NORTHERN TERRITORY GOVERNMENT SUBMISSION TO

THE JOINT SELECT COMMITTEE ON CYBER-SAFETY

INQUIRY INTO CYBER-SAFETY

JUNE 2010

A. INTRODUCTION

1. The Northern Territory Government (the NTG) welcomes the opportunity to provide its input into the Joint Select Committee on Cyber-Safety (the Committee) Inquiry into Cyber-Safety (the Inquiry).

2. The issue of cyber-safety and the protection of children in an online environment is one that affects the community in different ways. The impact of cyber-based forms of exploitation of children, on children themselves and on society as a whole, makes it an issue worthy of considerable focus and resources. Given the rapidly evolving nature of technology and communications, the Inquiry is strongly supported. It is hoped that the Inquiry will result in significant advances in the protection of children in the cyber-environment.

3. The NTG submission highlights some of the strategies that are currently in place within Australia and internationally to better protect children in the cyber-environment. These initiatives should be supported and where necessary, expanded. The submission also discusses areas where further attention is warranted and provides some examples of international initiatives, which if adopted in Australia, could make substantial gains in the protection of Australian children.

B. NORTHERN TERRITORY GOVERNMENT RESPONSE

The online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles).

4. Children in the Northern Territory have the same key physical points of access to internet service and carriage providers as children in other jurisdictions. The use of mobile phone technology amongst children is high, as is the practice of downloading and uploading images to and from both mobile devices and social networking sites.

5. While parents can control access on a home computer and schools providing access points controlled by an internal network (for example: individual user accounts), the high ownership of mobile devices by children means that there is no longer one place to access on-line/virtual environments.

6. Companies (both large and small), in particular those who carry out the business of Information and Communication Technologies (ICT), law enforcement, researchers, organisations, parents, teachers and governments all have important roles and responsibilities in the protection of children in the cyber-environment.

7. Joint approaches by ICT companies, law enforcement agencies, researchers and relevant organisations can result in the development and implementation of tools to locate, identify and ultimately, prosecute child pornographers. Initiatives have been developed and implemented internationally (for example, the Technology Coalition Against Child Pornography; established by the United States National Centre for Missing and Exploited Children (NCMEC) alongside numerous ICT companies including Google, AOL, Yahoo!, Microsoft, EarthLink and United Online), to enhance knowledge sharing among industry participants, improve law enforcement tools and research

perpetrators' technologies in order to enhance industry efforts and build solutions [NCMEC, 2006].

8. In South Australia, law enforcement agencies collaborated with researchers from the University of South Australia to develop a number of tools for investigating cases of online child grooming [Choo, 2009]. These collaborative initiatives are an essential component of efforts to protect children online and are worthy of ongoing support and expansion.

9. Large ICT companies are in a unique position, and have a significant corporate responsibility to contribute to efforts to protect children online. Microsoft is engaged in a number of collaborative initiatives specifically to address the problem of internet-based child exploitation. For example, Microsoft has partnered with law enforcement agencies and non-government organisations to combat crimes against children by providing a range of services including training for law enforcement officials on computer technology and educational information to consumers.

10. Microsoft has also actively assisted in investigations into suspected cases of child pornography, trafficking and prostitution and has provided expertise on computer and network technologies to law enforcement agencies. For example, the development of a private web portal for law enforcement agencies to assist with cyber crime investigations and internet safety threats which offers targeted technical assistance as well as training and information [Choo, 2009].

11. Financial service institutions also have the potential to play a major role in dealing with the online exploitation of children. One such initiative that has been effective to date is the partnership between Microsoft and the International Centre for Missing and Exploited Children (the Financial Coalition Against Child Exploitation) which has links with a number of financial institutions, enabling the monitoring and reporting of financial transactions involving crimes against children [BBC Online, 2006; NCMEC, 2006; Choo, 2009].

12. Other collaborative initiatives include the Global Campaign Against Child Pornography. This joint initiative involving organisations, individuals and law enforcement agencies promotes public awareness of the problem and encourages responsible internet behaviour in organisations and service providers [Choo, 2009].

13. The NTG considers that the participation of large ICT companies and financial institutions should be encouraged. Collaborative initiatives such as those outlined above demonstrate responsible and ethical corporate and community behaviour and are worthy of ongoing support and expansion.

14. In addition, some social networking sites have taken the initiative to work alongside law enforcement agencies in an effort to protect children from harm. For example, some social networking sites have specific terms of use that prohibit users from using the internet to bully or harass other users. Users who disregard these terms may be banned from the site and/or reported to the relevant authorities. In the United States, internet service providers (ISPs) face mandatory obligations to report child pornography on their systems to the NCMEC.

15. Children are especially vulnerable to cyber-based sexual exploitation when they are constantly exposed to sexual material that either displays them as sexual objects or directs sexual material at them (directly or inadvertently) for financial and other gain.

16. Research consistently reveals the damaging effects of the sexualisation of children in the media [Rush & La Nauze, 2006]. In order to make effective gains in the protection of children online; media corporations and governments need to take responsibility for the prevention of the sexualisation of children through all forms of media. Until this occurs, it is unlikely that children can or will be fully protected in the cyber-environment.

17. The NTG considers that similar obligations such as those outlined above, should be placed on Australian ISPs, as well as mobile phone carriers, web-hosting companies and social networking websites and that further action needs to be taken, particularly by media corporations and governments, to stop the sexualisation of children in and through the media.

The abuse of children online, particularly cyber bulling.

18. The cyber-environment has created a new space in which children communicate, play, experiment and learn. While this environment provides opportunities for children, it can also expose them to risks, where they may become victims of crime or the perpetrators of crime themselves.

19. Children are especially vulnerable to exploitation in the cyber environment as the internet can be a fun and attractive environment and children, due to their inexperience, may be naïve to the motives of others. As a result of the increasing use and availability of portable devices such as mobile phones, children may have opportunities to access the internet while unsupervised.

20. Research has highlighted the large numbers of children and young people who use the internet. For example, Lenhart & Madden reported 55 per cent of 12–17 year old children surveyed in the United States use social networking websites. The large number of child internet users leaves many children vulnerable to the multiple risks associated with it. For example, the Growing Up with Media study [Ybarra, Espelage and Mitchell, 2007] found that 35 per cent of young people aged 10–15 years reported being the victim of either internet harassment or unwanted sexual solicitation. It is likely that similar prevalence rates occur in Australia.

21. Children are especially vulnerable to exploitation in the cyber-environment by offenders who use technology to exploit children's innocence and curiosity. For example:

   ▪ 'grooming' children online to send them sexually explicit material or arrange to meet them and sexually exploit/assault them physically and/or coerce the child to submit sexual images of themselves;

   ▪ fraud, as children may unwittingly or without permission provide an offender with a family member's credit card details or the child's internet connection may be directed to an expensive telephone service;

   ▪ sale or distribution of banned pornography and/or other explicit material (for example, pop-up pornographic sites, pornographic sites set up with names that are deliberately similar to the names of popular children's websites, unsolicited emails with links to pornographic sites);

- spreading viruses as children may unwittingly download material or send emails that result in the spread of computer viruses; and

- the use of information and communication technologies such as bulletin boards by offenders or networks of paedophiles to sexually abuse children or facilitate child prostitution.

22. International investigations into online child pornography reveal a global problem that is escalating every year. For example:

- A 2002 report by ECPAT International and the Bangkok Post estimated that 100,000 child-pornography web sites existed on the Internet in 2001.

- The Internet Watch Foundation in the United Kingdom found that there has been a 1500 per cent increase in the number of child pornography images since 1997.

- In 2003, the National Criminal Intelligence Service in the United Kingdom estimated that child pornography websites had doubled worldwide; that half of the sites are hosted in the United States; and that the number of sites in Russia had doubled [International Centre for Missing and Exploited Children (ICMEC), 2010].

- Reports of child pornography passed to the NCMEC CyberTipline have increased from 24 000 reports in 2001 to more than 340 000 in 2005 [BBC Online, 2006].

23. In the Northern Territory, incidents investigated by the Northern Territory Police have involved:

- A female child who had taken images of her herself in various states of undress using a mobile phone and had transmitted these images to her boyfriend. Following the end of the relationship, the male retaining the images, transmitted them to a third party, another female child at the same school. The images were sent to an unknown number of persons by the second female child with the express intent of causing shame and embarrassment to the first female child. The second female child who sent the images stated that she did not know it was an offence to transmit or possess the images. Naked images of the second female were also located during analysis of her computer.

- A female child opens her own 'Twitter' account and other social networking accounts. She is approached by a person who states that they are a male of 23 years of age. The male entices the female to send personal details including home addresses, parent's names, dates of birth, home and mobile telephone numbers and then requests to meet with her at a park some days later. The female did not attend the park to meet this person. The child is now fearful that the male knows where she lives.

- The seizure of mobile phones following investigations into a series of unlawful entry offences. The phones were owned by male children. Two of these phones contained images of female children in various states of undress which appear to have been made within the Northern Territory and sent to the males.

24. In addition to the risks of grooming, child pornography and other forms of online sexual exploitation, children and young people are also at risk of bullying in the cyber-environment. Cyber bullying is a form of covert bullying that is carried out through the use of technology, such as via email, blogs and social networking sites, as well as other mediums such as mobile phones. The behaviour is aggressive in nature, repeated and intended to cause harm. It involves an imbalance of power and is unseen or unacknowledged by adults [Cross et al, 2009].

25. In a recent study of the incidence of cyber-bullying in Australia, Cross et al (2009) reported that up to 10 per cent of students in Year 4–Year 9 indicated having experienced cyber-bullying in the previous term. Other researchers (for example, Smith et al, 2008) have highlighted that the covert and hidden nature of cyber-bullying makes it difficult for teachers and school administrators to prevent.

26. Cross et al (2009) provided a number of recommendations, such as involving students, teachers and parents in the development of a whole-of-school approach to understanding, preventing and dealing with all forms of bullying, including cyber-bullying; providing teachers and parents with access to training in this and other internet safety issues; ensuring schools continually update anti-bullying policies as technologies evolve and addressing the root causes of all forms of bullying, including cyber-bullying.

27. School Based Police Officers (SBPOs) within the Northern Territory Police Crime Prevention Division have a significant role in the investigation of cyber-bullying complaints and the delivery of personal safety instruction to children. SBPOs have been delivering cyber-bullying education awareness presentations in Northern Territory schools since 2008. This is complemented by the immediate and thorough investigation of all complaints relating to cyber-safety made within the school environment.

28. While cyber-bullying is a problem that can have a profound impact on victims, the sample size of cyber-safety incidents in the Northern Territory is not sufficient to provide an objective analysis, however, it would be sufficient to say that there has been increase in incidents as children gain greater access to ICT and internet service and carriage providers.

29. The ease with which children can access social network sites and other carriage services (text and land-line) is of concern given that many are rarely monitored or controlled by parents, families or carers. This allows anyone to make threats, stalk another person, make racist or sexist remarks, or denigrate another person with anonymity which causes genuine fear to the victim particularly when they are unable to identify the offender.

30. Some of the effects cyber-bullying has on its victims range from apprehension or fear (the fear is real and indicators are obvious, mood/behaviour changes, heavy breathing, crying) and personality changes, which can affect home and social life including refusal to go out in public or attend school and in many cases results in the significant decline in school grades.

31. With the assistance of SBPOs, all incidents relating to cyber-safety in Northern Territory Schools are addressed and include requirements for parental support and information on the consequences for misuse of carriage providers. Education and encouragement is also provided to parents, families, and carers to become more conversant with the cyber-environment and to actively monitor what their children are accessing on the internet.

32. Northern Territory schools also have policies in place on bullying including cyber-bullying that are aligned to the Safe Schools Northern Territory Code of Behaviour. All schools require parents and students sign an acceptable use agreement which covers in general terms the inappropriate use of online environments including bullying and harassment. Positive Behaviour Advisors in schools are also teaching Student Representative Councils and School Captains about cyber-bullying with the expectation that they will then share with their schools (Government, Catholic and Independent).

33. The Northern Territory's Department of Education and Training is also developing a Professional Learning on Demand Module in Cyber-Safety for its educators to undertake in 2011. The module includes information on cyber-bullying, online reputations and cyber-stalking.

34. The NTG considers that all governments have an important role in the development of policies and programs to prevent and deal with all forms of bullying, including cyber-bullying; and for ensuring that their schools are appropriately supported and resourced to provide teachers and parents with access to training in cyber-bullying and other internet safety issues.

Inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of eating disorders, drug usage, underage drinking, smoking and gambling).

35. The NTG is aware of a growing incidence of cyber-safety issues associated with mobile phone technology amongst children and young people in remote Indigenous communities, where the use of mobile phones as a method of communication is far greater than the internet.

36. 'Sexting', or the distribution of self-created sexually-explicit photographs and videos via mobile phone communication, has become a growing trend amongst young people worldwide in recent years [Porter, 2008]. A danger associated with sexting is that material can be easily and widely distributed without the originator's consent. Both the Department of Health and Families Safe Places program and the National Association for the Prevention of Child Abuse and Neglect (NAPCAN) are reporting parental and community concerns about the increasing prevalence of sexting and bullying via mobile phone communication and the impact it is having on Indigenous children and young people.

37. The NTG encourages the Committee to further investigate the use of mobile phone technology in the propagation of 'sexting' and bullying, including amongst Indigenous children and young people, as part of its Inquiry.

Identity theft.

38. Identity theft is not prominent amongst children in the Northern Territory; however, there is a noted increase in the illegal access of email accounts and the creation of social networking pages without the owner's permission. A further concerning factor is the increase in incidents of physical assaults being recorded and uploaded to web based sites (e.g. You Tube and Facebook).

39. Currently, there are no specific offences in the Northern Territory relating to card-skimming or identity theft. While the Northern Territory Criminal Code could be used to prosecute identity crime, the absence of specific offences creates some uncertainty in this area. The NTG is currently considering options to address credit card skimming and identity theft offences.

Australian and international responses to current cyber-safety threats.

40. Child sexual abuse, including the production and distribution of child pornography, has a devastating impact on children, families and the community. The NTG is strongly of the view that all efforts, including legislative, law-enforcement, corporate, community-based, and educational initiative strategies that are in place to mitigate this crime need to be supported and encouraged.

Legislative Responses

41. A number of international jurisdictions have introduced legislation to prevent the exploitation of children in the cyber-environment, including the *Stop the Online Exploitation of Our Children Act* (USA) which requires social networking sites to ban offenders. In Europe, states have agreed to a *Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse.* Most Australian jurisdictions have introduced legislation to prevent online child grooming.

42. There are a number of cross jurisdictional issues which can complicate legislative approaches to dealing with internet-based child exploitation. For example, some countries do not have any online grooming legislation, the age of consent varies across countries and some countries have anti-child pornography legislation while others do not. The lack of consistency in legislation internationally impedes police investigations.

43. National and international initiatives that have been established to overcome some of the problems that have in the past made policing of the internet especially difficult require concerted support. These initiatives can facilitate the investigation of cyber-based crimes against children, the lawful collection of evidence and the prosecution of cases. For example, the Australian High Tech Crime Centre facilitates cooperation amongst law enforcement agencies across Australia to overcome jurisdictional issues at an early stage. Similarly, the Australian Federal Police Liaison Officer Network and Interpol provide international cooperation. These initiatives should continue to be fully supported.

44. Other international initiatives, such as the Combating Paedophile Information Networks in Europe (COPINE) and Interpol, which help to identify both victims and perpetrators of child pornography around the world [Krone, 2009], should receive recognition for the important work they do, and where possible, Australian agencies should be supported

to work in collaboration with these organisations/agencies and/or supported to develop their own similar initiatives.

45. Additional legislation could further protect children from cyber-based sexual predators, such as the regulation of the behaviour of sexual offenders on release from prison, sex offender registration and community notification, and the requirement that online operators remove offenders from social networking sites. However, it is imperative that the disparities in legislation across countries is addressed in a concerted and unified manner if advances are to be made in keeping children safe on the internet [Choo, 2009].

46. Where legislation is in place, it should be reviewed and amended if necessary to reflect the seriousness of the crime. For example, under s 578B (2) *Crimes Act 1900* (NSW) relating to offences of possessing child pornography and publishing child pornography under 578C (2A) of the Act, the maximum penalty is the equivalent of $11 000, two years imprisonment or both. The maximum penalty for the publishing child pornography is $110 000 or five years imprisonment or both [Krone, 2009].

47. A review of the sentencing from January 2000 to December 2003 revealed that of the 62 cases dealt with by the local court for the offence of possessing child pornography, 48 per cent were convicted and placed on a bond, with fewer than half of these being subjected to supervision as a condition of the bond. Suspended sentences were handed down in 9 cases and only 8 cases resulted in full-time custodial sentence (the average sentence being 6 months). Of the 11 cases dealt with for the offence of publishing child pornography, 5 were placed on a bond (only two of these cases were subject to supervision as a condition of the bond). In 2 cases the offenders were required to perform community service. One case saw the offender sentenced to a custodial sentence (three months) and one offender received a fine [Krone, 2009].

48. Given the devastating impacts on children and the community at large and the escalation in occurrences of the production and distribution of child pornography, serious consideration needs to be given to reviewing and amending the penalties associated with these crimes to reflect their seriousness.

International Police Taskforces and Specialist Units

49. The use of police task forces and specialist units enables collaboration with international counterparts including much-needed intelligence sharing. Australian authorities have played and continue to play a role in these taskforces (for example, the Australian Federal Police Online Child Exploitation Team is involved in the investigation and coordination of multi-jurisdictional and international cyber-related child sexual exploitation).

50. Unfortunately, given the extensive scale of the problem of internet-based child pornography and other forms of online child sexual exploitation worldwide, the number of actual arrests is relatively low. It is considered that taskforces and specialist units relating to online child sexual exploitation should be given high priority within law enforcement in general and that they need to be well resourced in order to address the growing problem.

Hotlines and Online Reporting

51. Current Australian strategies could be significantly enhanced by the adoption of additional services to address this problem with excellent examples found internationally, for example, the establishment of hotlines such as the Internet Hotline Providers in Europe (INHOPE). Hotlines can be effective in providing an avenue for public complaints and tip-offs about alleged illegal content and use of the internet, collecting intelligence for law enforcement agencies, removing illegal content from service providers, exchanging information and good practice, providing safety advice to consumers and promoting community awareness [Williams, 1999].

52. Given the growing nature of the problem of cyber-based child exploitation, consideration should be given to the adoption, expansion and widespread publication of an Australian cyber-safety hotline (based on, for example, the INHOPE hotline), similar in operation to the Crime Stoppers hotline. Internet-based initiatives that seek to overcome cyber-based exploitation of children, such as the website www.afp.gov.au/policing/e-crime.aspx, where individuals can report child exploitation, should also be supported and appropriately resourced.

Filters

53. A number of countries have introduced internet filtering to restrict access to websites that host illegal and / or objectionable material, including child exploitation (for example, China, Syria). However, such initiatives have been criticised as ineffective, expensive, cumbersome technologically and/or potentially undermining of democratic principles through potential political censorship.

54. The issue has received widespread media attention in Australia with a number of large-scale campaigns calling for the rejection of such a filter. While 'server-side' filtering is highly contentious and problematic on multiple levels, 'client-side' filtering (where the responsibility for blocking potentially objectionable materials lies with the individual user and his/her home computer rather than the internet service or content provider) offers promise to parents, teachers, and others who have care and responsibility for children. There is a significant role for information technology and security researchers to develop filtering software that is effective and non-cumbersome.

Ways to support schools to change their culture and reduce the incidence and harmful effects of cyber-bullying.

55. One of the most crucial strategies for protecting children from the dangers of the internet and other technological communication devices, such as mobile phones, is education. It is imperative that education programs are designed for and delivered to children of all ages to address this issue. Children need to be educated about the dangers of the internet as due to their age and limited experience, children are generally far more trusting and naïve than adults. They are therefore especially vulnerable to the strategies and tricks employed by sexual predators in an online environment.

56. Children need to be educated about the obvious dangers of the internet, such as disclosing personal information to 'friends' they meet online, making arrangements to meet online 'friends' in person, sending or receiving personal or intimate photos of themselves to online 'friends', on social networking sites, or on mobile phones. Children also need to be educated about the other dangers of the cyber-environment that are not so obvious, such as the impact of viewing sexually explicit material before they are mature enough, or engaging in sexually loaded 'chats' for 'fun'.

57. Other important considerations include children's rights and responsibilities when using the internet and other communication devices, including bullying prevention, and avenues for reporting inappropriate and/or illegal activity. Cyber-safety should be a high priority in the education system, given the numbers of children who use the internet and other electronic communication devices. Serious consideration should be given to incorporating this topic into the national curriculum, in addition to the provision of funding to organisations already involved in the education of children on topics of sexual abuse prevention (for example, Bravehearts Inc) to expand their program to include online safety for children [Bravehearts Inc, 2008].

The role of parents, families, carers and the community.

58. Public education is essential. Research indicates that many adults, particularly parents, are far less computer savvy than their children [Webwise, 2006]. There is concern about the lack of knowledge and resources currently available to families and communities to develop appropriate responses to issues such as sexting and cyber-bullying.

59. While parents can perform a monitoring role and give their children information and guidance on cyber-safety, it is equally as important that they have access to education and training on how they can protect their children online and how they can teach their children safety strategies when using the internet. The education of parents will need to be increased as a result of Building the Education Revolution 1:1 rollout of computers to students in years 9-12.

60. Training and education would ideally include communicating with their child and providing information about reporting cyber-safety issues. Programs could be made available from a range of child-related settings, such as child care centres and pre-schools, primary and secondary schools and other relevant community child and youth-based organisations. Given the rapid changes in technology, it is imperative that education and training programs are resourced appropriately so that they can be accessed by all who need it and can be reviewed and updated as necessary.

References

BBC Online (2006). Sites selling child porn targeted.
http://news.bbc.co.uk/2/hi/technology/4812962.stm

Bravhearts Inc. (2008). Program Evaluation: Ditto's Keep Safe Adventure Program.
Braveharts Incorporated. Australia.
http.www.bravhearts.org.au/docs/dksa_evaluation_2008.pdf

Choo, K-K. R., (2009). Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences. Australian Institute of Criminology Reports, Research and Public Policy series, 103, xii.

Cross, D. et al (2009). Australian covert bullying prevalence study. Perth. Edith Cowan University. www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx

ICMEC (2010). Global Campaign Against Child Pornography, International Centre for Missing and Exploited Children (ICMEC)
http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=1742

Krone, T (2005). International Police operations against child pornography. Australian Institute of Criminology. Canberra. Trends and Issues in Crime and Justice. Issue 297.

Krone, T (2009). High Tech Crime Brief No. 2 : Child Exploitation. Canberra: Australian Institute of Criminology.

Krone, T (2009). High Tech Crime Brief No. 8 : Child pornography sentencing in NSW. Canberra: Australian Institute of Criminology.

Lenhart, A. & Madden, M (2007). Social networking websites and teens: An overview. Washington, DC: Per Internet and American Life Project.

National Centre for Missing and Exploited Children (2006). Google joins industry –wide movement to combat child pornography
http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2629

Porter, L. (2008). Malice in Wonderland. The Age: Extra. 10 August, 18

Rush, E., & La Nauze, A. (2006). Corporate Pedophilia: The sexualisation of children in Australia. Discussion Paper Number 90. The Australia Institute.

Smith, P. et al (2008). Cyberbullying: Its nature and impact in secondary school pupils. The Journal of Child Psychology, 49 (4), 376 – 385.

Webwise (2006). Survey of children's use of the internet.
http://www.webwise.ie/GenPDF.aspx?id=1389

Wolak, J. Mitchell, K. & Finkelhor, D (2006). Online victimisation of youth: Five years later. Alexandria, VA: National Center for Missing and Exploited Children.

World Day Against Cyber Censorship (2010).
http://www.itnews.com.au/News/169456,global-campaign-seeks-to-crush-web-censorship.aspx

Williams, N (1999). The contribution of Hotlines to combating child pornography on the internet. Childnet International. London.

Ybarra, M. L, Espelage, D. L., and Mitchell, K. J. (2007). The co-occurrence of internet harassment and unwanted sexual solicitation, victimisation and perpetration: Associations with psychosocial indicators. Journal of Adolescent Health, 41 (6), 1, 31-41.