectionable content was blocked by the filters. Overall, 25% of objectionable content was not blocked while 21.3% of non-objectionable content was (Figure 8.4.2).

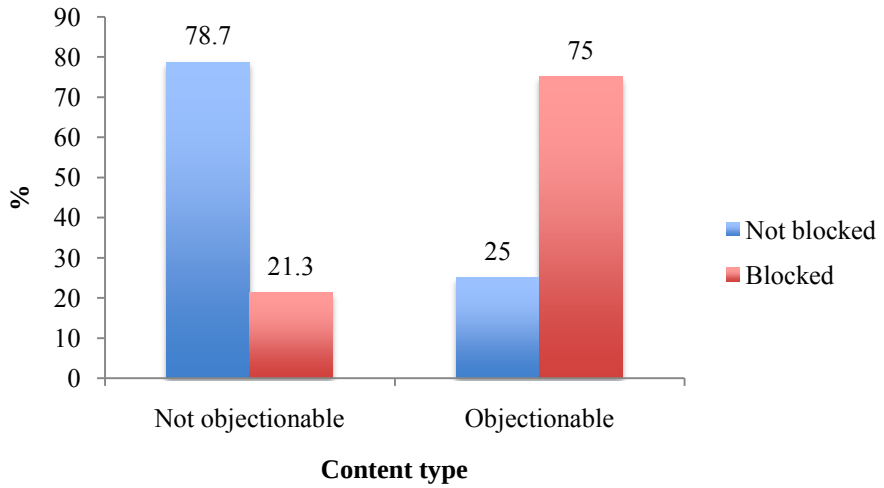

Figure 8.4.2 Effectiveness of four filters in successfully blocking content rated objectionable and non-objectionable (Hunter, 2000).

As illustrated in Table 8.4.1 below, there was considerable variation between the four filters used (CYBERsitter, Cyber Patrol, SurfWatch and Net Nanny) in relation to how

much objectionable content was blocked and how much non-objectionable content was. For example, less than 31% of objectionable content was not blocked using the CYBERsitter filter while over 83% of the same content was not blocked using the Net Nanny filter.

Table 8.4.1 *Percentage of non-objectionable and objectionable content blocked using four filters.*

Filter	Non-objectionable	Objectionable	Total
CYBERsitter			
Not blocked	85.4	30.6	75.5
Blocked	14.6	69.4	24.5
Cyber Patrol			
Not blocked	90.9	44.4	82.5
Blocked	9.1	55.6	17.5
SurfWatch			
Not blocked	92.7	55.6	86.0
Blocked	7.3	44.4	14.0
Net Nanny			
Not blocked	97.0	83.3	94.5
Blocked	3.0	16.7	5.5

Note: Adapted from Hunter (2000).

An Australian-based study demonstrated that four of the eight filters tested (8 in total) blocked 80 – 100% of pornographic content, 2 filters blocked 60 – 80%, one filter blocked 40 – 60% and one filter blocked 20 – 40% of pornographic content. Consistently, Stanley (2001) demonstrated that Internet filters block pornographic material about 80% of

the time. Although filters do work in terms of blocking access to pornographic content, they are not foolproof and need some expertise and time in order set them up properly to maximise their effectiveness. The ISTTF report (2008) suggested that there are limitations associated with filtering technology indicating, "some filtering tools address all Internet technologies, but some do not. For example, one package can restrict access to inappropriate websites but still allow unfiltered conversations to occur over instant messaging" (p. 11).

8.5 Why are Internet filters used?

Many reasons are usually given by parents as to why they do not use filtering software to protect their children online. Figure 8.5.1 below (adapted from NetRatings, 2005) illustrates the most common reasons generated by Australian parents for not using Internet filters. Clearly, half of the parents who responded to the survey indicated that they did not use Internet filtering software because they trusted their child and this was highest among parents of 12 – 13 year olds (59%). Further, the authors reported that, based on feedback from parents, "as children become teenagers direct supervision and rules become less effective and education and trust play greater roles" (p. 68). However, "other parents trusted their children, but did not believe that trust in their child alone would protect them against everything and everyone who might be on the Internet" (p. 68).

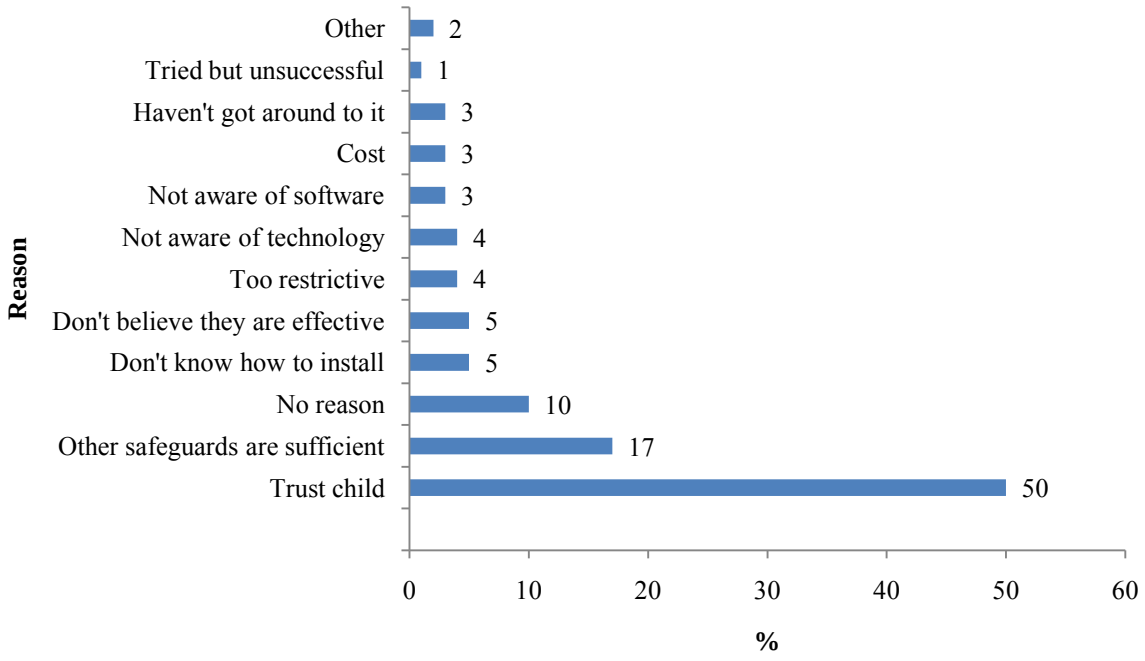

Figure 8.5.1 Reasons why Australian parents do not use Internet filtering software (NetRatings, 2005).

Data from the US revealed some interesting results about the households who were more likely to have Internet filtering software installed on the computer that youths used (Mitchell, et al., 2005). For example, the parents of younger children (10 – 15 years) were more likely to use filtering software – 36.9% of these households used Internet filters compared to 22.8% of houses with 16 – 17 year olds. Interestingly, a number of factors related to types and extent of youth Internet use (e.g., amount of use, using for email and chatroom activity) were related to not using filters. Further, talking to strangers online and giving out personal information were both related to not using Internet filters. Among

those households less likely to report using Internet filters, youths were more likely to use the Internet for school assignments, as were those households whose youth rated themselves as above average students. Among parents, those with "an extreme degree of concern over youth exposure to sexual material, a low degree of trust that a child would use the Internet responsibly and a high degree of knowledge about what a child did online were more likely to use filtering and blocking software" (p. 760). Interestingly, the amount of time parents spent online, parents using the Internet for work, school and personal use, as well as parents' experience and the importance of the Internet to parents were not related to the use of filtering and blocking software.

In a report of strategies utilised by parents across Europe, a variety of additional non-technical measures were employed. Among the most common were:

1. ***Time restrictions:*** This was the most common non-technical strategy employed by parents and was generally done by fairly dividing time on the Internet among children and making sure that school work is given priority.

2. ***Supervision / control:*** Done by either sitting next to their children when they are online or by watching the screen or checking up on them periodically.

3. ***Talking to / teaching children about safe Internet usage:*** This was a strategy employed by parents in close to 50% of the European countries sampled. Interestingly, data from the Czech Republic highlighted the potential error in assuming the effectiveness of this strategy by examining parental report

statistics alone. Over 80% of parents in the Czech Republic reported talking to their children about Internet safety while only 39% of children sampled said the same. This discrepancy raises a number of questions such as, whether parents and children talking about the same thing when they discuss safe Internet usage.

4. ***Rules against revealing personal information:*** Only 35% of countries (6 out of 17) sampled reported that parents indicated having rules about personal information. In 5 out of the 6 countries, parents reported that it was common to have these rules.

5. ***Rules not to visit certain sites:*** Only 35% of countries reported that parents had rules about visiting certain websites. Though it is unclear which websites (or types of websites) had rules associated with them, some reported that these rules were in relation to websites containing sexually explicit material.

6. ***Other strategies:*** Among the other strategies employed by parents across Europe were rules against meeting someone they have only met online, not talking to strangers in chatrooms, rules against downloading files, not buying things and rules against foul language and bad behaviour.

Figure 8.5.2 outlines the most common rules that Australian parents reported regarding Internet use and contrasts parent and child reports. Interestingly, in most cases, parents reported the existence of specific Internet-related rules. Among the exceptions to this trend, the most interesting discrepancy was reflected in the percentage of children who

reported no Internet-related rules in place (7%) compared with parents (0%). Another discrepancy of note related to the percentage of parents who reported rules regarding which websites were accessible with permission only (38%) compared with children (19%). Similarly, 20% of parents reported rules about the time spent online whereas only 14% of children reported the same. Although it is not feasible to comment on these differences in any statistically meaningful way, the trends are noteworthy.

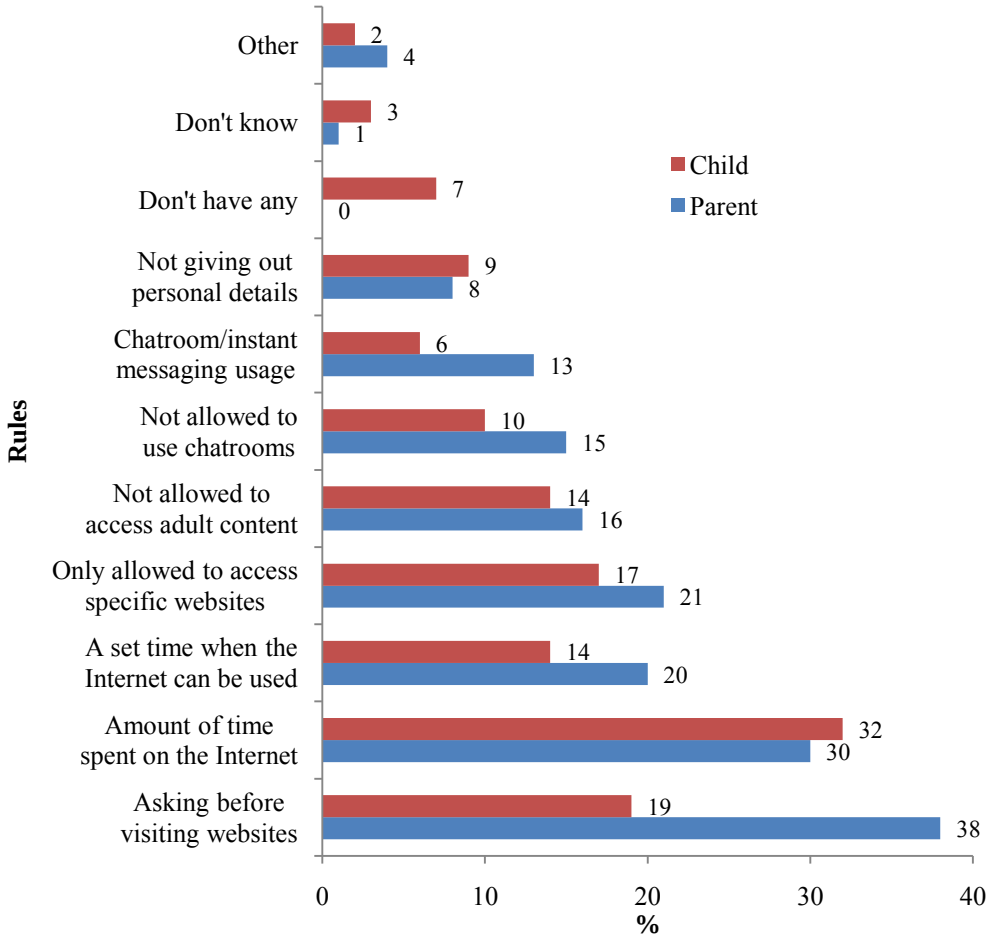

Figure 8.5.2 Internet rules in Australian households in 2007 (NetRatings, 2005)

8.6 Education-based strategies

In recent years, a plethora of cyber-safety resources has been released most of which have focused on cyber-bullying behaviours. However, few have been developed according to a specific theoretical framework with even fewer being empirically validated. Therefore, although the following section will provide an overview of a very small selection of the most promising programs available, we are not providing an endorsement of any particular program. In addition, we are not suggesting that by including a program in this section of the review that this is an indication of sufficient empirical evidence. Most of the promising programs reviewed (both Australian and non-Australian based) are in need of further testing and this prevents a critical appraisal.

8.6.1 Australian-based programs

A number of Australian-based program have been developed to address cyber-safety and, more specifically, cyber-bullying and here we review the more comprehensive ones.

8.6.1.1 Net Alert

In Australia, *Cyber Safe Schools* was released in 2005 by the Australian Government's Internet safety advisory body, *NetAlert*, whose educational functions were

subsequently (in 2007) merged with the cyber-safety functions of the Australian Communications and Media Authority (ACMA). The program was developed in response to a *NetAlert* study undertaken by the Curriculum Corporation which found very few relevant education resources and support materials were available for teachers. The recommended three-phase program was developed by *NetAlert* to support the teaching of Internet safety within Australian schools and is comprised of: teacher planning and professional development, *CyberQuoll* for primary schools and *CyberNetrix* for secondary schools. *A Teacher's Guide to Internet Safety* (NetAlert, 2007a) is included in the first phase as a general introduction to a whole school approach and topics related to cyber-safety. Within the *CyberQuoll* and *CyberNetrix* programs, corresponding materials are provided for each of the following groups: students, teachers and parents. Each student activity for *CyberNetrix* relates to an individual case study provided in both video format and as a written transcript.

A series of questions are provided for group discussions, led by teachers, and designed to encourage students to publicly and actively participate in preventing cyber-safety risks such as cyberbullying. *CyberQuoll* promotes an active and inclusive approach and includes five 'episodes' in video and written format. Multiple activities are provided for each of the five episodes and all include discussion questions, activities to create posters and other activities to engage students in generating solutions to problematic encounters (e.g., write a 'what should I do?' letter to a magazine and incorporate classroom discussions about the letters). The Cyber Safe Schools program is intended to provide education on multiple cyber safety issues. Therefore, *CyberNetrix* includes one case study on

cyberbullying while one episode of *CyberQuoll* addresses netiquette (i.e., Internet etiquette).

Resources include Internet safety education guides for both primary school teachers (*CyberQuoll*) and secondary school teachers (*CyberNetrix*), which correspond to resource activity sheets for students (NetAlert, 2005a, 2006a). Objectives, materials, tasks, and guidelines to help students are included in the 45-page Teachers Guide. A survey is included for teachers to complete to facilitate assessment of the program, and accommodate suggestions for future program development.

Internet safety education for primary schools: A parent guide is available for *CyberQuoll* (NetAlert, 2005b) and *CyberNetrix* (NetAlert, 2006b) and provides instructions about the specific NetAlert Cyber Safety Schools program used at school. The *CyberQuoll* parents' guide includes definitions of Internet topics, reasons why children engage in digital technology activities, suggestions to help make Internet use safer for children and additional resource websites. The *CyberNetrix* guide provides a list of topics covered for each lesson activity and encourages parents to support and discuss issues raised in the lesson plans. The brief guide does not provide information on how parents can assist in completing and learning new information through the activities provided by teachers. Students are provided access to a specific *CyberQuoll* website (NetAlert, 2007b) and *CyberNetrix* website (NetAlert, 2007c) to allow interaction through computer activities at their own level.

8.6.1.2 Bullying. No Way!

Bullying. No Way! (2009a) is part of a project called Safe and Supportive School Communities: Finding workable solutions for countering bullying, harassment and violence in schools (SSSC). The project is developed and managed by all participating Australian education authorities: State and Territory government education systems, the National Catholic Education Commission (NCEC), the Independent Schools' Council of Australia (ISCA) and the Commonwealth Department of Education, Employment and Workplace Relations (DEEWR). Resources are available in the following areas: legislation, policies and procedures, teaching materials, support services, and information sources. There is some variation in the range and content included in the resource pack provided by the various education departments. For example, those resources provided by the Western Australia (WA) Department of Education and Training (DET) and the Tasmanian (TAS) Department of Education are somewhat limited in contrast to the resources provided from New South Wales (NSW) and Victorian (VIC) departments. Teacher specific resources include a list of books and websites for teachers to access.

The TAS Department of Education suggests that schools should educate students about cyber-safety offences, such as cyber-bullying, and results of these behaviours. Some of the resources provide a basic introduction to the laws relating to cyber-safety risks. For example, the Commonwealth's Criminal Code Act 1995 (Section 4.7.4.15, Department of Education and Training, 2009a), which cautions that it is an offence for a person to use 'a carriage service to make a threat' is mentioned in the available resources. A Tasmanian

Criminal Code Amendment (stalking) Bill 2004 is also mentioned which 'includes publishing or transmitting offensive material and sending electronic messages with the intention of causing physical or mental harm.' There is additional information provided to assist with other technical issues (e.g., how to report videos viewed on YouTube). A magazine for parents and carers has also been released as a result of recommendations from the Engaging Our School Communities Taskforce. To date, two issues of Engage have been released (Department of Education, 2009b).

The VIC Government Department of Education and Early Childhood Education also references similar laws to that of the TAS Department of Education and generalizes anti-bullying policies, from the Safe Schools and Effective Schools to be applied to cyberbullying (Department of Education and Training, 2006). References are made the information in peer-reviewed articles being used to develop policy measures. For example, a review of cyber-bullying provided evidence for policy makers to consider when contemplating new and/or modified polices (Brown, Jackson, & Cassidy, 2006). Schools are also encouraged to access the *Let's Fight It Together* cyber-bullying resource (this resource is described in detail below).

The NSW Department of Education and Training provides a 40-page parent guide but, as at the production of this report, no teacher guidelines were available. This parent guide (Department of Education and Training, 2008) addresses the positives of digital technology, definitions, online safety, homework (researching online), mobile safety, cyber-bullying and buying a computer. In addition to general cyber-safety suggestions, the

resources produced by the NSW Department of Education and Training also include specific recommendations that were drafted in collaboration with leading experts such as Dr. Marilyn Campbell from Queensland University of Technology. A number of issues are presented in an attempt to provide parents with some practical background information and advice about cyber-bullying. Prevalence rates, examples of cyber-bullying, and issues of concern were provided by Dr. Campbell. Additionally, warning signs associated with exposure to cyber-bullying behaviours as well as practical tips for preventing cyber-bullying are included.

There is a great deal of information on the *Bullying. No Way!* website that is focused on cyber-bullying as well as face-to-face bullying. For example, the website includes information about other Australian researchers including previous studies, results and background information.In additional to external resources and current research, *Bullying. No Way!* offers brief overviews about cyber-bullying specific topics including: general descriptions about cyberbullying; project guidelines for creating an anticyber-bullying mobile movie, and the role of schools and parents. Most of the research findings available on the website focus primarily on prevalence rates.

Evidence based whole-school community approaches are presented which outline the topic stage and the roles of school 'in and out of class', staff, students and carers (*Bullying. No Way!*, 2009b). These strategies appear to cater more to face-to-face bullying rather than cyber-bullying specifically. Case studies related to these approaches are detailed for topics such as homophobia, building positive student relationships and peer

mediation (*Bullying. No Way!*, 2009c). More generic whole-school community approaches are described in a separate section of the website, including suggestions for students, classrooms, parents and carers and the school community. Some examples for students are organising a local forum to discuss issues affecting young people, carrying out their own community research project and organising school and community programs to educate young people. While these generic approaches may be applied to cyber-bullying, they appear to have been created within the framework of traditional bullying topics.

8.6.2 International programs

As with the Australian-based program, various international programs have been developed to address cyber-safety and, more specifically, cyber-bullying. We will review here those programs that appear to be the most comprehensive. Further, we only review those programs that are English-language based but acknowledge that the work ongoing in other countries.

8.6.2.1. Childnet International – Know IT All, Let's Fight It Together, Jenny's Story

Childnet International has produced a series of resources beginning with the launch of the *Know IT All* for Schools CD-ROM released in 2005 in collaboration with MSN UK. The material was targeted at young people (12 – 18 years) and distributed to all UK

secondary schools. This suite of resources primarily focused on cyber-safety (Childnet International, 2005a) and additional ones were then developed to be used in conjunction with *Know IT All* for certain issues. For example, *Let's Fight It Together* is solely devoted to cyber-bullying and mainly produced for teachers in an assembly or classroom situation with students 11 – 14 years of age. The resource comprises a video and two 45-minute lesson plans (Childnet International, 2007c) with guidance on where cyber-bullying can be taught within the UK National Curriculum. The video is a drama documentary and includes interviews with the characters in the documentary (the person who bullies, teacher, mother, bystander and the target). The first lesson plan introduces the topic of cyber-bullying through classroom discussions held prior to and after viewing the video. These identify forms of cyber-bullying (awareness of types of cyber-bullying such as forwarding a message via mobile phone), explore why people are bystanders choose to engage in cyber-bullying, and consider ways to stop cyber-bullying.

The second lesson explores perspectives of each of the characters in the video through watching their interviews, role-play scenarios, character debate questions with some answers and prompts, and discussions. Teaching points are listed in chart form for both lesson plans, which address main category objectives from the National Curriculum (e.g., healthy, safer lifestyle) and what young people should be taught in relation to each category (e.g., recognise when pressure from ICT threatens their personal safety and wellbeing and developing effective ways of resisting pressure). For each category, there are questions to engage young people in discussion and/or prompts and objectives.

Let's Fight It Together is based on a good guidance practice guideline from Childnet International for the Department for Children, Families, and Schools (DCFS; 2007a). The eight-page summary report of the good guidance practice guidelines (DCSF, 2007b) incorporates an easy to read reference guide for schools to use along with the *Let's Fight It Together* resource. The 56-page full report (DCSF, 2007a) provides more in-depth information about a range of issues and addresses additional areas such as 'working with the bully and applying sanctions', 'updating existing policies and practices' and UK laws relating to cyber-bullying.

Getting to Know IT All was released along with *Know IT All for Schools* to aid in the delivery of the latter resource. As part of *Getting to Know IT All*, volunteers from Microsoft and law enforcement were trained to deliver the interactive elements from the *Know IT All for Schools* resource, reaching an estimated 50,000 young people face-to-face in schools. An evaluation study funded by Ofcom and conducted by researchers at the University of Bristol (Wishart, Andrews, & Ching Yee, 2005) evaluated the volunteers' delivery of the *Know IT All* presentation (suitable knowledge, quality control procedures to ensure future success of volunteer model, volunteers were suitably trained to deliver presentation). The study also assessed if the objectives of the presentation were met: development of a cyber-safety campaign to effectively empower teachers to deliver the information; raising awareness of cyber-safety for parents, teachers, schools and young people; easy delivery of the presentation, ease of understanding and relevance to the audience, and inspiring a call to action by the audience.

Initial input was obtained from stakeholders through phone interviews, followed by trained volunteers completing a paper based evaluation form once training was complete, but prior to delivery of the presentation. Immediately following the delivery of the presentation, a paper-based evaluation form was completed by students (n = 657) and teachers (n = 52) and an online evaluation form was completed by volunteer presenters (n = 43). Thirteen teachers (just under 10% of the total number of teachers who received the presentation) were later followed up with a phone interview. Phone interviews were also conducted with 16 volunteers (representing 10% of the volunteers who completed the online evaluation survey). Results from the student and teacher evaluations demonstrated that 80% of students felt called to action and reported plans to follow up the presentation in various ways. In addition, 80% of teachers reported feeling called to action and planned to visit at least one of the websites cited in the presentation; 40% planned to use or apply for resources in the presentation; and 50% of teachers reported planning to follow up the presentation in their classes. Follow-up teacher interviews found that schools incorporated a range of actions which included changes in school policy, provided advice to the school on Internet safety (provided on school website). However, some schools made no changes after the presentation. Additionally, phone interviews with volunteers revealed that police volunteer presenters who participated considered that presenting to schools on cyber-safety was an important aspect to their everyday work. Students also noted their appreciation for volunteer presenters who appeared to have technical expertise and knowledge. Overall, 100% of volunteers and 98% of teachers reported that they would recommend the program to a colleague. Among the recommendations that were made to improve the program were

the need for schools to specify who and which subject area to deliver the curriculum, training more volunteers to deliver the resource – due to teachers' appreciation of their time and delivery, information specifically targeted at parents, and better suggestions on how teachers can use the resources.

Know IT All for Parents was produced in 2006 and distributed to approximately 100,000 families in collaboration with the UK Government Department of Education and Skills (DFES). Childnet International indicate that discussions were undertaken with a 'wide range or parents' in creating the resource but we were unable to locate any data or report for these findings. Parents involved in the study noted that their apprehension stems from lack of computer experience, which inhibits them from getting involved and understanding the benefits of the Internet (Childnet International, 2007a). Thus, the aim of the parent resource is to encourage dialogue between parents and their children about the Internet. To achieve this goal activities with quizzes and games for parents and their children to complete together are included along with the prompt to draft Internet agreements.

Know IT All for Teachers (now called *Know IT All for Secondary Schools*) was launched in 2007 and sent to every teacher training institution across England and Wales as well as being made available online. The resource is the result of a pilot program undertaken by Woollard, Wickens, Powell and Russell (2007). The pilot program was presented to 400 trainee teachers of which 283 completed the online evaluation. The main research goal was to assess the needs and practicalities of implementing a cyber-safety

teacher resource rather than evaluating the effectiveness of specific components of the resource. Key findings include the following:

1. Cyber-safety should be taught by all teachers, not specifically ICT teachers, although one staff member should be designated to teach cyber-safety;
2. A large majority valued the importance of cyber-safety and wanted to see schools address the issue;
3. A significant minority of trainees received no information about cyber-safety from their placement schools, and
4. Face-to-face presentations provided higher uptake of contents, especially when presented in smaller groups.

Trainee teachers highlighted the importance of having a portal available for them to access resources on cyber-safety that would also include classroom materials, appropriate training and information resources on the topic. The *Know IT All for Parents* and *Know IT All for Teachers* resources have limited information on cyberbullying; parents are advised to consult the *Let's Fight It Together* resource for additional information on cyber-bullying. Although parents can watch the video and engage in the activities with their children, the activities are designed to be delivered via group discussions, which may be challenging for some parents to adapt.

Know IT All for Teachers also includes a documentary video, *Jenny's Story*, which addresses general cyber-safety. The video was developed using focus groups of young people in both the UK and Denmark (12 – 16 years) to help deliver a resource based on real stories (this approach was also supported by research undertaken by Childnet International and Becta, which found case studies were an effective way to encourage meaningful open dialogue with teenagers (Childnet International, 2005b). The aim was to develop a film based on a true story that would challenge young people to ultimately change their risk taking behaviour online to help prevent cases such as in Jenny's story from occurring and this resource was then tested by Childnet International. The summary report contains feedback from 2,000 students and 19 teachers from 12 secondary schools in Lancashire (Childnet International, 2005c). The resource was found to be successful, with 80% of the pupils in the pilot study reporting the video had significantly affected them and challenged them to change their online behaviour. After reviewing the video, a significant decrease from 18% to 3% was seen in young people who would share personal details with someone they met online only. The majority of teachers also felt equipped to deliver the resource in terms of their knowledge of Internet safety and felt it vital to explain the background and to be able to answer questions. It is not clear if recommendations and changes, if any, were made based on the research.

8.6.2.2 NetSmartz

NetSmartz was developed by the National Center for Missing and Exploited Children in America. Resources are available for parents/guardians, educators, law enforcement officials, teenagers and children and focus predominantly on cyber-safety with some emphasis on cyber-bullying. A study was conducted to assess the effectiveness of the *NetSmartz* program I-360 (Branch Associates, 2002) which was created by the Boys and Girls Clubs of America (BGCA) and *NetSmartz* Workshop, and released under the name of *NetSmartz* Teens: I-360 as a resource for BCGA and the National Centre for Missing & Exploited Children (2006). A research summary report described the sample as consisting of 15 members of the BGCA from four age groups (6 to 7 years, 8 to 12 years, and 12 years and above) and reported that 83% of young people aged 12 years and older reported that the program changed specific online behaviours (Branch Associates, 2002; see Table 8.6.1 below).

Table 8.6.1 *List of reported behavioural and knowledge change after completion of the NetSmartz Teens: I-360*

Question	**Pre-test** Agree	**Post-test** Agree
If someone is harassing me by sending nasty e-mails, I should just ignore him or her. The person will eventually stop.	39%	34%
Victims of Internet crimes are almost always females.	32%	34%
The Internet is a great place for me to express my anger and opinions because no one knows who I am on the Internet.	27%	16%
I feel more comfortable talking to people online than in person.	27%	32%
What I do on the Internet doesn't really matter because, once I log off, no one will be able to find me.	24%	13%
As long as I have online friends, there is no need for me to go outside and play with other friends.	8%	10%

There were a number of limitations associated with this study, for example, it is unclear whether a comparison group was included to confirm any differences between pre- and post-test scores were related to the program. The study authors report that the changes observed after participation in the program were consistent with expectations[35]. We were unable to find any evidence suggesting that the *NetSmartz* resources were based on the available empirical evidence. Researchers at George Washington University assessed the effectiveness of the NetSmartz Program. Two studies were independently conducted, although identical research questions were pursued. The two studies included 24 students (aged 8 – 9 years) from the Saco School District in Maine and 98 students (aged 8 – 14

[35] Available from: hwww.netsmartz.org/pdf/evalstathigh.pdf

years) of Palermo school in Maine, respectively. Pre-test measures were taken and compared to post-test results (see Table 8.6.2).

Table 8.6.2 *Evaluation of the* NetSmartz*cyber-safety program*

Question	**Pre-test** Unsure or believed it was safe		**Post-test** Not safe	
	Saco	**Palermo**	**Saco**	**Palermo**
Safe to meet someone in person after they had been chatting with them for a long time.	54%	13%	83%	82%
Safe to say what school they attend.	50%	36%	92%	96%
Safe to tell people where they hang out	29%	16%	92%	100%
Safe to state their real name on the Internet	25%	20%	92%	98%
Safe to put their address on the Internet	25%	16%	88%	95%
Safe to post their picture on the Internet.	25%	15%	96%	98%

Available at www.netsmartz.org/pdf/gw_evaluation.pdf

The results from these pre-test / post-test studies indicate increased evidence for cyber-safety awareness. It is almost as interesting to examine the low rates of students (in both schools but more so in Palermo) who believed that certain risky behaviours on the Internet were safe.

8.6.3 Education strategies summary

Overall, we could find only limited evidence indicating that theoretical structure and/or empirical data were building blocks of the cyber-safety resources made available to parents and teachers. Of all the specific topics addressed in the cyber-safety resources, cyber-bullying appears to be a central concern. While this research may provide insight into prevalence rates, motivations for cyber-bullying, emotions felt by those cyber-bullied, they do not appear to substantiate the intervention advice provided to parents. For example, in the US, the National Crime Prevention Council (NCPC) released the Cyber-bullying Research Report (2006) after surveying 824 teens (aged 13 – 17 years) on aspects of cyber-bullying. Based on these research findings, NCPC released a 'Stop Cyberbullying Before it Starts' guide (NCPC, 2008), which reported that:

1. Nearly 20% of teens reported that a person who was cyber-bullying them pretended to be someone else in order to trick them online, getting them to reveal personal information;
2. Nearly 50% of teens felt angry after they were cyber-bullied; and
3. Thirty-four percent talked to friends about bullying.

Among the advice that followed was: consider the location of computer in the house, talking to children about cyber-safety and communicate online rules and responsibilities.

8.7 Text analysis

In addition to filtering and education, other strategies have been utilised to mitigate the risks associated with Internet usage. One such method involves the development of text analysis software. As this is novel software and its efficacy in relation to enhancing cyber-safety (in terms of the specific issues outlined in this review) has not been determined, we will present a case study illustrating the utility of this approach. Specifically developed as a tool to address the risk of online grooming, Crisp Thinking (a UK based company) recently made software available that is designed to monitor and assess the content and patterns in conversation that minors have online. These conversations are flagged if it is determined that the patterns are consistent with those similar to online grooming interactions. If similarities are observed between grooming and a minor's current interactions, parents are notified that their child is engaging in risky online interactions. In addition, this technology has recently been made available for mobile phones (My Mobile Watchdog is one example) but the effectiveness of these approaches remains unclear.

8.8 Other strategies

A number of other strategies have been and are being used to mitigate youth cyber-safety risks. Among the more commonly used strategies are: age verification / identity authentication and biometrics. Age verification technologies essentially seek to utilise verified age as a means of limiting interactions between minors and adults. To date, there

are a number of strategies that have been employed to verify the age of a user such as using a trusted third party for verification (e.g., schools or government agencies). Identity authentication technologies are designed to verify the identity of a user. The ISTTF (2008) reported that available technologies make it difficult for children to pretend to be adults or adults to pretend to be children but rarely does one technology do both functions. Moreover, Willard (2009) has raised many issues that cast doubt over the utility of this technology.

The ISTTF Technology Advisory Board (2008) noted some important limitations associated with age verification / identity authentication technologies. For example, the verification credentials that are received as part of the process (thus enabling future browsing) can be obtained from victims under duress. Further, and importantly, much of the age verification movement is based on an assumption that age related deception is at the heart of online grooming and sexual solicitation interactions. However, as outlined previously, the research evidence suggests that the average "groomer" is not necessarily a paedophile. The final conclusion reached by the ISTTF was that "age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness" (2008, Appendix D, p. 10).

In response to the potential for identity theft, the Australian Government Attorney-General's Department (2006) offered the following technical and behavioural strategies to minimise the potential of being targeted:

1. **Use passwords and access controls:** This will make it more difficult for identity thieves to access information directly from a computer.

2. **Avoid giving out personal information over the Internet**: It is suggested that only those companies whom the user initiated contact with should be provided with information and only the minimum amount should be given.

3. **Never click on a link or open an attachment in an e-mail from someone you don't know and trust:** Rather than clicking on the link, users should type in the web address to avoid downloading malicious software.

4. **Regularly install and update anti-virus protection software:** Only those anti-virus programs that are most up-to-date will protect a computer from the latest viruses and malicious software.

5. **Avoid using public computers to access your personal information:** Personal information, including passwords, credit card and account numbers can be retrieved from a computer's hard drive.

Further, the Attorney-General's Department (2006, p. 18) provided the following checklist that computer users can use to determine their level of security. If users answer any of the following questions in the affirmative, they are advised that they are open to being the victim of identity theft.

Computer Security	**Yes / No**
Are you forgetting to change your ISP password regularly?	
Do you keep personal information on your computer hard drive?	
Do you forget to regularly update your virus protection?	
Do you use public access computers?	
Do you lack personal firewall protection?	

Finally, biometrics have recently been used to mitigate risks to cyber-safety relates to biometrics by identifying users physical features (e.g., fingerprint or iris colour), or behavioural traits (e.g., walking gait). We were unable to identify any research examining how biometric measures mitigated the risks to cyber-safety outlined in this review. However, the ISTTF Technology Advisory Board (2008) noted that facial images can be altered by, for example, manipulating lighting or altering facial hair. Although these tools show promise (ISTTF, 2008), there are a number of challenges hindering their widespread appeal (e.g., cost). Further, the underlying logic for biometric technologies is that at the core of the risks to cyber-safety is an offender's intent to deceive potential victims about their true identity. However, as discussed previously (Section 1.3.1) very few offenders

concealed their identity when they first met potential victims online (Wolak, et al., 2004). Therefore, using this technology may result in a false sense of security regarding the safety of children and youth who use the Internet.

SECTION 9

GAPS IN THE LITERATURE

Section Summary

Gaps

- There are gaps in the literature describing all areas of cyber-safety research. This is particularly true in relation to Australian-based research.
- Some areas (e.g., cyber-bullying) have received much attention and, consequently, more is known about the prevalence and outcomes associated with these behaviours.
- There are various ethical and methodological issues that make it difficult for researchers to examine certain risk areas (e.g., online grooming).

9.1 Overview

This review of the Australian and international research literature has revealed that, overall, relatively little research has addressed cyber-safety risks. Some areas such as cyber-bullying, however, have received much greater attention by both the scientific community and the media. Nevertheless, in relation to cyber-safety risks in general, there appears to be an inconsistency between what is reported in the media and in the scientific research literature. For example, much has been written in the media about online grooming and the dangers of interacting with strangers online. However, the research in this area is practically non-existent. On the other hand, other risk areas, such as the promotion of self-harming behaviours or eating disorders on the Internet, have received scant media attention.

At the time of preparation of this report, cyber-bullying was receiving much attention both in the scientific community and the media. The research in this area has greatly increased over the past five years and the importance of this issue is reflected in a Special Issue on cyber-bullying being prepared by the prestigious Journal of Psychology. Although little is currently known about the mechanisms that drive cyber-bullying behaviours, including if and how they differ from face-to-face bullying, there is growing interest in the theory of cyber-bullying (e.g., Dooley, et al., in press). However, the research to date is primarily descriptive such that relatively little is known about, for example, the cognitive mechanisms of cyber-bullying. Overall, gaps have been identified across almost all areas of cyber-safety research. These research gaps were more apparent in relation to some issues than others (e.g., hate crimes versus exposure to pornography). It is unclear why certain areas of cyber-safety research attract greater interest than others. Clearly, certain types of risks (e.g., contact risks and the associated risk of physical harm) represent a much greater potential danger to young people using the Internet than other types of risks (e.g., content risks).

Several other issues may, in some ways, contribute to the gaps or hurdles in the literature. One such issue relates to the theoretical development and framework describing the various constructs and behaviours associated with cyber-safety. For example, despite the extent of writings describing cyber-bullying behaviours (as well as the associated outcomes), it is only recently that a detailed examination of the theory underlying these behaviours has been conducted (Dooley, et al., in press). Similarly, we were unable to locate any in-depth and detailed discussion about the nature of cyber-stalking, online

grooming, sexual solicitation and associated behaviours. A consequence of this is that there is often disagreement about how the target behaviour (e.g., cyber-bullying) is defined and this can impact on how motivations for technology use are measured.

> "Certainly, users have different social and psychological needs that motivate their choices. These needs compel people to seek information or enter into communication, and they have expectations about what they will gain from such activity. Owing to these motives and expectations people select particular media channels, sources and content. Different people will use the same channels, sources, and content for quite diverse reasons and with contrasting expectations."
>
> *Mesch, 2009, p. 604*

Clearly, variations in how behaviours are defined result in methodological differences. This often leads to differences in reported prevalence rates and outcomes associated with exposure. For example, definitional differences have prompted researchers to measure electronic harassment, cyber-bullying and online bullying each of which is subtly different in terms of its relationship to offline behaviours and issues of repetition and intent (see Section 3 for more detail on theoretical and definitional differences associated with cyber-bullying research). Furthermore, there is ongoing debate about the appropriateness of the term "Internet addiction" to describe the pathological over-use of the Internet. Many have argued that Internet addiction is a legitimate disorder given the evidence describing the consequences, associated with not using the Internet (for those who

report being addicted), which are very similar to those described in people addicted to gambling. However, some research evidence indicates that it is functions of the Internet (e.g., chat) that is the focus of the addiction.

Another issue that is associated with gaps and limitations in cyber-safety research is the relationship between online and offline behaviours. This issue has a similar effect to definitional problems in that there is the potential for aspects of the behaviour to be measured only in relation to the way in which they are associated with offline behaviours. For example, in the cyber-stalking research literature, there are many who consider those behaviours to be mere extensions of offline stalking behaviours and this perspective is reflected in the laws describing cyber-stalking. However, it has been demonstrated that there are differences between those who are subjected to cyber-stalking behaviours compared to those who are subjected to offline stalking behaviours. For example, a proportion of those people who experienced cyber-stalking described themselves as disabled in contrast to offline cyber-stalking experiences.

9.2 Australian context

This report identified that there are clear gaps in the Australian cyber-safety research literature. Of the areas of cyber-safety risks outlined in the tender document DCON/08/93 (which this report was undertaken to address), significant gaps were identified in almost all areas of cyber-safety research. For example, we were unable to

identify any quality research studies (published or otherwise) that addressed online grooming or sexual solicitation. Similarly, we could not locate any research studies on drifting in relation to cyber-safety and exposure to certain types of age-inappropriate content (e.g., hate websites, pro-ana websites). Further, limited work has been done in the areas of cyber-stalking, promotion of inappropriate social or health behaviours (in particular smoking), privacy, identity theft and identity fraud issues associated with technology use. There is some research currently being done on exposure to age-inappropriate content (mostly focused on pornography) and cyber-bullying but published scientific research in these areas remains relatively limited. However, despite the limited published work in the area of cyber-bullying, there is much ongoing work being conducted in Australia on a number of aspects of these behaviours. For example, the Child Health Promotion Research Centre at Edith Cowan University is currently developing and empirically testing several cyberbullying specific interventions. This ongoing work represents a first attempt to empirically validate a cyberbullying specific intervention and is, at the time of the production of this report, the first large-scale cyber-bullying specific intervention being empirically trialled in the world.

Overall, there are several areas of cyber-safety research that are attracting interest from Australian research community; however, work in this area remains limited. It is clear that, as technology develops and the interactive and seamless nature of technology is enhanced, many of the risk factors outlined in this report are likely to increase. Given the clear hurdles faced by researchers interested in examining cyber-safety risks, the major gaps in this area are not unexpected. However, given the sensitive nature of some of the

risks associated with technology use, it may not be feasible to ethically investigate the nature of particular risk areas. Importantly, if these hurdles remain insurmountable, the conclusions that are drawn from methodologically unsound research studies should be interpreted cautiously if at all.

SECTION 10

OPTIONS FOR MAINTAINING THE CURRENCYOF THE INFORMATION CONTAINED IN THIS REPORT

Section Summary

- High level monitoring: The Published International Literature On Traumatic Stress (PILOTS) database is an example of a high level monitoring option for maintaining currency of the research literature.
- Moderate level monitoring: A basic database would be maintained by an organisation or government department and updated based on the input of the research community. This could be designed to include material not published in scientific journals (e.g., government reports).
- Low level monitoring: Comprised of an email alert system that would provide notification of new publications on a specific topic.

10.1 Overview

This section describes three options, which can be used to maintain the currency of the information collected and considered throughout this report, ranging from high intensity involvement (providing an extensive amount of information) to minimal involvement providing only perfunctory information. As with other sections in this report, any programs discussed or referred to in this section should not be interpreted as an endorsement or promotion of that product.

10.2 High level monitoring

At the current time, a large number of databases are available that can be used to identify the most current research literature. However, as evidenced in the methodology of this report, it can be somewhat difficult to identify all the relevant research publications on a particular topic (e.g., cyber-bullying). As was the case when researching the scientific and grey literature for this report (peer-reviewed and not), the identification of quality and relevant publications is a huge task requiring extensive resources, highly competent staff, and sufficient time to review a vast amount of highly diverse material. Given the range of issues encompassed by the term "cyber-safety", it is necessary to search through a large number of databases. For example, manuscripts addressing Internet filters are published in different journals to those addressing cyber-bullying. One strategy to overcome this is to have all cyber-safety manuscripts listed in a separate repository.

The following section describes an example of one such repository, the Published International Literature On Traumatic Stress (PILOTS) database, which is an electronic index to the published literature on post-traumatic stress disorder (PTSD) and associated mental-health consequences of exposure to traumatic events. The database is produced by the National Center[36] for PTSD (NCPTSD) in the US and is electronically available to the public free of charge and does not require an account or password[37]. Each record in PILOTS is a representation of a document, containing:

[36] The NCPTSD is a sub-division of the US Department of Veterans Affairs, a government agency.
[37] A password is required to search the database and this is available on the NCPTSD website.

- A bibliographic citation, giving information (author, title, and source) required to locate the document;

- A brief description of the article's content containing information which basic search techniques can use in selecting documents, and

- A brief summaryof the manuscript to help determine if it is relevant to a particular enquiry.

The NCPTSD also provides additional resources that are associated with the PILOTS database. For example, a thesaurus gives a listing of terms that are used to describe exposure to trauma. This is a very useful resource especially for those not actively working in the area of PTSD. A similar cyber-safety resource would be crucial given the diversity of terminology employed within each risk area outlined in this review (e.g., the terms cyberbullying, online aggression, electronic bullying, and electronic harassment are often used interchangeably). The NCPTSD also supports, through the PILOTS database, a free e-mail alert system which can provide users with weekly e-mail notifications of all new additions to the database (up to 250 per alert). Alerts are specific to a sub-topic of the PTSD literature (e.g., psychotherapy, drug therapy) and the manuscript is also described in the e-mail.

A final resource made available through the PILOTS database is a listing of all PTSD-related measures that are used. Users of PILOTS are provided with a citation and each record includes an "Instruments" field which lists all the assessment instruments used

(psychological and medical) in the research or clinical work reported in the document enabling users to:

- Identify the instruments used in the research described in a particular manuscript;
- Determine which published papers have used a particular assessment instrument, and
- Locate papers whose focus is the description, validation, or use of a particular instrument.

Finally, as assessment is an important issue, a listing is also available of each instrument that has been used in any manuscript that has been indexed in the PILOTS database. The NCPTSD reported that, by mid-2006 there were over 30,000 references in the database. The PILOTS database is updated every two months by a staff of four people – an Information Scientist, a Librarian/Bibliographer, an Information Resource Developer and a Resource Centre Coordinator. In addition, journal authors are encouraged to contact the NCPTSD and provide information about their published research papers. Although unpublished conference presentations are not included in the database (nor do they index published articles from manuscript copy), publications from obscure and well-known journals, books, book chapters, pamphlets, technical reports, and materials in all languages are all uploaded to the database. Therefore, the database contains all the relevant research and grey literature. Finally, the PILOTS database had links to full text articles for about 40% of citations as of mid-2006.

Clearly, the PILOTS database represents a major resource with extensive and impressive utility. Nonetheless, there are some limitations associated with information in this form. For example, what is available is a listing of all updated published manuscripts across all issues associated with PTSD. This means that a user is still required to search within a specific topic if necessary. Although the e-mail alert system removes the need to search for newly added publications, those currently held in the database are not included in the alert. Furthermore, less than half of the manuscripts included in database are available in full print, which means that once an article of interest is identified, users may need to pursue alternative avenues to obtain a full text copy. Despite these limitations, the PILOTS database is a very useful resource for researchers, clinicians and others working in the area of traumatic stress studies. The approach utilised in the PILOTS program would be well suited to the cyber-safety research area given the diversity of topics that comprises cyber-safety. Although this option would require a substantial initial investment (both of time and money) in order to generate and test a list of keywords, identify the relevant publications and identify world leading cyber-safety research experts[38], once the systems are in place they should be easier to maintain.

[38] It is estimated that level of commitment would be similar to the commitment and investment made by the Department of Broadband, Communications and the Digital Economy in this report.

10.3 Moderate level monitoring

We are not aware of any independent program, similar to PILOTS database but offering only a moderate level of monitoring. Therefore, we describe an approach that combines feedback obtained from some leading international cyber-safety researchers. In effect, the approach outlined here involves a government agency developing and monitoring an informal database (i.e., one that is not web-based or open to the general public). The information (which would be uploaded into a database) would be provided by the research community as well as other agencies working in the cyber-safety area. Further, researchers would be encouraged to provide full text copies, which would be stored with the database. This approach would provide an opportunity to maintain an ongoing list of resources that would, in essence, be updated by the research community. Of course, for this option to be viable, it would necessitate the involvement of the research community. One strategy to increase the potential for engagement by the research community is by making the database available only to those that contribute to it. It would be anticipated that other government agencies, not for profit agencies and other community groups would be keen to participate in and access the database. This strategy would increase the possibility that a large amount of the grey literature would be identified.

However, there are some limitations associated with this strategy. While the research community would complete the bulk of the manuscript identification, there is no guarantee that a sufficient number of researchers would become involved. Further, this option also requires the resources to store information (i.e., space on a server) as well as

personnel to enter information obtained from the research community. Nonetheless, obtaining updates from the research community would ensure that the information is relevant, current, and accurate as it is researchers actively working in the area of cyber-safety who are in the best position to inform the rest of the community. In effect, the research community would be acting as a filter by providing only those resources that are related to cyber-safety.

10.4 Low level monitoring

This option provides the lowest level of monitoring capability when compared to the other two options outlined above. The strategy involves a series of e-mail alerts being set up by an expert in cyber-safety research using a wide range of databases (such as those outlined in the methodology section of this report). These e-mail alerts would then be sent to a central e-mail address on a weekly[39] basis. Of course, this option only provides basic information about the resources that are identified based on consistency with preset keywords. Given that, as with the two options outlined above, there is no filtering of resources, there is an increased likelihood of resources being identified that are not strictly relevant to cyber-safety. In addition, this option does not make any of the grey literature available. Finally, this option does not permit engagement with the research community (as well as other government and community agencies), and thus limits the beneficial outcomes.

[39] For most databases, this can be more of less frequently or can be received on a specified day of the week.

SECTION 11

REFERENCES

Adler, P. A., & Adler, P. (2007). The demedicalization of self-injury: From psychopathology to sociological deviance. *Journal of Contemporary Ethnography, 36*, 537-550.

Adler, P. A., & Adler, P. (2008). The cyber worlds of self-injurers: Deviant communities, relationships, and selves. *Symbolic Interaction, 31*(1), 33.

Aisbett, K. (2001). *The Internet at home: A report on Internet use in the home*. Sydney: Australian Broadcasting Authority.

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of Cyberstalking Among College Students.*Brief Treatment and Crisis Intervention, 5*(3), 279-289.

American Psychiatric Association. (2004). *DSM-IV: Diagnostic and Statistical Manual of Mental Disorders*. Washington, DC: American Psychological Association.

American Psychological Association. (2006). *Testimony on behalf of the American Psychological Association*. Retrieved 19 March 2009, from http://www.apa.org/ppo/childmedia/testimony2.html.

Anderson, C. A. (2003). Violent video games: Myths, facts and unanswered questions. *Psychological Science Agenda, 16*(5), 1-8.

Anderson, C. A., & Bushman, B. J. (2001). Effects of violent video games on aggressive behaviour, aggressive cognition, aggressive affect, physiological arousal, and prosocial behaviour: A metaanalytic review of the scientific literature. *Psychological Science, 12*, 353-359.

AUSTRAC. (2004). The extent of money laundering in and through Australia in 2004. Report prepared for the Criminology Research Council. Retrieved 5 March, 2009 from http://www.criminologyresearchcouncil.gov.au/reports/200304-33.pdf

Australian Broadcasting Authority. (2001). *The Internet at home: A report on Internet use in the home*. Sydney, Australia.

Australian Bureau of Statistics. (2007). *Household use of information technology*. Retrieved 23 March 2009. from http://www.abs.gov.au/AUSSTATS/abs@.nsf/ProductsbyTopic/ACC2D18CC958BC7BCA2568A9001393AE?OpenDocument.

Australian Bureau of Statistics. (2008). Personal fraud Australia ABS cat No. 4528.0., Retrieved 23 March, 2009 from www.abs.gov.au/ausstats/abs@.nsf/cat/4528.0

Australian Communications and Media Authority. (2008). Filtering Software. Retrieved 16 March 2009, from http://www.acma.gov.au/WEB/STANDARD/pc=PC_90167

Australian Institute of Criminology. (2008). Crime facts info: No. 169. Retrieved 24 March, 2009, from http://www.aic.gov.au/publications/cfi/cfi169.pdf

Australian Law Reform Commission. (2008). *For Your Information: Australian Privacy Law and Practice*. Retrieved 20 February, 2009 from http://www.austlii.edu.au/au/other/alrc/publications/reports/108/11.html#Heading21

Australian Psychological Society. (2000). Median representations and responsibilities. Retrieved 11 March, 2009, from http://www.psychology.org.au/Assets/Files/media_position_paper.pdf

Australian Psychological Society. (2004). Psychological aspects of mobile phone use among adolescents. *The Australian Psychological Society, 3*(November), 1-7.

Bardone-Cone, A. M., & Cass, K. M. (2007). What does viewing a pro-anorexia website do? An experimental examination of website exposure and moderating effects. *International Journal of Eating Disorders, 40*(6), 537-548.

Baume, P., Rolfe, A., & Clinton, M. (1998). Suicide on the Internet: a focus for nursing intervention? *Australian and New Zealand Journal of Mental Health Nursing, 7*(4), 134-141.

Barak, A., Fisher, W., Belfry, S., &Lashambe, D. R. (1999). Sex, guys, and cyberspace: effects of Internet pornography and individual differences on men's attitudes toward women. *Journal of Psychology and Human Sexuality, 1,* 63-91.

BBC News UK. (2004). Extent of child net porn revealed. *BBC News*. Retrieved 27 April, 2009 from http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/3908215.stm

Becker, K., Mayer, M., Nagenborg, M., El-Faddagh, M., & Schmidt, M. H. (2004). Parasuicide online: Can suicide websites trigger suicidal behaviour in predisposed adolescents? *Nordi Journal of Psychiatry, 58*, 111-114.

Belsey, B. (2004). Cyberbullying, an emerging threat to the 'always-on' generation. Retrieved 23 March, 2009, from http://www.cyberbullying.ca/pdf/Cyberbullying_Presentation_Description.pdf

Beran, T., & Li, Q. (2007). The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing, 1*(2), 15-33.

Berliner, L., & Elliott, D. M. (2002). Sexual abuse of children. In J. E. B. Myers, L. Berliner, J. Briere, C. T. Hendrix, C. Jenny & T. Reid (Eds.), *The APSAC handbook on child maltreatment* (2 ed., pp. 55-78). Thousand Oaks, CA: Sage.

Berrier, T. (2007). *Sixth, seventh, and eighth-grade students' experiences with the Internet and their Internet safety knowledge*. Paper presented at the Educational Leadership and Policy Analysis, East Tennessee State University.

Berson, I., & Berson, M. (2006a). Children and their digital dossiers: Lessons in privacy right in the digital age. *International Journal of Social Education, 21*(1), 135-147.

Berson, I., & Berson, M. (2006b). Privileges, privacy and protection for youth bloggers in the social studies classroom. *Social Education, 70*(5), 124-128.

Berson, I. R. (2003). Grooming cybervictims: The psychosocial effects of online exploitation for youth. *Journal of School Violence, 2*(1), 5-18.

Berson, I. R., & Berson, M. J. (2005). Challenging online behaviors of youths: Findings from a comparative analysis of young people in the United States and New Zealand. *Social Science Computer Review, 23*(1), 29-38.

Blazczynski, A. (2006). Internet use: In search of an addiction. *International Journal of Mental Health Addiction, 4*, 7-9.

Bocij, P., Bocij, H., & McFarlane, L. (2003). Cyberstalking: A case study of serial harassment in the UK. *British Journal of Forensic Practice, 5*(2), 25-32.

Borzekowski, D. L. (2006). Adolescents' use of the Internet: A contoversial, coming-of-age resource. *Adolescent Medicine Clinics, 17*(1), 205-216.

Bowker, A., & Gray, M. (2005). The Cybersex Offender and Children. *FBI Law Enforcement Bulletin, 74*(3), 12.

Bozin, D. (2009). *Look who's watching*: Paper to the National Court of the Future.

Branch Associates. (2002). *NetSmartz evaulation project: Internet safety training for children and youth ages 6 to 18*. Atlanta: GA: Boys & Girls Clubs of America and National Center for Missing & Exploited Children.

Braun-Courville, D. K., & Rojas, M. (in press). Exposure to Sexually Explicit Web Sites and Adolescent Sexual Attitudes and Behaviors. *Journal of Adolescent Health*.

Brennan, M. (2006). *Understanding online social network services and risks to youth: stakeholder perspectives*: Child Exploitation and Online Protection Centre.

Brian, D. N., & Wiemer-Hastings, P. (2005). Addiction to the Internet and online gaming. *CyberPsychology & Behavior, 8(2),* 110-113.

Brookshire, M., &Maulhardt, C. (2005). *Evaluation of the effectiveness of the NetSmartz program: A study of Main public schools*. Retrieved 8 May, 2009 from http://www.netsmartz.org/pdf/gw_evaluation.pdf.

Brown, J. D., & L'Engle, K. L. (2009). X-rated: Sexual attitudes and behaviors associated with U.S. early adolescents' exposure to sexually explicit media. *Communication Research, 36*(1), 129-151.

Brown, K., Jackson, M., & Cassidy, W. (2006). Cyber Bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying. *Canadian Journal of Educational Administration and Policy, 57(December 18),* 1-35.

Brown, S. J. (2006). The surge in online gambling on college campuses. *New Directions for Student Services, 113*(Spring 2006), 53-61.

Bryant, C. (2009). Adolescence, pornography and harm. *Trends & issues in crime and criminal justice, No. 368*, 1-6.

Bryant, J. A., Cody, M. J., & Murphy, S. T. (2002). Online sales: Profit without question. *Tobacco Control, 11*(3), 226-228.

Buhi, E. R., Clayton, H., & Surrency, H. H. (2009). Stalking victimization among college women and subsequent help-seeking behaviors. *Journal Of American College Health: J Of ACH, 57*(4), 419-426.

Bullying. No Way! (2009a). Bullying. No way! Retrieved 27 February, 2009 from http://www.bullyingnoway.com.au/

Bullying. No Way! (2009b). Bullying. No Way!: Ideas box: Strategies map. Retrieved 23 March, 2009 from http://www.bullyingnoway.com.au/docs/strategies-map.rtf

Bullying. No Way! (2009c). Ideas box: School case studies. Retrieved 23 March, 2009 from http://www.bullyingnoway.com.au/ideasbox/schools/

Burgess-Proctor, A., Hinduja, S., & Patchin, J. (2009). *Cyberbullying research summary: Victimization of adolescent girls*. Retrieved 11 March, 2009 from http://www.cyberbullying.us/cyberbullying_girls_victimization.pdf.

Burgess-Proctor, A., Patchin, J., & Hinduja, S. (2009). Cyberbullying and online harassment: Reconceptualizing the victimization of adolescent girls. In V. Garcia & J. Clifford (Eds.), *Female crime victims: Reality considered* (Vol. In print). Upper Saddle River, NJ: Prentice Hall.

Burgess, A. W., & Baker, T. (2002). Cyberstalking. In J. C. W. Boon & L. Sheridan (Eds.), *Stalking and psychosexual obsession: Psychological perspectives for prevention, policing and treatment* (pp. 201-219). Chichester: Wiley.

Burke, V., Beilin, L. J., Durkin, K., Stritzke, W. G., Houghton, S., & Cameron, C. A. (2006). Television, computer use, physical activity, diet and fatness in Australian adolescents. *International Journal of Pediatric Obesity, 1*, 248-255.

Cai, X., & Gantz, W. (2000). Online privacy issues associated with websites for children. *Journal of Broadcasting & Electronic Media, 44(2),* 197-214.

Cameron, K. A., Salazar, L. F., Bernhardt, J. M., Burgess-Whitman, N., Wingood, G. M., & DiClemente, R. J. (2005). Adolescents' experience with sex on the web: Results from online focus groups. *Journal of Adolescence, 28(4),* 535-540.

Campaign for Tobacco-Free Kids. (2005). *Campaign for tobacco-free kids. Speical report: Internet tobacco sales*.

Campbell, A. J., Cumming, S., R., & Hughes, I. (2006). Internet use by the socially fearful: Addiction or therapy? *CyberPsychology & Behavior, 9(1),* 69-81.

Center for Media Education. (2001). *COPPA: The first year - A survey of sites. A report on website compliance*: Center for Media Education.

Chau, M., & Xu, J. (2007). Mining communities and their relationships in blogs: A study of online hate groups. *International Journal of Human-Computer Studies, 65(1),* 57-70.

Chesley, E. B., Alberts, J. D., Klein, J. D., & Kreipe, M. D. (2003). Pro or con? Anorexia nervosa and the Internet. *Journal of Adolescent Health, 32(2),* 123-124.

Child On-line Protection Act (COPA) Commission. (n.d.). *Internet filter effectiveness: testing over and under inclusive blocking decisions of four popular filters*.

Child Welfare Group. (2003). *A preliminary study into the accessibility by minors of pornography in Cambodia*. Retrieved 13 March, 2009 from http://www.licadho-cambodia.org/reports/files/38Pornography%20Report%20Final%20English1.pdf

Childnet International. (2005a). Know IT All. Retrieved 23 March, 2009 from www.childnet.com/kia

Childnet International. (2005b). Jenny's Story background. Retrieved 23 March, 2009 from http://www.childnet-int.org/jenny/background.html

Childnet International. (2005c). Promoting internet safety through the "Jenny's Story" film: Executive summary of pilot study. Retrieved 23 March, 2009 from http://www.childnet-int.org/downloads/js_executivesummary.pdf

Childnet International. (2007a). Parents helped to Know "It All" in their own language. Retrieved 23 March, 2009 from http://www.childnet-int.org/kia/press/pressArticle/160507.aspx

Childnet International. (2007b). Let's fight it together. Retrieved 23 March, 2009 from http://www.digizen.org/cyberbullying/film.aspx

Childnet International. (2007c). A guide to let's fight it together. Retrieved 23 March, 2009 from http://www.digizen.org/downloads/Let'sFightItTogether-guide.pdf

Chisholm, J. F. (2006). Cyberspace violence against girls and adolescent females.*Annals Of The New York Academy Of Sciences, 1087*, 74-89.

Chou, C., & Hsaio, M. (2000). Internet addiction, usage, gratification, and pleasure experience: The Taiwan college students' case. *Computers and Education, 35*, 65-80.

Chriqui, J. F., Ribisl, K. M., Wallace, R. M., Williams, R. S., O'Connor, J. C., & Arculli, R. E. (2008). A comprehensive review of state laws governing Internet and other delivery sales of cigarettes in the United States. *Nicotine and Tobacco Research, 10*(2), 253-265.

CIFAS. (2004). *Decreased frauds - research results December 2004*: CIFAS.

Clarke, R. (1990). Armed Robbery: Final report: Newspaper publicity and bank robberies. Report to the Australiasian Centre for Policing Research. Retrieved 11 March, 2009 from http://www.acpr.gov.au/pdf/ACPR99.pdf

Collins, L., Love, P., Landeldt, B., & Coroneos, P. (2008). *Feasibility study: ISP level content filtering*. Report prepared on behalf of the Internet Industry Association.

Committee on Government Reform. (2003). *Children's exposure to pornography on peer-to-peer networks*: United States House of Representatives.

Commonwealth of Australia (2004). Criminal code amendment: Telecommunications offenses and other measures - Suicide related material offenses. Commonwealth of Australia.

Cross, D., Shaw, T., Hearn, L., Epstein, M., Monks, H., Lester, L., et al. (2009). Australian Covert Bullying Prevalence Study (ACBPS). Child Health Promotion Research Centre, Edith Cowan University, Perth.

Cuganesan, S., & Lacey, D. (2003). *Identity fraud in Australia: An evaluation of its nature, cost and extent*. Securities Industries Research Centre of Asia-Pacific, Sydney.

De Souza, Z., & Dick, G. N. (2008). Information disclosure on MySpace: the what, the why and the implications. *Pastoral Care in Education, 26(3),* 143-157.

Department for Children Schools and Families. (2007a). Cyberbullying - Safe to Learn: embedding anti-bullying work in schools. Retrieved 23 February, 2009 from http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Department for Children Schools and Families. (2007b). Cyberbullying, a whole-school community issue: summary. Retrieved 23 March, 2009 from http://www.digizen.org/downloads/cyberbullyingOverview.pdf

Department of Education and Training. (2006). *Safe schools are effective schools*. Retrieved 23 March 2009 from http://www.eduweb.vic.gov.au/edulibrary/public/stuman/wellbeing/SafeSchoolsStrategy.pdf.

Department of Education and Training. (2008). *Click: A technology guide for parents*. Retrieved 23 March 2009 from http://www.schools.nsw.edu.au/media/downloads/schoolsweb/news/technology/click.pdf.

Department of Education and Training. (2009a). *Classroom Management in Schools: Resourcing the curriculum - cyberbullying*. Retrieved 23 March 2009 from http://www.det.wa.edu.au/education/cmis/eval/curriculum/ict/cyberbullying/.

Department of Education and Training. (2009b). Engage. Retrieved 23 March, 2009 from http://www.education.tas.gov.au/school/parents/engage/Engage-Issue-2-web.pdf

Descy, D. E. (2006). Keeping Kids Safe Online. *TechTrends: Linking Research and Practice to Improve Learning, 50(5),* 3-4.

Dooley, J. J., Pyzalski, J., & Cross, D. (in press). Cyberbullying versus face-to-face bullying: A review of the similarities and differences. *Journal of Psychology*.

Doran, K. (2008). The economics of pornography. Retrieved 2 May, 2009 from http://www.winst.org/family_marriage_and_democracy/social_costs_of_pornography/Doran%20-%20%20Economics%20of%20Pornography.pdf

Douglas, A. C., Mills, J. E., Niang, M., Stepchenkova, S., Byun, S., Ruffini, C., et al. (2008). Internet addiction: Meta-synthesis of qualitative research for the decade 1996-2006. *Computers in Human Behavior, 24*, 3027-3044.

Edelman, B. (2009). Red light states: Who buys online adult entertainment? *Journal of Economic Perspectives, 23(1),* 209-220.

Epstein, M. (2006). *Supportive Schools Project*. Perth: WA: Child Health Promotion Research Centre, Edith Cowan University.

Erdur-Baker, Ö. (under review). *Cyber Bullying and Its Correlation to Traditional Bullying, Gender, and Frequent and Risky Usage of Internet Mediated Communication Tools.* Unpublished manuscript.

Federal Trade Commission. (1998). *Title 13 - Children's Online Privacy Protection*. Retrieved 21 March 2009 from http://www.ftc.gov/ogc/coppa1.htm.

Federal Trade Commission. (2002). *Protecting children's privacy under COPPA: A survey on compliance (staff report)*. Retrieved 15 April, 2009 from http://www.ftc.gov/os/2002/04/coppasurvey.pdf

Ferguson, C. J. (2007). The good, the bad and the ugly: A meta-analytic review of positive and negative effects of violent video games. *Psychiatric Quarterly, 78*, 309-316.

Finkelhor, D., & Baron, L. (1986). High-risk children. In D. Finkelhor (Ed.), *A source on child sexual abuse* (pp. 60-88). Beverly Hills, CA: Sage.

Finkelhor, D., Mitchell, K., & Wolak, J. (2000). *Online victimization: A report of the nation's youth*. Retrieved 19 April, 2009 from http://www.missingkids.com/en_US/publications/NC62.pdf.

Finn, J. (2004). A survey of online harassment at a university campus.*Journal of Interpersonal Violence, 19(4),* 468-483.

Fisher, B., Cullen, F., & Turner, M. (2000). *The sexual victimization of collece women*: U.S. Department of Justice, Office of Justice Programs.

Fix, B. V., Zambon, M., Higbee, C., Cummings, K. M., Alford, T., & Hyland, A. (2006). Internet cigarette purchasing among ninth grade students in western New York: 2000-2001 vs. 2004-2005. *Preventative Medicine, 43(3),* 191-195.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. *Youth and Society, 38*(2), 135-154.

Flood, M. (2007). Exposure to pornography among youth in Australia. *Journal of Sociology, 43(1),* 45-60.

Flood, M. (in press). The harms of pornography exposure among children and young people. *Child Abuse Review*.

Flood, M., & Hamilton, C. (2003). *Youth and pornography in Australia: Evidence on the extent of exposure and likely effects*: The Australia Institute.

Fox, N., Ward, K., & O'Rourke, A. (2005). Pro-anorexia, weight-loss drugs and the Internet: An 'anti-recovery' explanatory model of anorexia. *Sociology of Health & Illness, 27(7),* 944-971.

Francoeur, R. (2004). Premarital sex before age 15. In R. Francoeur & R. J. Noonan (Eds.), *The continuum complete international encyclopedia of sexuality* (pp. 1187-1196). New York: Continuum International.

Freeman, B., & Chapman, S. (2007). Is "You Tube" telling or selling you something? Tobacco content on the YouTube video-sharing website. *Tobacco Control, 16*, 207-210.

Freeman, B., & Chapman, S. (2008). Gone viral? Heard the buzz? A guide for public health practitioners and researchers on how Web 2.0 can subvert advertising restrictions and spread health information. *Journal of Epidemiological Community Health, 62*, 778-782.

Freeman, B., & Chapman, S. (2009). Open source marketing: Camel cigarette brand marketing in the Web 2.0 world. *Tobacco Control*.

Funk, J. B., Baldacci, H. B., Pasold, T., & Baumgardner, J. (2004). Violence exposure in real-life, video games, television, movies, and the internet: Is there desensitization? *Journal of Adolescence, 27(1),* 23-39.

Gennaro, C. D., & Dutton, W. H. (2007). Reconfiguring friendships: Social relationships and the Internet. *Information, Communication and Society, 10(5),* 591-618.

Gentile, D. A., Saleem, M., & Anderson, C. A. (2007). Public policy and the effects of media violence on children.*Social Issues and Policy Review, 1*, 15-61.

Gerstenfeld, P. B., Grant, D. R., & Chiang, C. (2003). Hate online: A content analysis of extremist Internet sites. *Analyses of Social Issues and Public Policy, 3(1),* 29-44.

GetNetWise. (2008). GetNetWise. Retrieved 23 March, 2009 from http://kids.getnetwise.org/tools/

Greenfield, P. M. (2004). Inadvertent exposure to pornography on the Internet: Implications of peer-to-peer file-sharing networks for child development and families. *Journal of Applied Developmental Psychology, 25(6),* 741-750.

Griffiths, M., & Wood, R. T. (2000). Risk factors in adolescence: The case of gambling, videogame playing, and the Internet. *Journal of Gambling Studies, 16(2-3),* 199-225.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks*. Paper presented at the Workshop on Privacy in the Electronic Society 2005.

Grunwald, M., Wesemann, D., & Rall, L. (2008). Pro-anorexia websites: An underestimated and unchartered danger. *Child and Adolescent Mental Health, 13(2),* 96-98.

Hakala, P. T., Rimpela, A. H., Saarni, L. A., & Salminen, J. J. (2006). Frequent computer-related activities increase the risk of neck-shoulder and lower back pain in adolescents. *European Journal of Public Health, 16(5),* 536-541.

Harmon, A. (2004, August 26). Internet gives teenage bullies weapons to wound from afar. *The New York Times*. Retrieved April 1, 2009 from: http://www.nytimes.com/2004/08/26/education/26bully.html

Hasebrink, U., Livingstone, S., & Haddon, S. (2008). *Comparing children's online oppurtunities and risks across Europe: cross-national comparisions for EU Kids Online*: London: EU Kids Online (Deliverable D3.2).

Hinduja, S., & Patchin, J. (2007). Offline consequences of online victimization: School violence and delinquency. *Journal of School Violence, 6(3),* 89-112.

Hinduja, S., & Patchin, J. (2008a). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29(2),* 129-156.

Hinduja, S., & Patchin, J. (2008b). Personal information of adolescents on the Internet: A quantitative content anlysis of MySpace. *Journal of Adolescence, 31*, 125-146.

Hinduja, S., & Patchin, J. (2009a). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage.

Hong, T., & Cody, M. J. (2002). Presence of pro-tobacco messages on the web. *Journal of Health Communication, 7*, 273-307.

Huesmann, L. R. (2007). The impact of electronic media violence: scientific theory and research. *Journal of Adolescent Health, 41*(6), S6-13.

Huffaker, D. (2006). *Teen blogs exposed: The private lives of teens made public.* Paper presented at the American Association for the Advancement of Science.

Hunter, C. (2000). Internet Filter EffectivenessTesting Over- and Underinclusive Blocking Decisions of Four Popular Web Filters. *Social Science Computer Review, 18(2),* 214-222.

Identity Theft Resource Centre. (2007). Fact Sheet 120 - Identity Theft and Children. Retrieved 31 March, 2009 from http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_120.shtml

IDology Inc. (2009). IDology Expands on Its Member Statement to Internet Safety Technical Task Force's Final Report. Retrieved 17 April, 2009 from http://theidspace.idology.com/archives/100

Internet Safety Technical Task Force. (2008). *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force*: Harvard University.

Jacobs, K., & Baker, N. (2002). The association between children's computer use and musculoskeletal discomfort. *Work, 18*, 221-226.

Jang, K. S., Hwang, S. Y., & Choi, J. Y. (2008). Internet addiction and psychiatric symptoms among Korean adolescents.*Journal of School Health, 78(3),* 165-172.

Javelin Strategy. (2007). *2007 Identity fraud survey report: Identity fraud is dropping, continued vigilance necessary*: Javelin Strategy & Research.

Jensen, J. A., Hickman, N. J., & Landrine, H. (2004). Availability of tobacco to youth via the Internet. *Journal of the Amercian Medical Association, 291(15),* 1837-1838.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health, 78(9),* 496-506.

Kaiser Family Foundation. (2001). *Generation Rx.com: How young people use the Internet for health information*. Menlo Park, CA: Henry J. Kaiser Family Foundation.

Kaltiala-Heino, R., Lintonen, T., & Rimplela, A. (2004). Internet addiction? Potentially problematic use of the Internet in a population of 12-18 year-old adolescents. *Addiction Research and Theory, 12(1),* 89-96.

Kautianen, S., Koivusilta, L., Lintonen, T., Virtanen, S., & Rimpela, A. (2005). Use of information and communication technology and prevalence of overweight and obesity among adolescents. *International Journal of Obesity, 29(8),* 925-933.

Keski-Rahkonen, A., & Tozzi, F. (2005). The process of recovery in eating disorder sufferers' own words: An Internet-based study. *International Journal of Eating Disorders, 37*, S80-S86.

Kideo Player. (2009). Kideo Player. Retrieved 23 March, 2009 from www.kideoplayer.com

Kirsh, S. J. (2006).*Children, adolescents, and media violence: A critical look at the research*. Longdon: Sage.

Knowles, J. H., Wanke, K., & Kawachi, I. (2004). Internet sales of tobacco: Heading off new e-pidemic. *Journal of Public Health Policy, 25(1),* 58-68.

Ko, C., Yen, J., Yen, C., Lin, H., & Yang, M. (2007). Factors predictive for incidence and remission of Internet addiction in young adolescents: A prospective study. *CyberPsychology & Behavior, 10(4),* 545-551.

Ko, C., Yen, J., Liu, S., Huang, C., & Yen, C. (in press). The associations between

aggressivebehaviors and Internet addiction and online activities in adolescents. *Journal of Adolescent Health*.

Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health, 41*, S22-S30.

Kowalski, R. M., Limber, S. P., &Agaston, P. W. (2008). *Cyber Bullying: Bullying in the digital age*. Malden, MA: Wiley-Blackwell.

Kranich, N. (2004). Why filters won't protect children or adults. *Library Administration & Management, 18(1),* 14-18.

Kraus, S. W., & Russell, B. (2008). Early sexual experiences: The role of internet access and sexually explicit material. *Cyberpsychology & Behavior, 11(2),* 162-168.

Lang, R. A., & Frenzel, R. R. (1988). How sex offenders lure children. *Annals of Sex Research, 1(2),* 303-317.

Lanning, J. (2002). Cyberstalking awareness and education. Retrieved 23 March, 2009, from http://www.acs.ucalgary.ca/-dabrent/380/webproj/jessica.html

Laughren, J. (2000). Cyberstalking awareness and education. Retrieved 23 March, 2009, from http://www.acs.ucalgary.ca/-dabrent/380/webproj/jessica.html

Laulik, S., Allam, J., & Sheridan, L. (2007). An investigation into maladaptive personality functioning in Internet sex offenders. *Psychology, Crime & Law, 13(5),* 523-535.

Lee, J. (Feb 17, 2005). Teens with mobiles steal thunder from 3G revolution. The Sydney Morning Herald. Retrieved 29 April, 2009 from http://www.smh.com.au/articles/2005/02/16/1108500153501.html

Leets, L. (2001). Responses to internet hate sites: Is speech too free in cyberspace? *Communication Law and Policy, 6(2),* 287-317.

Lenhart, A., & Madden, M. (2007). *Teens, privacy and online social networks*: PEW Internet and American Life Project.

Lewandowski, J. L. (2003). Stepping off the sidewalk: an examination of the data collection techniques of Websites visited by children. *Journal of School Violence, 2(1),* 19-63.

Li, Q. (2005). Cyber-bullying in schools: A research of gender differences. *School Psychology International, 27(2),* 157-170.

Li, Q. (2006a). Cyberbullying in schools: a research of gender differences. *School Psychology International, 27(2),* 157-170.

Li, Q. (2007a). Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology, 23(4),* 435-454.

Li, Q. (2007b). New bottle but old wine: A reserach of cyberbullying in schools. *Computers in Human Behavior, 23*, 1777-1791.

Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research, 50(3)*, 223-234.

Livingstone, S., & Bober, M. (2005). *UK children go online: Final report of key findings*. London, UK: LSE Research Online.

Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's Internet use. *Journal of Broadcasting & Electronic Media, 52(4),* 581-599.

Lo, V., & Wei, R. (2005). Exposure to Internet pornography and Taiwanese adolescents' sexual attitudes and behavior. *Journal of Broadcasting and Electronic Media, 49(2),* 221-237.

Lo, W., & Wei, R. (2002). Third-person effect, gender and pornography on the Internet. *Journal of Broadcasting & Electronic Media, 46*, 13-33.

Lodge, J., & Frydenberg, E. (2007). Cyber-Bullying in Australian schools: profiles of adolescent coping and insights for school practitioners. *The Australian Educational and Developmental Psychologist, 24(1),* 45-58.

Lucks, B. D. (2001). Electronic crime, stalkers and stalking: relentless pursuit, harassment and terror online in cyberpsace. In J. A. Davis (Ed.), *Stalking Crimes and Victim Protection: Prevention, Intervention, Threat Assessment, and Case Management*: CRC Press.

Lwin, M., Stanaland, A., & Miyazaki, A. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing, 84(2),* 12.

Maharaj, G. (23 January 1999). Chilling cyberstalking case illustrated new breed of crime. *Los Angeles Times.* Retrieved 29 March, 2009 from http://www.infowar.com/index.shtml?http://www.infowar.com/law/99/law_012799aj.shtml

Maher, D. (2008). Cyberbullying: An ethnographic case study of one Australian upper primary school class. *Youth Studies Australia, 27(4),* 50-57.

Main, G., & Robson, B. (2001). *Scoping identity fraud*. Canberra: Attorney General's Department.

Malamuth, N., Addison, T., & Koss, M. (2000). Pornography and sexual aggression: Are there reliable effects and can we understand them? *Annual Review of Sex Research, 11*, 26-91.

Malamuth, N. M., & Impett, E. A. (2001). Research on sex and media: What do we know on the effects on children and adolescents? In D. G. Singer & J. L. Singer (Eds.), (pp. 269-287). Thousand Oaks: Sage.

Malone, R. E., & Bero, L. A. (2000). Cigars, youth, and the Internet link. *American Journal of Public Health, 90(5),* 790-792.

Maury, S. (2004). Developments in combating cyberstalking in Australia. *Internet Law Bulletin, 6(10),* 126-128.

McGrath, M. G., & Casey, E. (2002). Forensic psychiatry and the internet: practical perspectives on sexual predators and obsessional harassers in cyberspace. *The Journal Of The American Academy Of Psychiatry And The Law, 30(1),* 81-94.

McKee, A., Albury, A., & Lumby, C. (2008). *The porn report*. Melbourne: Melbourne University Press.

Mehta, M. D. (2001). Pornography in Usenet: A study of 9,800 randomly selected images. *CyberPsychology & Behavior, 4(6)*, 695-703.

Mehta, M. D., & Plaza, D. E. (1997). Content analysis of pornographic images available on the Internet. *The Information Society, 13(2),* 153-161.

Mesch, G. S. (2009). Social bonds and Internet pornographic exposure among adolescents. *Journal of Adolescence, 32*, 601-618.

Mishara, B. L., & Weisstub, D. N. (2007). Ethical, Legal, and Practical Issues in the Control and Regulation of Suicide Promotion and Assistance over the Internet *Suicide & Life - Threatening Behavior 37(1),* 58.

Mitchell, K., Finkelhor, D., & Wolak, J. (2001). Risk factors for and impact of online sexual solicitation of youth. *Journal of the American Medical Association, 285(23),* 3011-3014.

Mitchell, K., Finkelhor, D., & Wolak, J. (2005b). Police posing as juveniles online to catch sex offenders: Is it working? *Sexual Abuse: A Journal of Research and Treatment, 17(3),* 241-267.

Mitchell, K., & Ybarra, M. (2007). Online behavior of youth who engage in self-harm provides clues for preventive intervention. *Preventative Medicine, 45*, 392-396.

Mitchell, K. J., Becker-Blease, A., & Finkelhor, D. (2005a). Inventory of Problematic Internet Experiences Encountered in Clinical Practice. *Professional Psychology : Research and Practice, 36(5),* 498-509.

Mitchell, K. J., Finkelhor, D., & Becker-Blease, K. A. (2007a). Linking youth internet and conventional problems: findings from a clinical perspective. *Journal of Aggression, Maltreatment & Trauma, 15(2),* 39-58.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003a). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact, and prevention. *Youth and Society, 34(3),* 330-358.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2005c). Protecting youth online: Family use of filtering and blocking software. *Child Abuse & Neglect, 29(7),* 753-765.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007b). Online requests for sexual pictures from youth: Risk factors and incident characteristics. *Journal of Adolescent Health, 41*(2), 196-203.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2007d). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the Internet. *Journal of Adolescent Health, 40(2),* 116-126.

Model Criminal Law Officers' Committee. (2008). *Final report: Identity crime*: Standing Committee of Attorneys-General. Retrieved March 24, 2009 from http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_FinalReport-IdentityCrime-March2008

Molitor, F., & Hirsh, K. W. (1994). Children's toleration of real life aggression after exposure to media violence: A replication of the Drabman and Thomas studies. *Child Study Journal, 24*, 191-207.

Moscardelli, D. M., & Divine, R. (2007). Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal, 35(3),* 232-252.

Moyer, M., Haberstroh, S., & Marbach, C. (2008). Self-injurious behaviors on the Net: A survey of resources for school counsellors. *Professional School Counseling, 11(5),* 277-284.

Murray, C. D., & Fox, J. (2006). Do Internet self-harm discussion groups alleviate or exacerbate self-harming behaviour? *Australian e-Journal for the Advancement of Mental Health, 5(3),* 1-9.

Murray, L. (23 June, 2006). Parents get free software to trap net nasties. *Sydney Morning Herald.* Retrieved 2 May, 2009 from http://www.smh.com.au/news/technology/free-software-to-trap-internet-nasties/2006/06/21/1150845247846.html

National Center for Missing & Exploited Children and Boys & Girls Clubs of America. (2006). Netsmartz Teens: I-360. Retrieved 23 March, 2009 from http://ext.bgcayouthnet.org/outsidesites/nsteens/index.htm

National Crime Prevention Council. (2008). Stop cyberbullying before it starts. Retrieved 23 March, 2009 from http://www.ncpc.org/topics/by-audience/parents/bullying/cyberbullying/cyberbullying.pdf

NetAlert. (2005a). *CyberQuoll - Teacher's guide*. Retrieved 23 March 2009 from http://www.netalert.gov.au/__data/assets/pdf_file/0013/4126/02451-CyberQuoll-Teachers-Guide.pdf.

NetAlert. (2005b). *CyberQuoll parent's guide*. Retrieved 23 March 2009 from http://www.netalert.gov.au/__data/assets/pdf_file/0010/4132/02353-CyberQuoll-Parents-Guide.pdf.

NetAlert. (2006a). *Teacher's guide: Internet safety education for secondary school students*. Retrieved 23 March, 2009 from

www.netalert.gov.au/__data/assets/pdf_file/0015/4056/cybernetrix_teacher_guide.pdf.

NetAlert. (2006b). *A parent's guide to CyberNetrix*. Retrieved 23 March 2009 from http://www.netalert.gov.au/__data/assets/pdf_file/0014/4055/CyberNetrix_Parent_Guide.pdf.

NetAlert. (2007a). *A teacher's guide to internet safety: How to teach internet safety in our schools*. Retrieved 23 March, 2009 from www.netalert.gov.au/__data/assets/pdf_file/0019/1819/01427-A-Teachers-Guide-to-Internet-Safety.pdf

NetAlert. (2007b). Paedophiles and online grooming. Retrieved 15 April, 2009 from http://www.netalert.gov.au/advice/publications/information_sheets/paedophiles_and_online_grooming.html

NetAlert. (2008a). *CyberQuoll*. Retrieved 23 March 2009 from www.cyberquoll.com.au

NetAlert. (2008b). *CyberNetrix*. Retrieved 23 March 2009 from www.cybernetrix.com.au.

NetRatings Australia. (2005). *Kidsonline@home:Internet use in Australian homes.* Sydney: Australian Broadcasting Authority and NetAlert Limited.

O'Connell, R. (2003). *A typology of child cybersexploitation and online grooming practices*: University of Central Lancashire: Preston.

Office of the Privacy Commissioner. (2007). *Community attitudes to privacy*: Office of the Privacy Commissioner.

Ogilvie, E. (2000). *The Internet and cyberstalking.* Paper presented at the Criminal Justice Responses Conference, Sydney.

Okrent, D. (1999). Raising kids online: What can parents do? *Time*.

Olweus, D. (1993a). Bullies on the playground: the role of victimisation. In C. Hart (Ed.), *Children on Playgrounds*: SUNY Press.

Olweus, D. (1993b). *Bullying at school: what we know and what we can do*. Oxford: Blackwell.

Osterman, K., Blorkqvist, K., Lagerspetz, K.M.J.,Kaukiainen, A., Landau,S.F., Fraczek,A., Caprara, G.V. (1998). Cross-cultural evidence of female indirect aggression. *Aggressive Behavior, 4*, 1-8.

Palfrey, J., Sacco, D., Boyd, D., & Internet Safety Technical Task Force. (2008). *Enhancing Child Safety & Online Technologies*: Berkman Center for Internet & Society: Harvard University.

Pardun, C. J., L'Engle, K. L., & Brown, J. D. (2005). Linking exposure to outcomes: Early adolescents' consumption of sexual content in six media. *Mass Communication and Society, 8(2),* 75-91.

Park, S. K., Kim, J. Y., & Cho, C. B. (2008). Prevalence of Internet and correlations with family factors among South Korean adolescents. *Adolescence, 43*, 895-900.

Parliamentary Joint Committee on the Australian Crime Commission. (2004). *Cybercrime*. Retrieved March 29, 2009 from http://www.aph.gov.au/Senate/committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf.

Patchin, J., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4(2),* 148-169.

Pelling, N. J. (2004). Children and Adolescents: The Impact of the Internet. *Australian Journal of Guidance & Counselling, 14(2),* 176-186.

Peter, J., & Valkenburg, P. (2008). Adolescents' exposure to sexually explicit internet material, sexual uncertainty, and attitudes toward uncommitted sexual exploration: is there a link? *Communication Research, 35(5),* 579-601.

Peter, J., & Valkenburg, P. M. (2006). Adolescents' exposure to sexually explicit material on the Internet. *Communication Research, 33(2),* 178-204.

Peter, J., Valkenburg, P. M., & Schouten, A. (2005). *Charcteristics and motives of adolescents: Talking with strangers on the Internet and its consequences*. Paper presented at the International Communication Association.

Philips, F., & Morrissey, G. (2004). Cyberstalking and cyberpredators: A threat to safe sexuality on the Internet. *Convergence: The International Journal of Research into New Media Technologies, 10(1),* 66-79.

Piazza, P. (2004). Fighting Online Sex Crimes. *Security Management, 48(2),* 39.

Pierce, T. A. (2006). Talking to strangers on MySpace: Teens' use of social networking sites and the potential dangers. *Journal of Media Psychology, 11*(3). http://www.calstatela.edu/faculty/sfischo/myspace.htm

Pierce, T. A. (2007). X-posed on MySpace: A content analysis of 'MySpace' social networking sites. *Journal of Media Psychology, 12*(1). http://www.calstatela.edu/faculty/sfischo/X-posed_on_%20MySpace.htm

Polman, H., de Castro, B. O., & van Aken, M. (2008). Experimental study of the differential effects of playing versus watching violent video games on children's aggressive behaviour.*Aggressive Behavior, 34,* 256-264.

Punamaki, R., Wallenius, M., Nygard, C., Saarni, L., & Rimpela, A. (2007). Use of information and communication (ICT) and perceived health in adolescence: The role of sleeping habits and waking-time tiredness. *Journal of Adolescence, 30*, 569-585.

Purcell, R., Flower, T., & Mullen, P. E. (2009). *Adolescent stalking: Offense characteristics and effectiveness of intervention orders*. *Trends and Issues in Crime and Criminal Justice,* 369. Canberra, ACT.

Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. *Developmental Psychology, 43(3),* 564-575.

Ribisl, K. M. (2003). The potential of the Internet as a medium to encourage and discourage youth tobacco use: Role of the Internet. *Tobacco Control, 12(2),* 48-71.

Ribisl, K. M., Kim, A. E., & Williams, R. S. (2002). Are the sales practices of Internet cigarette vendors good enough to prevent sales to minors? *American Journal of Public Health, 92(6),* 940-941.

Ribisl, K. M., Williams, R. S., & Kim, A. E. (2003). Internet sales of cigarettes to minors. *Journal of American Medical Association, 290(10),* 1356-1359.

Richardson, C. R., Resnick, P. J., Hansen, D. L., Derry, H. A., & Rideout, V. J. (2002). Does pornography-blocking software block access to health information on the Internet? *Journal of the American Medical Association, 288(22),* 2887-2894.

Rimm, M. (1995). Marketing pornography on the information superhighway: A survey of 917, 410 images, descriptions, short stories, and animations downloaded 8.5 million times by consumers in over 2000 cities in forty countries, provinces, and territories. *Georgetown Law Review, 83*, 1849-1934.

Roberts, D. F., Foehr, U. G., & Rideout, V. (2005). Generation M: Media in the lives of 8-18. Retrieved March 26, 2009 from http://www.kff.org/entmedia/upload/Generation-M-Media-in-the-Lives-of-8-18-year-olds-Report.pdf

Rodham, K., Gavin, J., & Miles, M. (2007). I hear, I listen and I care: A qualitative investigation into the function of a self-harm message board. *Suicide and Life-Threatening Behavior, 37(4),* 422-430.

Rogosch, F. A., Cicchetti, D., & Aber, J. L. (1995). The role of child maltreatment in early deviations in cognitive and affective processing abilities and later peer relationship problems. *Developmental Psychology, 7*, 591-609.

Rosen, L. D., Cheever, N. A., & Carrier, L. M. (2008). The association of parenting style and child age with parental limit setting and adolescent MySpace behavior. *Journal of Applied Developmental Psychology, 29(6),* 459-471.

Royal Australasian College of Physicians. (2004). Children and the media: Advocating for the future. Retrieved 11 March, 2009 from http://72.14.235.132/search?q=cache:pF9XAnclXBQJ:www.racp.edu.au/download.cfm%3FDownloadFile%3DA8AAE08D-2A57-5487-

DCDDF906EED5AC32+Children+and+the+media:+advocating+for+the+future&cd=1&hl=en&ct=clnk&gl=au

Russell, M. (2008). Net blamed as 10,000 kids turn to crime. Retrieved 2 February, 2009 from http://www.theage.com.au/national/net-blamed-as-10000-kids-turn-to-crime-20080802-3p00.html

Sabina, C., Wolak, J., & Finkelhor, D. (2008). The nature and dynamics of internet pornography exposure for youth. *Cyberpsychology & Behavior: The Impact Of The Internet, Multimedia And Virtual Reality On Behavior And Society, 11(6),* 691-693.

Schafer, J. A. (2002). Spinning the web of hate. Web-base hate propagation by extremist organizations. *Journal of Criminal Justice and Popular Culture, 9*, 69-88.

Schepis, T. S., Marlowe, D. B., & Forman, R. F. (2008). The availability and portrayal of stimulamts over the Internet.*Journal of Adolescent Health, 42*, 458-465.

Schmidtke, A., & Schaller, S. (2000). The role of mass media in suicide prevention. In K. Hawton& K. van Heeringen (Eds.), *The international handbook of suicide and suicide attempts*. New York: Wiley.

Seay, A., & Kraut, R. E. (2007). *Project massive: Self-regualtion and problematic use of online gaming*. Paper presented at the CHI Games Proceedings.

Shade, L. R. (2003). *Weborexics: The ethical issues surrounding pro-ana websites*. Paper presented at the Fifth International Conference on Computer Ethics-Philosophical Enquiry, Chestnut Hills, MA.

Shapira, N., Lessing, M., Goldsmith, T., Szabo, S., Lazoritz, M., Gold, M., et al. (2003). Problematic Internet use: Proposed classification and diagnostic criteria. *Depression and Anxiety, 47(4),* 207-216.

Shariff, S., &Gouin, R. (2005). *Cyber-dilemmas: gendered hierarchies, free expression and cyber-safety in schools*. Paper presented at the Oxford Internet Institute (OII), Oxford University Conference.

Sheehan, P. W. (1997). *The effects of watching violence in the media: Policy, consensus, and censorship*. Paper presented at the Violence, Crime and the Entertainment Media.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime and Law, 13(6),* 627-640.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another type of bullying? *Scandinavian Journal of Psychology, 49*, 147-154.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49(4),* 376-385.

Snyder, H. N. (2000). *Sexual assult of young children as reported to law enforcement: Victim, incident, and offender characteristics*. Washington, DC: U.S. Department of Justice.

Solicitor General Canada, & U.S. Department of Justice. (2002). *Public advisory: Special report for consumers on Identity theft.*

Soole, D. W., Mazerolle, L., & Rombouts, S. (2008). School-Based Drug Prevention Programs: A Review of What Works. *The Australian and New Zealand Journal of Criminology, 41(2),* 259-286.

Southern Poverty Law Center. (2004). Hate groups, militias on rise as extremists stage comeback. Retrieved 6 March, 2009 from http://www.splcenter.org/center/splcreport/article.jsp?aid=71

Spence-Diehl, E. (2003). Stalking and technology: The double-edged sword. *Journal of Technology in Human Services, 22(1),* 5-18.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media and Society, 4(1),* 71-92.

Stahl, C., & Fritz, N. (1999). Internet safety: Adolescents' self-report. *Journal of Adolescent Health, 31*, 7-10.

Stanley, J. (2001). *Child abuse and the Internet*. Retrieved 30 March, 2009 from www.aifs.gov.au/nch/pubs/issues/issues15/issues15.html

Subrahmanyam, K., Smahel, D., & Greenfield, P. (2006). Connecting developmental constructions to the Internet identity presentation and sexual exploration in online chatrooms. *Developmental Psychology, 42(3),* 395-406.

Taylor, M., & Quayle, E. (2008). *Child pornography: An Internet crime*. East Sussex, UK: Brunner-Routledge.

The New York Academy of Medicine. (2009). The New York Academy of Medicine (Publication.:http://www.nyam.org/library/pages/current_grey_literature_report

Thomas, J. (1996). When cybersearch goes awry: The ethics of the Rimm 'cyberporn' study. *The Information Society, 12*(2), 189-198.

Topçu, C., Erdur-Baker, Ö., & Çapa-Aydin, Y. (2008). Examination of cyberbullying experiences among Turkish students from different school types. *CyberPsychology & Behavior, 11(6),* 643-648.

Tsai, C., & Lin, S. S. J. (2003). Internet addiction of adolescents in Taiwan: An interview study. *CyberPsychology & Behavior, 6(6),* 649-652.

Turow, J. (2001). *Privacy policies on children's websites: Do they play by the rules?* : The Annenberg Public Policy Center of the University of Pennsylvania.

Turtle, M. (2007). Pro-smoking 'ads' target youth market on YouTube. *ABC News*.

Tynes, B., Reynolds, L., & Greenfield, P. M. (2004). Adolescence, race, and ethnicity on the Internet: A comparison of discourse in monitored versus unmonitored chat rooms. *Journal of Applied Developmental Psychology, 25*, 667-684.

U.S. Department of Justice. (2001). *Drugs and the Internet: An overview of the threat to America's youth*. Retrieved 5 March, 2009 from http://www.usdoj.gov/ndic/pubs/682/682p.pdf

U.S. Department of Justice. (2002). *Drugs, youth, and the Internet*. Retrieved 5 March, 2009 from http://www.usdoj.gov/ndic/pubs2/2161/2161p.pdf.

Unger, J. B., Rohrbach, L. A., & Ribisl, K. M. (2001). Are adolescents attempting to buy cigarettes on the Internet? *Tobacco Control, 10*, 360-363.

Vandebosch, H., & van Cleemput, K. (2008). Defining cyberbullying: a qualitative research into the perceptions of youngsters. *CyberPsychology & Behaviour, 11(4),* 499-503.

Wales, E. (2003). Identity Theft. *Computer Fraud & Society, 2*, 5-7.

Wallace, J., &Mangan, M. (1996). *Sex, laws, and cyberspace*. NY: Henry, Holt, and Company.

Wallis Consulting Group. (2007). *Community attitudes to privacy 2007*. Sydney: Office of the Privacy Commissioner.

Wan, C., & Chiou, W. (2007). The motivations of adolescents who are addicted to online games: A cognitive perspective. *Adolescence, 42(165),* 179-197.

Wang, R., Bianchi, S. M., & Raley, S. B. (2005). Teenagers' Internet use and family rules: A research note. *Journal of Marriage and the Family, 67*, 1249-1258.

Whitlock, J. L., Powers, J. L., & Eckenrode, J. (2006). The virtual cutting edge: The Internet and adolescent self-injury. *Developmental Psychology, 42(3),* 407-417.

Widyanto, L., & Griffiths, M. (2006). Internet addiction: A critical review. *International Journal of Mental Health Addiction, 4*, 31-51.

Willard, N. (2009). Research that is "outdated and inadequate?": An analysis of the Pennsylvania Child Predator Unit arrests in response to Attorney General criticism of the Berkman Task Force Report. Retrieved 19 April, 2009 from: http://www.cyberbully.org/PDFs/papredator.pdf

Willard, N. E. (2005). An educator's guide to cyber bullying and cyberthreats: Responding to the challenge of online social agression, threats, and distress. Retrieved 23 March, 2009 from http://www.cyberbully.org/docs/cbcteducator/pdf

Williams, A. L., & Merten, M. J. (2008). A review of online social networking profiles by adolescents: implications for future research and intervention. *Adolescence, 43(170),* 253-274.

Williams, K. R., & Guerre, N. G. (2007). Prevalence and predictors of Internet bullying. *Journal of Adolescent Health, 41*, S14-S21.

Wilson, P., & Nugent, S. (1987). *Sexually explicit and violent media material: Research and policy implications*. *Trends and Issues in Crime and Criminal Justice*, (No. 9). Woden, Australian Capital Territory: Australian Institute of Criminology.

Windham, C. (2008). *The changing landscape of adolescent Internet communication and its relationship to psychosocial adjustment and academic performance*. Washington, D.C.: George Washington University.

Wishart, J., Andrews, J., & Ching Yee, W. (2005). *Evaluation of the 'Getting to Know IT All' presentation as delivered in UK schools during November 2005*: Bristol University.

Wolak, J., Finkelhor, D., & Mitchell, K. (2007a). 1 in 7 youth: The statistics about online solicitations. Retrieved 22 April, 2009 from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/1in7Youth.pdf

Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health, 35(5),* 424.

Wolak, J., Finkelhor, D., & Mitchell, K. (2008a). Is talking online to unknown people always risky? Distinguishing online interaction styles in a national sample of youth

Internet users. *CyberPsychology&Behavior: The Impact Of The Internet, Multimedia And Virtual Reality On Behavior And Society, 11(3),* 340-343.

Wolak, J., Finkelhor, D., Mitchell, K., & Ybarra, M. (2008b). Online "predators" and their victims: myths, realities, and implications for prevention and treatment. *The American Psychologist, 63(2),* 111-128.

Wolak, J., Mitchell, K., & Finkelhor, D. (2002). Close online relationships in a national sample of adolescents. *Adolescence, 37(147),* 441-455.

Wolak, J., Mitchell, K., & Finkelhor, D. (2003b). *Internet sex crimes against minors: The response of law enforcement*. Alexandria, VA: National Center for Missing & Exploited Children.

Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization: 5 years later*: Alexandria, VA: National Center for Missing & Exploited Children.

Wolak, J., Mitchell, K., & Finkelhor, D. (2007b). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *Journal of Adolescent Health, 41*, S51-S58.

Wolak, J., Mitchell, K., & Finkelhor, D. (2007c). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *Pediatrics, 119*(2), 247-257.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2003a). Escaping or connecting?Characteristics of youth who form close online relationships. *Journal of Adolescence, 26(1),* 105-119.

Wolfe, D. A., Jaffe, P. G., & Crooks, C. V. (2006). *Adolescent risk behaviours: Why teens experiment and strategies to keep them safe*. New Haven, CT: Yale University Press.

Woollard, J., Wickens, C., Powell, K., Russell, T. (2007). *E-safety: evaluation of key stage 3 materials for initial teacher education*: Childnet International.

Yao-Guo, G., Lin-Yan, S. & Feng-Lin, C. (2006) A research on emotion and personality characteristics in junior high school students with internet addiction disorders. *Chinese Journal of Clinical Psychology, 14,* 153-155.

Ybarra, M., & Mitchell, K. (2004a). Online aggressors/targets, aggressors and targets: a comparison of associated youth characteristics. *Journal of Child Psychology, 45(7),* 1308-1316.

Ybarra, M., & Mitchell, K. (2004b). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence, 27*, 319-336.

Ybarra, M., Mitchell, K., Finkelhor, D., & Wolak, J. (2007c). Internet prevention messages: Targeting the right online behaviors. *Archives of Pediatrics and Adolescent Medicine, 161*, 138-145.

Ybarra, M. L., Espelage, D. L., & Mitchell, K. J. (2007b). The co-occurrence of Internet harassment and unwanted sexual solicitation victimization and perpetration: Associations with psychosocial indicators. *Journal of Adolescent Health, 41(6),* S31-S41.

Ybarra, M. L., & Mitchell, K. J. (2005). Exposure to internet pornography among children and adolescents: a national survey. *CyberPsychology & Behavior: The Impact Of The Internet, Multimedia And Virtual Reality On Behavior And Society, 8(5),* 473-486.

Yen, J., Ko, C., Yen, C., Wu, H., & Yang, M. (2007). The commorbid psychiatric sympotms of Internet addiction: Attention deficit and hyperactivity disorder (ADHD), depression, social phobia, and hostility. *Journal of Adolescent Health, 41*, 93-98.

Youn, S. (2008). Parental influence and teens' attitude toward online privacy protection. *The Journal of Consumer Affairs, 42(3),* 362.

Youn, S., & Hall, K. (2008). Gender and online privacy among tenns: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior, 11(6),* 763-765.

Young, K. (1996a). Internet addiction: The emergence of a new clinical disorder. *CyberPsychology & Behavior, 3*, 237-244.

Young, K. (1996b). Psychology of computer use: XL. Addictive use of the internet: A case that breaks the stereotype. *Psychological Reports, 79*, 899-902.

Zboralski, K., Orzechowska, A., Talarowska, M., Darmosz, A., Janiak, A., Janiak, M., et al. (2009). The prevalence of computer and Internet addiction among pupils. *PostepyHig Med Dows, 63*, 8-12.

APPENDIX A

KEYWORDS USED IN LITERATURE SEARCH

Keyword[§]		
*Mobile phone	Block*	Australian Youth
Abuse	Chat rooms	Breach
Adolesce*	Computer mediated Communication	Bully*
Victim*	COPPA	Cyber crime
Australia*	Criminal	Cyber threat
Chat	Cyber security	Cyberbully*
Child abuse	Cyber victimisation	Cybervictim*
Child*	E-mail	Eating disorders
Cyber	Electronic aggress*	Fraud
Cyberstalk*	Electronic mail	Hack*
Electronic bully*	False identity	Identity theft
Exploit*	Filter*	Illicit drugs
Girl	Graphic	Information theft
Grooming	Inappropriate	Internet behavio(u)r
Illegal	Instant messeng*	Internet use
Internet	Internet bully*	Monitor*
Internet harass	Internet Service Provider	Online gambling
MySpace	Online predators	Password
Online	Online privacy	Password safety
P(a)eodophil*	Online safety	Phishing
Predator*	Online security	Prevalence
Risk	Password theft	Privacy
Sex*	Pornograph*	Priva*
Sexual grooming	Protect*	Scam
Solicit*	Social networking	Self harm
Stalk*	Stolen password	Smoking
Teenagers	Student*	Stolen identity
Text*	Technology	Stolen password
Victimization	Violen*	Theft
Youth	Young	Threats

Note: * indicates truncated terms. Truncating a term will result in all terms with that stem being included in the search. Thus, "child*" will reveal results for child, children, childhood, childish, etc.
[§]This table lists 89 keywords which were combined in a number of searches. For example, "Internet behavio(u)r" was combined with "smoking" to identify relevant articles.

APPENDIX B

DATABASES USED IN LITERATURE SEARCH

Databases used in literature search

A+ Education

ABS

Academic one files line

Academic OneFile

Academic Research Library (ProQuest)

ACM Digital Library

AGIS Plus

APA-FT Australian Public Affairs Full Text

Association for Computing Machinery

Digital library

Attorney General's Information Service - AGIS - Plus

Text

Australian Public Affairs Full Text - APAFT

CINAHL

CINAHL Plus

CINCH Australian Criminology

Current Contents Connect

Digital Dissertation Extracts

Databases used in literature search

EJS

eLibrary Australasia

Emerald Journals

ERIC

Health & Society

IEEE Electronic Library

Informaworld

ISI

ISI Web of knowledge

Lawlex

Legal Trac

LISA

LISTA

Meditext

MEDLINE

PROQUEST

Proquest 5000

ProQuest 5000 International

Proquest health and medical complete

PsycARTICLES

Databases used in literature search

PSYCINFO

Science Direct

SCIRUS

Wiley Inter Science

APPENDIX C

AGENCIES AND WEBSITES SEARCHED TO IDENTIFY CYBER-BULLYING RESOURCES

Organisation / Author name	Website
Pew/Internet & American Life Project	http://pewinternet.org
Cyber-safety symposium Report/National Centre Against Bullying	www.ncab.org.au
Tackling sexual grooming Conference Westminster, London 2003	www.childnet.com/downloads/
Cyber safety plan	www.dbcde.gov.au/
European Commission: Information Society & Media Directorate –General, Child safety & mobile phone services	http://europa.eu.int/information_society
National Coalition Against Bullying Survey 2004, National Crime Prevention Council	www.ncpc.org
National Safe Schools Framework	www.dest.gov.au
Bullying No Way	www.bullyingnoway.com.au
Cyber bullying: issues for policy makers/ Australian Institute of Criminology	www.aic.gov.au/publications/ crm/crm059.html
Alannah & Madeline Foundation	www.amf.org.au/
Cyberbullying: Anti-bullying Alliance	www.anti-bullyingalliance.org.uk
Cyberbullying: Safe to learn	www.teachernet.gov.uk/
Working to halt online abuse	www.haltabuse.org
CyberAngels: Internet safety program	www.cyberangels.org
The child exploitation & online protection centre	www.ceop.gov.uk
Crimes against Children Research Centre	www.unh.edu/ccre/survey_internet .mental_health.html
Cybersmart - ACMA	www.cybersmartkids.com.au
Childnet International	www.childnet-int.org/
Australian Clearinghouse for Youth Studies	www.acys.info/topics/bullying
National Child Protection Clearinghouse	www.aifs.gov.au/nch/bib/bully.html
National Centre Against Bullying	www.ncab.org.au
Social Care Online	www.scie.socialcareonline.org.uk
Centre on Child Abuse & Neglect	www.ncsby.org
The Clearinghouse of Information on Child Abuse & Neglect	http://nccanch.acf.hhs.gov
International Society of Prevention of Child Abuse & Neglect	www.ispcan.org/

Organisation / Author name	Website
Child Abuse Prevention Network	www.childabusenetwork.org
National Clearinghouse for Child Abuse & Neglect	www.calib.com/nccanch/
National Child Traumatic Stress Network	www.nctsn.org
Electronic Frontiers Australia	www.efa.org.au
Youth Affairs Network of Queensland	www.yanQ.org.au
Government of New South Wales (Police)	www.police.nsw.gov.au
Australian Federal Police	www.afp.gov.au
US Department of Justice	www.ncjrs.gov
Government of New South Wales (Youth)	www.youth.nsw.gov.au
Commonwealth of Australia	www.edna.edu.au
Department of Education and Early Childhood Development, Victoria	www.education.vic.gov.au
Australian Institute of Criminology	www.aic.gov.au
Department of Education, Tasmania	www.education.tas.gov.au
New South Wales Department of Education and Training	www.schools.nsw.edu.au
Child Wise	www.childwise.net
Tom Worthington	www.tomw.net.au
Wise Kids	www.wisekids.org.uk
SafeKids	www.safekids.co.uk
Larry Magid	www.safekids.com
National Society for the Prevention of Cruelty to Children	www.childline.org.uk
Department of Broadband, Communications and the Digital Economy	www.dbcde.gov.au
Australian Communications and Media Authority	www.acma.gov.au
learn.org	www.learn.org/internetsafety.html
Department for Children, Schools and Families, UK	www.dcsf.gov.uk
Berkman Center for Internet and Society and Harvard University	www.cyber.law.harvard.edu

Organisation / Author name	Website
Department of Education and Training, WA	www.det.wa.edu.au
Mental Health Association NSW Inc	www.mentalhealth.asn.au
Sameer Hinduja & Justin W. Patchin	www.cyberbullying.us
Department of Education and Children's Services, South Australia	www.decs.sa.gov.au
Bill Belsey	www.cyberbullying.ca
NetAlert	www.netalert.gov.au