Submission to the Joint Select Committee on Cyber-Safety, June 2010

Submission prepared by Candice Jansz, Monash University.

Candice Jansz is a current PhD candidate in the School of English, Communications and Performance studies at Monash University, Caulfield Campus, undertaking research into young people's disclosure, safety and privacy within online social networking websites, and corresponding youth education strategies. She also holds a Bachelor of Arts (Criminology), from the University of Melbourne and a Master of Arts, (Communication) from RMIT University.

Ms Jansz is also a member of the Office of the Victorian Privacy Commissioner's Youth Advisory Group, and recently presented a paper entitled 'Growing up Networked – An analysis of youthful risk-taking and disclosure within online social networking websites' at the 'Watch this Space: Children, Young People and Privacy' conference held at the Crown Promenade Hotel, Melbourne, on Friday 21 May 2010.

Background

The 2010 federal government enquiry into cyber-safety seeks to address a number of cyber-safety issues and how they relate to children and young people. This submission is concerned primarily with young people's experience of online social networking websites, their perceptions of online privacy, and ways to curb the potential negative effects of online interaction through education and awareness building from early ages. This submission will also outline the value of educative measures designed for parents, teachers and caregivers in keeping young people safe online.

Online technology plays a vital role in the lives of Australian children and young people, most notably within their academic and social pursuits. In the last decade, online interaction has grown in popularity as online social networking websites have advanced to encompass a number of previously separate commonly-used communicative facilities. This technological convergence has made online social networking sites increasingly attractive to young people, due to their 'one stop shop' convenience, high levels of customisation, low cost and widespread peer adoption.

Contemporary concerns raised by both popular media and academic sources surrounding young people's online expression are extremely valid, as the potential consequences of excessive or even routine online disclosure can be grave. The most serious of these is evidenced by the highly publicised online solicitation and tragic murders of Australian teenagers Carly Ryan and Nona Belomesoff in two separate predatory incidents within just the last 3 years.

However, it must be stressed that solely denying or restricting young people's access to online technologies without first considering and implementing age-appropriate educative measures is not a viable option when searching for solutions or designing strategy in this area. Younger members of the Australian community must be provided with the means, knowledge and the confidence to utilise the internet for their purposes in safety.

Awareness education targeted at parents, teachers and other youth-orientated caregivers is also a vital step in maximizing online opportunities for young Australians, whilst minimizing threats to their safety and wellbeing.

Key Findings

1. There is no one overarching strategy that can be employed to preserve young people's safety online. Governments, schools, community organizations, parents and young people must all work together through a number of differing approaches and age-specific strategies in order to achieve the best possible outcome.

2. As online interaction permeates every facet of young people's lives, so too must education concerning it. Young people are going online at ever-younger ages, and as such, education on the safe use of online technologies, including negotiating their inherent risks and the importance of ensuring the privacy of personal information disclosed therein, must also begin in early childhood. Suggested strategies include specifically commissioned picture story books and character merchandise.

3. While young people today are taking steps to actively manage their own online privacy, ongoing educative strategies including input from and components for parents, teachers and other youth-orientated caregivers are vital in ensuring online safety messages are received by young people and misinformation or complacency avoided.

The design and implementation of peer-run educational programs should also be a central facet of any such measure, as youth place great importance on the views and actions of their peers. This diversification of advice and information will ensure that messages concerning the permanency of actions, the gravity of choices and the dangers of online disclosure are reiterated and more comprehensively understood by young people in the long term.

4. Currently, access to educative and helpline resources concerning cyber-safety and the use of online technologies are fragmented and difficult to quickly and conveniently access, particularly for those who are unfamiliar with the internet but have a vested interest in the area, for example, parents. The introduction of a comprehensive, highly publicised and well organised government-hosted portal providing access to the majority of Australian resources would aid greatly in both communicating cyber-safety messages and providing easy access to related helpline information, for example, the Kids Helpline, Parentline or SuicideLine.

Youth Online

The internet and it's many offerings now play a vital role in young people's lives, and heavily influence their ongoing development, through concentrated use throughout their school years and beyond. Children as young as three now utilise the internet, encouraged by parents, older siblings, and the lure of online gaming websites such as Club Penguin, or popular toys and television shows with corresponding online components, for example Bratz dolls, Ben 10 and ABC Kids website 'The Playground'.

For pre-school children and those in primary school, the internet is primarily utilised as a means of entertainment, for music downloads, online gaming portals, the exploration of hobbies and interests or as an academic resource. Once young people commence high school, social pursuits are commonly added to this mix, and interaction with their peers and others on online social networking websites such as Facebook, MySpace, Twitter, Bebo, MSN Messenger and YouTube feature prominently in their time spent online.

The importance placed on peer interaction and self-representation by contemporary youth is not uncommon, and was exhibited by the young people in preceding generations in various other ways, for example through clothing, music or television preferences. In kind, as the internet grows in scope and capability, the gravitation of these and other normal adolescent behaviours and expression into the online arena is to be expected.

Young people's online profiles are often highly personalised and expressive, comparable to creating a pictorial avatar within a computer game, albeit via textual or other symbolic elements, such as fan pages, quizzes or uploaded photographs. The information depicted can be quite detailed, with the average social networking profile containing up to 40 separate pieces of personal information, including full name, birth date, offline contact details, sexual preference and relationship status.

These personal snippets, coupled with activity carried out within online groups, applications and posts to other's profiles can depict a startlingly comprehensive picture of the private life of the young individual portrayed. Such exposure in what is an essentially public setting, can leave young people open to potentially unsavory consequences, including but not limited to damage to their long-term reputations and employment prospects, cyberbullying and online solicitation.

Youth Privacy

While both academic and media accounts alike describe contemporary youth as a narcissistic, over-sexed and self-obsessed generation with delinquent desires and little concern for their privacy or the consequences attached to their actions, it is unfair to utilise these sentiments to describe the entirety of this group.

What must be understood is that young people's seemingly blazé attitudes towards what they disclose online, (despite an often comprehensive awareness of the risks involved) is not necessarily due to any form of inherent delinquency.

Rather, the seemingly raucous or explicit interactions that young people engage in online can be attributed to the fact that both themselves and their peers do not see their online behaviours as any different to the interactions that they carry out in the physical world, due to their high level of comfort and familiarity with online technologies.

Further to this, teenagers in particular are at a stage in their lives where peer approval and belonging is of paramount importance to them. In kind, it is to be expected that normal adolescent risk taking and rebellion would also be exhibited in the online arena though the exploration of alternate personas, the publication of risqué images, the use of profanity or the display of sexual or violent content, by way of example.

As such, the inherent risks presented by online social networking websites are unlikely to be viewed as particularly pressing or problematic for young people when considering their participation within them, when weighed against strong peer encouragement or pressure to participate and interact with one another on such sites.

What is most likely to change such attitudes is not restriction, but rather, metered levels of trust and responsibility, which includes controlled access to these now vital youth resources. What is heartening is that young people are now illustrating considerable cognitive adaptations to the online environment, and take steps to actively manage their own privacy and safety, whilst still reaping the benefits of these powerful technologies.

However, it must be also noted here that privacy settings within online social networks can also be problematic in terms of cyber-safety. Not only are default settings formulated in an open, 'opt out' manner (no doubt to facilitate maximum interaction and connectivity on the websites), but they are constantly changing. As such, even if young people are vigilant in customizing their privacy settings when they first sign up to the site, regular reviews are required to maintain their online security long-term.

Parents and Guardians

The recent ACMA 'Click and Connect' report on Young Australian's use of online social media conducted in July 2009 found that parents believed that offline risks, (for example, face-to-face bullying) exceed potential online dangers. The same report also found that parents were likely to be largely unaware of the true scope of their child's online network or friends, and that the majority of parents believed that it would not be their own child who would be involved in negative online incidences or risky behaviours. These are startling revelations for a group directly responsible for the safety and education of the next generation.

Education for parents run through schools and community groups, including relevant testimony from young people is vital in altering such inaccurate perceptions. Online bullying is just as damaging to young people, if not more so than face-to-face bullying due to its public nature and ability to be quickly replicated and broadcast to disparate audiences. Cyber-bullying can also be experienced alongside physical bullying or harm, compounding their effects, and at times leading to isolation, self harm and tragically, youth suicides. Finally, young people have been known to make mistakes and errors in judgement, and the old adage 'never talk to strangers' can often seem less pertinent to a young person online.

At the other end of the spectrum, portraying the online environment as a place full of risks beyond young people's control creates an air of trepidation around online interactions. In an age where young people are, as a general rule, equally if not more technologically competent than their parents, parental education will serve to dispel common fears that often exist as a result of ignorance or misinformation surrounding online facilities and their true uses. Most prominently, extensive and pervasive media coverage concentrating solely on the negative effects of the internet as a whole, and more recently, online social networks in particular.

Such education, particularly for parents of younger children, is also likely to aid in opening the lines of communication between parents and young people regarding online social networks, their use and their potential risks from an early age. Such ongoing communication is likely to minimise the taboos surrounding such common communicative behaviours as children reach their teens, and perhaps even encourage young people to educate and include their parents in their use of these technologies.

While 'friending' their children on such social networking websites may not be an ideal solution in all scenarios, a general awareness of the networks in question, and the ability to discuss these openly with children as they develop would greatly aid in the prevention or minimisation of negative consequences.

Teachers and Non-parental caregivers

The importance on educating educators on cyber-safety is rarely disputed, and many Australian schools already have comprehensive cyber-safety programs and policies in place for their staff and students. These forms of teacher training should also include external presentations from cyber-safety and childhood development experts, so that teachers are able to ask complex questions concerning their own learning environments, and receive answers that they are able to translate into their own teaching practices.

There are also persons outside the school environment for whom education on cyber-safety and cyber issues would also beneficial. Namely, those who supervise, teach and care for young people in their more generalised extra-curricular activities. For example, the scout and guiding movements, tutoring, dance, sporting and youth organizations.

Policies for such organizations concerning cyber-bullying in particular would likely benefit the young people who participate in these activities, as such conduct is not only isolated to the schoolyard. Bullying at extra-curricular activities is just as likely to occur, and in the same vein, so too is cyber-bulling.

The targeted education of non-parental caregivers such as teachers and other youth-orientated workers through community and school-run programs will acknowledge that the effects of online interaction encompass so much more than just the realms of school and the home. The informed formulation of individual cyber policies for such organizations, concerning the handling of online issues will help to shield young people from negative consequences in such environments, and provide them with a point of contact should they encounter any.

Peer Education

A strategy that is likely to be the most effective in combating the negative effects of online interaction for children and young people is peer-run education through groups such as Privacy Victoria's Youth Advisory Group, or mentor groups within school and community environments. Groups such as this, composed of enthusiastic and dedicated young people are more likely to be able to reach and connect with a young audience than older presenters, despite lacking in formal training and experience. They are at an age where they are mature enough to understand and communicate the risks and issues involved in online communication, yet young enough to remember their childhood and teen years clearly, making them able to easily relate to and empathise with their audience's issues, concerns and communicative needs.

Dynamic and enjoyable presentations on cyber-safety by young people in schools and community venues for children, young people, parents and teachers alike are more likely to be remembered than academic or expert testimonies, which can inspire message fatigue as old materials and slogans are constantly rehashed and reused.

The use of young people to educate young people also means that messages can be dispersed through alternate delivery methods, for example peer-created artwork, merchandise and posters, concerts, dynamic websites (including vox pops, videos and competitions etc.) and even delivery on the mediums deemed problematic in the first place, for example, Facebook advertising, groups or fan pages.

More serious content should also be interspersed in any such presentation (for example testimony from a victim's parent or sibling), as real-life examples delivered directly by young people are likely to hit home much more effectively than if delivered by a parent or other authority figure.

Access to online resources

At present, access to valuable online resources concerning cyber-safety such as staysmartonline.gov.au, cybersmart.com.au, Thinkuknow.org.au, Privacy.vic.gov.au and virtualglobaltaskforce.com are fragmented, and difficult to easily navigate or find online, without knowing exactly what you're looking for.

The ability to access detailed resources on cyber-safety and any related Australian helplines or regulatory bodies via one comprehensive government-hosted online portal is strongly advisable, particularly for individuals who are not familiar with the internet and online social networks. A simple, well publicised web address, (i.e. Cybersafety.gov.au) would ensure it is easily remembered, and as such is accessed without difficulty when required.

Easily executed access to such information would help to ensure that messages surrounding cyber-safety are still received and understood by those who aren't necessarily tech-savvy, as well as provide a quick reference point for young people, parents, teachers and professionals actively seeking information or the assistance of authorities.

Directly linking such a portal to popular social networks such as Facebook and MySpace via an online 'panic button' is also likely to be effective, as it would offer immediate help and advice concerning online technologies directly within the mediums in question.

Conclusions

Online technologies have much to offer young Australians by way of connectivity, opportunity and worldwide exposure. However, young people's familiarity with the internet and high levels of technological competence within the medium can breed complacency, as awareness of the potential risks of online communications pales in significance to the easily perceived benefits of participation, enjoyment and belonging in the online environment. Such complacency can be minimized through dispelling commonly-held attitudes amongst young people, most notably 'everyone's doing it' and 'it won't happen to me'.

While many parents, caregivers and teachers are quick to denounce online social networks and other online technologies for their privacy failings or member screening procedures, really the safety of young people is in their hands. Resources and education programs targeted at these groups are vital in any strategy concerning the safety of children and young people, so that adults can learn about and monitor which technologies the young people in their care are using and how, in order to eliminate their own apprehensions, and encourage safe use of the technology.

If young people are utilizing the internet from an early age, safety education concerning its use must start at this time, at pre-school or kindergarten level, alongside traditionally taught life lessons and skills. In kind, if young people are influenced strongly by their peers, peer education utilizing relevant language, examples and even peer-created imagery and resources will likely be more effective than adult-led alternatives.

Cyber-safety must be upheld and negative consequences minimized through a number of diverse and varied approaches, as the utility of the internet continues to grow and evolve. Online risks are well within the competencies of Australian young people to navigate and manage, if armed with the correct information and attitudes from early ages into young adulthood.

Young people's online development, learning and expression should be undertaken with strong support, encouragement and guidance from their parents, teachers and peers in order to ensure that they have the ability to make informed and intelligent decisions surrounding not only their disclosure, but with whom they are communicating, and what they are communicating about.

Such a support network is an option far better than attempting to restrict or deprive young people of communicative tools that they are likely to utilize with or without the permission of authority figures, and taking from them the opportunities for self expression, social participation and success that they offer.

Recommendations

This submission makes the following recommendations towards Australian cyber-safety strategy. The approaches suggested are both diverse and targeted, and are designed to be part of a fully integrated cyber-safety campaign - an approach that through its multifaceted nature will ensure messages are delivered to their desired audiences more effectively that any one strategy could achieve in isolation.

1. Comprehensive online portal containing links to disparate online resources concerning cyber-safety from key bodies, for example ACMA, Privacy Victoria and the Australian Federal Police.

2. The formulation of a series of educational online safety picture books and merchandise for young children ages 3 - 7, undertaken in consultation with early childhood educational bodies/online safety researchers and popular Australian children's authors and illustrators.

3. Peer-designed educational materials (posters, booklets) for primary school aged children (separate materials for pre-prep to grade 1, grades 2 to 4, and grades 5 & 6 in order to encompass developmental changes).

4. Targeted age-specific online safety education and training programs (formulated in consultation with young people for relevance) run in schools and community organisations for students, parents, teachers and caregivers.

5. Educational programs/school visits involving activities and merchandise run by young people in an advisory capacity for grades 7 and up, including project work and focus groups.

6. The installation of a 'panic button' on popular online social networking websites (for example Facebook and MySpace) linking through to an abuse reporting facility, Australian emergency numbers and a government-hosted online information portal with email facility.

*****

References

Berson, I & Berson M (2005) Challenging Online Behaviours of Youth: Findings from a Comparative Analysis of Young People in the United States and New Zealand, Social Science Computer Review, Vol, 23, No. 1, Spring 2005 pp 29-38

Boyd, D. & Ellison, N. (2007) ‘Social network sites: definition, history and scholarship’, Journal of Computer Mediated Communication, 13(1), pp 210-230

Boyd, D. (2008) Facebook’s privacy trainwreck: Exposure, invasion, and social convergence, The International Journal of Research into Media Technologies, 14(1), pp 13–20

Boyd, D (2008i) Why Youth ♥ Social Network Sites: The Role of Networked Publics in Teenage Social Life, in Youth, Identity, and Digital Media. Edited by David Buckingham. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA, The MIT Press, 2008, pp 119–142

Cassell, J & Cramer, M (2008) High Tech or High Risk: Moral Panics about Girls Online. Digital Youth, Innovation, and the Unexpected. Edited by Tara McPherson. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, pp 53–76.

De Souza, D & Dick, G (2009) Disclosure of information by children in social networking—Not just a case of “you show me yours and I’ll show you mine” International Journal of Information Management 29 pp 255–261

Debatin, B, Horn, A, Hughes, B & Lovejoy, B (2009) Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, Journal of Computer-Mediated Communication 15 pp 83–108

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007), ‘Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace’, Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, USA, 9–12 August. 2007 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.2959&rep=rep1&type=pdf

Dwyer, C., Hiltz, S.R. and Widmeyer, G. (2008), ‘Understanding Development and Usage of Social Networking Sites: The Social Software Performance Model’, Proceedings of the 41st Hawaii International Conference on System Sciences,http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.3696&rep=rep1&type=pdf

Ellison, N. B., Steinfield, C., & Lampe, C. (2007) The benefits of Facebook "friends": Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4) http://jcmc.indiana.edu/vol12/issue4/ellison.html

Espinoza, G, Reich, S, Subrahmanyam, K, Waechter, N (2008) Online and offline social networks: Use of social networking sites by emerging adults, Journal of Applied Developmental Psychology, 29 pp 420-433

Gasser, U & Palfrey, J (2008) Born Digital, Basic Books, New York, pp 1-110

GFC Bluemoon (2009) Click and connect: Young Australians' use of online social media, Australian Communications and Media Authority, Qualitative report, July 2009, pp 1-100

Govani, T. and Pashley, H. Student awareness of the privacy implications when using Facebook. Unpublished manuscript. http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Grimmelmann, J (2009) Saving Facebook, Iowa Law Review 94, pp 1137-1206

Gross, E, Juvonen, J & Gable, S (2002) Internet use and well-being in adolescence, Journal of Social Issues, vol. 58, no. 1, pp 75–90.

Gross, R, & Acquisti, A (2005) Information revelation and privacy in online social networks, Proceedings of the 2005 ACM workshop on Privacy in the electronic society 2007, pp 71-80 http://delivery.acm.org/10.1145/1110000/1102214/p71-gross.pdf?key1=1102214&key2=0589659621&coll=GUIDE&dl=GUIDE&CFID=81666340&CFTOKEN=33849376,

Holloway, S, Valentine, G (2001) On-line Dangers: Geographies of Parents' Fears for Children's Safety in Cyberspace, Professional Geographer, 53(1) pp 71–83

Holmes, J (2009) Myths and missed opportunities: Young people's not so risky use of online communication, Information, Communication & Society 2009, pp 1 – 23

Lenhart, A & Madden, M (2007) Teens, Privacy & Online Social Networks, Pew Internet & American Life Project pp i-45 http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.

Lenhart, A & Madden, M (2007a) Social Networking Websites and Teens: An Overview Pew Internet & American Life Project pp 1-10 http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf

Livingstone, S. & Bober, M. (2005) UK Children Go Online: Final Report of Key Project Findings, ESRC & e-Society, Media@LSE, London pp 1-41

Livingstone, S & Milwood Hargrave, A (2006) Harmful to Children? Drawing Conclusions from Empirical Research on Media effects in Regulation, Awareness and Empowerment, Young People and Harmful Media Content in the Digital Age. Edited by Ulla Carlsson, The International Clearinghouse on Children, Youth and Media, Nordicom, Sweden, pp 21-48

Livingstone, S, and Haddon, L (2009) EU Kids Online: Final report. LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5) pp 1-46

Livingstone, Sonia (2007) Do the media harm children?: reflections on new approaches to an old problem. Journal of children and media, vol 1 (1), pp 5-14.

Livingstone, S (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression, New Media and Society Vol 10 (3), Sage Publications Los Angeles, London, New Delhi and Singapore, pp 393 - 411

Luders, M (2008) Conceptualising Personal Media. New Media & Society 10(5) pp 683-702

Morrison, M & Mcmillan, S (2006) Coming of age with the internet: A qualitative exploration of how the internet has become an integral part of young people's lives. Sage Publications, London, Thousand Oaks CA, New Delhi pp 73-95

Rosenblum, D. (2007) What Anyone Can Know: The Privacy Risks of Social Networking Sites, Security & Privacy, IEEE, Vol. 5 (3), pp 40 - 49

Stern, S (2008) Producing sites, Exploring identities: Youth Online Authorship, in Youth, Identity, and Digital Media. Edited by David Buckingham, The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA, The MIT Press, pp 95- 117

Tapscott, D (2009) Grown Up Digital, McGraw-Hill, New York pp 1-120

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010), Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook^{TM} profiles as an example, International Journal of Media and Cultural Politics 6(1), pp 81–102

Thompson, J (2005) The New Visibility, Theory, Culture & Society (SAGE, London, Thousand Oaks and New Delhi),Vol. 22(6) pp 31–51

Tufekci, Z (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society, 28(1), pp 20–36

Van Dijk, J (2009) Users Like You? Theorizing Agency in User-Generated Content Media, Culture, Society 31 pp 41-58