SUBMISSION No. 34

BRAVE HEARTS

"Protecting children against sexual assault"

Monday, 28 June 2010

The Secretary
Joint Select Committee on Cyber-Safety
Attorney-General's Department
R1-109, Parliament House
PO Box 6021
Canberra, ACT 2600
E-mail: jscc@aph.gov.au

Submission: Inquiry into Cyber-Safety

To whom it may concern:

Bravehearts Inc is a not for profit organisation dealing exclusively and specifically with child sexual assault. Bravehearts has been operating for over 12 years providing child focused healing and preventative strategies including comprehensive therapeutic, support and education programs. In addition, we are heavily involved in legislative reform and research. Based in Queensland, Bravehearts has branches in Brisbane, the Gold Coast, Cairns, Shepparton and Sydney.

As an agency that is focussed on lobbying for policies and legislation in relation to child sexual assault, Bravehearts is actively involved in promoting cyber-safety, both through our own activities and our involvement in the Federal Government's Cyber-Safety Consultative Working Group. Concerns around cyber-safety and children and young people have grown over recent years, gaining much prominence in media and political debates. The issues are wide and varied, from e-security, on-line fraud and cyber-bullying through to risks in relation to sexual exploitation and grooming of children. We provide this submission with particular attention paid to issues relating to on-line risks in relation to the sexual exploitation and grooming of children.

The recommendations set out in our submission are:

1. Bravehearts advocates for structured, consistent and thorough curriculum-based teaching of Internet safety within our school environments
2. Bravehearts advocates for a National **'Tick, Tech, Know'** campaign raising awareness and providing information on safe Internet usage targeted to

three sectors of the community: children and young people, parents and the general public

3. Bravehearts advocates that Government actively engage with public libraries and commercial businesses, where children and young people may access the Internet to ensure that adequate protections are in place against identified cyber-threats
4. Bravehearts supports the introduction and promotion of programs aimed to provide treatment and support for on-line child sex offenders.
5. As part of an holistic approach to addressing on-line threats, Bravehearts supports the ISP level filtering of Refused Classification rated websites.
6. Bravehearts recommends an alert page replace blocked websites that provides options for the user to contact should they believe the site should not be blocked, or in the event that they wish to seek assistance with their behaviour or thoughts.
7. Bravehearts supports the development of a Cyber-Safety Help Button, and advocates that the Help Button be made mandatory in schools and libraries.
8. Bravehearts advocates that the Australian Government actively engage with overseas Governments to work towards consistency and strengthening of responses to a crime that knows no boundaries.
9. Bravehearts advocates for the continuation of the Federal Government Consultative Working Group on Cyber-Safety.
10. Bravehearts recommends a National Law Enforcement Cyber-Safety Taskforce be established to strengthen current jurisdictional responses to cyber-crime.

For child sex offenders advances in on-line technologies are continuing to provide increased opportunities; including for grooming victims, accessing child exploitation material and networking. Bravehearts believes that to address on-line threats to children there needs to be a *concerted, collaborative and holistic approach* from Federal and State governments, Federal and State policing and regulatory agencies, those working within the on-line environment (including ISPs, and social networking sites), media and on-line oversight bodies and those in the child protection sector. The ultimate aim must be to ensure the safety and protection of children in the on-line environment with an underlying emphasis on the best interests of children.

The On-line Environment in which Children Currently Engage

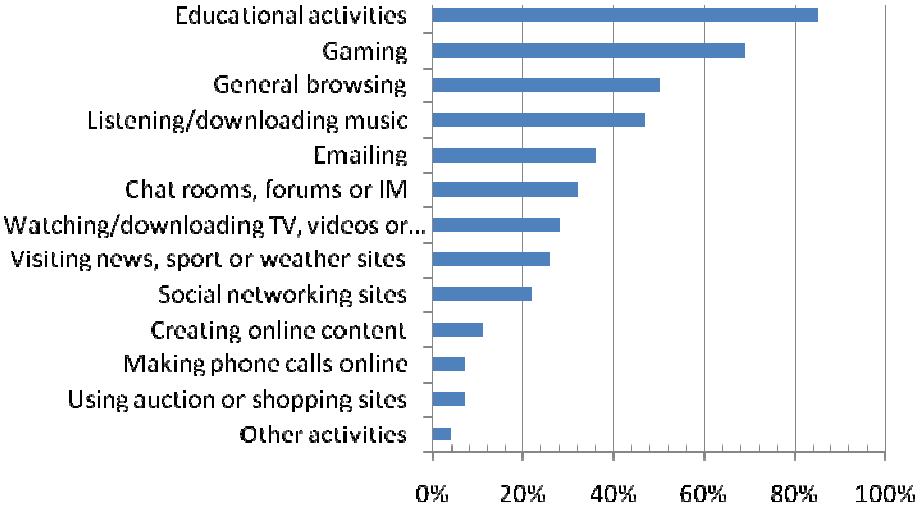
Children use the Internet in different ways and for different reasons depending on their age and particular circumstances and interests. Typically:

- *Pre-School Aged Children:* This age group are just beginning to learn how the computer works. Their on-line activity may include visiting children's websites and communicating with family and friends through e-mails.
- *Primary School Aged Children:* Children of this age feel more confident using other services provided by the Internet such as chat rooms, with some deciding to search for prohibited material.
- *High School aged Children:* For high-school aged children the Internet is a necessity to assist with research for projects and homework. This age group will be asserting more freedom and independence while using the Internet,

and they will increasingly use the on-line environment as a social tool. Young people may also feel they want to explore prohibited material.

Findings from the Australian Bureau of Statistics' publication "Children's Participation in Cultural and Leisure Activities" (2009), provides a picture on the usage of the Internet by children and young people in Australia. Data showed that from April 2008 to April 2009 around 2.2million children accessed the Internet. Internet usage varied over age with 59.9% of 5 to 8 year olds accessing the Internet compared with 88.5% of 9 to 11 year olds and 95.5% of 12 to 14 year olds.

The following graph has been produced from the data available in the ABS report (2009). The most popular on-line activities for children between the ages of 5 and 14 years include educational activities (85%), on-line gaming (69%) and listening or downloading music (47%). Using the Internet for social interaction were also popular activities: e-mailing (36%), accessing chat rooms or instant messaging (32%) and utilising social networking sites (22%).



While the ABS data show that the majority of children under the age of 14 are accessing the Internet for educational purposes or for on-line gaming, an ACMA study (2008) it found that 72% of girls and 52% of boys between the ages of 14 and 17 years have personal profile pages set up on social networking sites such as Facebook and MySpace.

The majority of children accessed the Internet at home (92%) or at school (86%), with 45% of children also accessing the Internet at other locations (such as public libraries, Internet cafes etc) (ABS, 2009). In addition, the study found that while around 76% of 12 to 14 year olds had a mobile phone, only around 4% of children used their mobile phone to access the Internet during the time period covered by the survey (ABS, 2009).

This emphasises the issue that in protecting children from on-line threats, we must be cognisant that children access the Internet within a range of environments and

ensure that adequate frameworks are in place to assure, as much as possible, the protection of children wherever they are accessing the Internet.

Generally, it is crucial that we engage with children and young people – from an early age – to instil safe practices and habits for Internet usage. Children and young people should be taught cyber-safety as a matter of course. With around 2.2million children actively engaging on-line, we need to resource our education system to effectively respond to this environment where children are increasingly spending substantial time.

Our schools have the capacity to reach large numbers of children at the one time. In schools children are taught how to stay safe in traffic, how to stay safe from fire, water and electricity and increasingly personal safety programs; it is logical that schools should progress to also teach children how to stay safe on-line.

1. Bravehearts advocates for structured, consistent and thorough curriculum-based teaching of Internet safety within our school environments.

With 92% of children accessing the Internet while at home (ABS, 2009) it is absolutely vital that parents and carers are aware of the potential on-line threats to children, openly engage with their children about their Internet usage and are active in protecting their children on-line.

However, while it is notionally true that parents and carers must take ultimate responsibility for educating and protecting their children, it is also true that the internet and new communication technologies are becoming increasingly foreign to many parents thus reducing their ability to protect their children. The reality is that more often than not, children know more about the internet and mobile phone technologies than adults do. Continuing calls for parents to educate themselves are falling on the predominately 'out of their depth', baffled and frightened ears of parents and carers.

The truth is that new and rapidly emerging technologies are increasingly leaving parents and carers behind.

Bravehearts believe that the best way to protect children is to inform adult through a television and radio campaign that delivers easy to understand basic information: **'Tick, Tech, Know'** – Take a **tick** to learn the **Tech** and **know** how to keep safe. We are confident that through quick infomercials, aimed at kids and adults, accurate and useful information delivered in a simple, easy to understand, engaging and informative way will work. After cursory conversations of agreement, we would propose this Bravehearts initiative in collaboration with the ANZPAA Child Protection Committee and/or the Australian Federal Police.

General community-based education campaigns are an essential component of an effective and holistic approach to cyber safety. With data showing that almost half of

children (45%, ABS 2009) access the Internet outside of the home and school environment, it is crucial that National, broad-level campaigns focus on raising awareness on Internet risks and management of those risks.

The International Safer Internet Day in February is an ideal opportunity to emphasise the focus on managing on-line threats, but a more consistent and targeted campaign is needed. A broad campaign should include advertising safety messages via television, print and the Internet.

2. Bravehearts advocates for a National **'Tick, Tech, Know'** campaign raising awareness and providing information on safe Internet usage targeted to three sectors of the community: children and young people, parents and the general public.

Children and young people are accessing the Internet in environments that may not have the same level of controls that a parent or school may implement; from friend's homes where rules and supervision may differ to that in the child's home, to Internet cafes, public libraries, commercial businesses (such as coffee shops and book stores). Children and young people may, for example, set up a personal page on a social networking site, and then access this page from an Internet cafe against their parent's knowledge.

It is essential that we identify the various environments through which children and young people access the Internet and work cooperatively to put in place policies and processes aimed at increasing the level of protection for children. We need to ensure, as much as possible, that these environments are as safe as possible for children and young people. For example, Internet cafes may section off computers that have the appropriate filters against adult material or sites for use by children under the age of 16.

3. Bravehearts advocates that Government actively engage with public libraries and commercial businesses, where children and young people may access the Internet to ensure that adequate protections are in place against identified cyber-threats.

The Nature, Prevalence, Implications of and Level of Risk Associated with Cyber-Safety Threats

In relation to child sexual assault, there are a number of on-line threats to children and young people:

- *Exposure to inappropriate material, such as pornography or violence*
  Children and young people access the Internet for a wide variety of reasons. In navigating cyberspace and searching for information on a wide range of topics, children and young people are at risk of exposure to inappropriate material, such as pornography or violent material.

A 2006 study by the National Centre for Missing and Exploited Children and the Crimes Against Children Research Centre, indicated a marked increase in the proportion of young people being exposed to unwanted sexual material. The survey found that more than a third of young people had been exposed to sexual material over a twelve-month period; an increase from a quarter who had disclosed seeing unwanted sexual material in the previous study. The authors reported that this increase occurred 'despite the use of filtering, blocking and monitoring software in the households of youth Internet users'.

Statistics from an Australian survey of 200 Australian youth aged 16-17, showed higher rates of unwanted exposure to on-line sexual material with 84% of males and 60% of female respondents reporting inadvertent exposure (cited in Bryant, 2009).

Technology provides parents with the option to install filters on their computers to reduce the risk of exposure to inappropriate material, but it must be integrated with education for best results. While filters are popular technology-based tools, they are inherently imperfect, and may allow some inappropriate material to leak through to a child. It is important to note that an adult who relies primarily on filters to protect their child may think the child is "safe" when, in fact, the risk of exposure has only been reduced, not eliminated. Therefore, regardless of whether filters are used, a child must learn how to deal with inappropriate material they may come across on-line.

- *Physical dangers, such as meeting up with strangers met on-line*
  Meeting and corresponding with new people is an exciting aspect of the on-line world. The Child Exploitation and On-line Protection Centre in the United Kingdom found that of the eight million children in the UK with Internet access, a staggering one in twelve have admitted to meeting someone, who they initially met on-line, offline (2007). Similar findings (cited in Choo, 2009) reported that 7% of young people reported that they had met someone offline after meeting them on the Internet.

  Unfortunately, not everyone is honest about who they are and children and young people can be particularly susceptible to trusting people on-line. The reality is that there are predators who pretend to be a young person in order to befriend and gain the trust of children and young people. Twenty-four percent of the young people in findings discussed in Choo (2009) reported that the person they met had presented themselves as a child on-line, but had turned out to be an adult.

  We need to teach our children that just as we learn to protect ourselves from strangers in the off-line world, we need to do the same on-line. Children and young people often feel that they know someone simply because they have talked to them on-line. However it is easy to pretend to be someone you are not and meeting someone you have met on-line is one of the most dangerous things that a young person can do.

Parents should ensure that if a child wants to meet with someone they have befriended on-line that the parent speaks to the other person's parents first and accompanies them to a public place to meet.

- *Exposure of personal information and privacy*
  It is also important that children understand how important it is to ensure that they do not publish any information that will identify them. Children and young people should be taught not to give out their full name, address, phone number or other identifying information such as the name of their school as this type of information can be used by predators to identify who the child is and where they are.

  A study reported by i-Safe (2006) found that 49% of high school student admitted to posting personal information on-line that could assist a stranger in identifying or locating them; including their full name, address and date of birth. These findings have been found similar studies, with one study finding that almost one-third of young people aged between 7 and 17 were willing to disclose their home address on-line, with 14% will to post their e-mail address (Ropelato cited in Choo, 2009)

- *Exploitation*
  There are a number of ways in which people may exploit children on-line. Some people will misuse information that a child or young person gives them. For example, people may begin to send explicit or abusive messages or post photos of the child or young person on other websites.

  Statistics on the number of children receiving on-line solicitations are alarming. The United States department of Justice reported that one in five children who use the Internet had been approached by a sex offender (cited on Protect Your Children On-line, www.privateclienttechnologies.com). The Child Exploitation and On-line Protection Centre (2007) in the UK reportedly received 400 phone calls a month from young people reporting they have been approached by a sex offender on the Internet. Ybarra, Espelage & Mitchell (2007) found that 35% of young people aged between 10 & 15 reported being harassed on-line or receiving unwanted sexual solicitations (15%) at least once over a twelve-month period.

  Not giving out identifying information (as discussed above) is key to protecting children against exploitation. In addition, it is important that children know that any images they upload to the Internet can be downloaded by someone and passed around. Before posting any photos of themselves children and young people should ask themselves, how they would feel about people seeing it. Parents should talk to their children about the risks of sharing photos and how to safeguard against these risks. Most social networking sites have privacy settings that allow children and young people to stipulate who can access their photos.

Children and young people should also be taught to not respond to e-mails or messages that are explicit, abusive or inappropriate. On-line contact where someone is asking a child or young person to engage in a sexual conversation or activity or asking them to send a sexually explicit image is a form of exploitation. Children and young people should be advised to not respond to these types of contact and to block or delete that person from their friend list. Parents should encourage children to let them know if this happens as these types of communication should be passed on to the authorities.

Child Exploitation Material & Offline Behaviours

While the production, dissemination and access to, child exploitation material are not new, the explosion of Internet technologies has meant that the problem of child exploitation material has grown exponentially (Taylor & Quayle, 2003).

The Supreme Court of Canada outlined the risks of the availability of child exploitation material in a challenge to the child pornography provisions in the Canadian criminal code (*R v. Sharpe, 2001)*. In its ruling the Canadian Supreme Court outlined the "heightened risk of attitudinal harm" and evidence of "the connections between the possession of child pornography and harm to children" (*R v. Sharpe, 2001)*, including the promotion of cognitive distortions that serve to normalise sexual activity between adults and children and the incitement of sexual fantasies that motivate adults to offend against a child (Clough, 2008).

Although there can be seen to exist a correlation between pornography usage and child molesting, it is much more difficult, if not impossible, to prove an actual causal link between the two. Experts differ over any causal link, with some experts saying that use of child porn reduces the risk of offending through providing an outlet for sexual fantasies involving children, while others arguing that it increases the risk of off-line offending.

Some of the research in this area includes:

- Marshall (2000) argues that while there is no evidence that exposure to child pornography has a causal relationship to off-line sexual offending, it can impact on psychological processes and augment offenders' cognitive distortions.
- In data from 39 Internet offenders, Galbreath, Berlin and Sawyer (2002) found 33% had attempted to meet a child or young person offline.
- In findings from the *National Juvenile On-line Victimisation Survey*, Wolak, Finkelhor and Mitchell (2005) found that 40% of on-line child pornography offenders were "dual offenders"; that is they were found to both possess on-line child pornography and have had sexually victimised children.
- Seto, Cantor and Blanchard (2006) reported that men charged with child pornography offences showed a greater sexual arousal to children than men charged with contact sexual offences against children and those charged with sexual offences against adults.
- 80-85% of inmates convitced of possessing or distributing child pornography admited they had sexually offended against children after they had

completed treatment. This is compaired to only 26-45% admitting sexually offences against children at the time of sentencing (USAToday, 16th April, 2008)

- In a longitudinal study of convicted child sex offenders (n=341) in the United States, Kingston, Fedoroff, Firestone, Curry and Bradford (2008) found:
    - that there was a significantly higher risk of sexual reoffending for higher-risk offenders who viewed pornography
    - highly deviant pornography was significantly correlated with increased in sexual reoffending for all child sex offenders
- Several studies found that one in four men arrested for possessing child pornography also had a history of sexually offending against children (Bourke & Hernandez, 2009).

It is essential that responses to cyber-threats, include intervention and preventative measures aimed at child sex offenders. Resources need to be placed into programs that target on-line offenders.

Evidence from the Stop It Now! programs run in the United States and the United Kingdom show that potential offenders will call for help:

- A four-year evaluation of the Stop it Now! program in Vermont (Stop It Now!, 2000) showed that of the 657 calls received over the four year period, 99 (15%) were from self-identified abusers, seeking help.
- While the Stop It Now! program does not have a formal system for tracking the number of self-identified abusers who go on to seek support or treatment, it is suggested that there is anecdotal evidence that this occurs: "According to clinicians (surveyed by Stop It Now!), 118 people have voluntarily sought out help for their sexually abusive behaviours (20 adults and 98 adolescents)… 15 adults and 10 adolescents have turned themselves in to the legal system (Stop It Now!, 2000).
- In the UK Stop It Now! has dealt with 13,803 contacts (13,169 calls and 634 e-mails):
    - 48% from abusers/potential abusers
    - 28% from Internet offenders/potential Internet offenders (Stop it Now! UK & Ireland, 2009)

4. Bravehearts supports the introduction and promotion of programs aimed to provide treatment and support for on-line child sex offenders.

Australian and International Responses to Current Cyber-Safety Threats

Filtering

Data on on-line child pornography suggests that there is an estimated 20,000 images of child pornography posted on-line each week (National Society for the Prevention of Cruelty to Children, 2003) with over 100,000 websites offering child pornography (*The Australian*, 8th January 2008). In June 2008, as a result of Operation Centurion,

the Australian Federal Police announced that Federal and State police had seized one million child exploitation images in coordinated raids across the country.

Along with these frightening figures the debate on the Government's ISP-level filtering scheme continues. What is clear is that to date the regulation of the Internet has been largely lax and there needs to be some level of governance in terms of rules and what type of information is ultimately available on-line.

Bravehearts supports the mandatory ISP level filtering of illegal material that is currently already blacklisted by the Australian Communications and Media Authority. It is our position that material that is rated as RC (refused classification), including child pornography is material that breaches Australian laws and is illegal to produce, own and distribute. As such, this material should not be made available on-line.

In addition, we support a second tier of filtering that allows families, organisations or businesses to optionally request filtering of other material that may be objectionable. These sites may include those that promote terrorism, suicide, drug use, or adult pornography.

5. As part of an holistic approach to addressing on-line threats, Bravehearts supports the ISP level filtering of Refused Classification rated websites.

Concerns have been expressed to Bravehearts that the mandatory filtering scheme will result in a loss of information gathering by policing authorities. Intelligence from monitoring these websites has assisted in the identification of both offenders and victims. In 2006 Interpol reported that on-line investigations had resulted in rescuing 426 victims of on-line child pornography images from the 475,899 images in Interpol's database (Griffith & Simon, 2008).

It is absolutely essential that information from sites that are identified and blocked be made available immediately to Police to act on. CIRCAMP, an internet filtering system that is managed by Police, has been suggested to Bravehearts as a system that the Government should look into. Experience of this system has shown it to be a successful model for filtering that allows Police to maintain information on websites (see Attachment 1).

It is important for Government and industry to acknowledge that no filtering system is foolproof and that technology savvy individuals may circumvent it. The limitations of the mandatory filtering of child pornography websites need to be acknowledged and subsequently addressed. Peer to Peer (P2P) networks and Internal Relay Chat (IRC) rooms are alternative methods that on-line offenders utilised to share images and videos. For example, on-line offenders may set up a subscription-based private IRC room where they are able to stream live child sexual assault videos to paying participants. It is essential that (a) Government work with industry to identify and limit on-line opportunities and (b) that adequate resourcing be provided to specialised policing units to monitor and respond to these threats.

On-line Alerts

It is our position that when a site is blocked a page should replace the site alerting the individual that the site they have attempted to access has been blocked because its content is illegal and has been Refused Classification and providing details for support and advice, for example:

ALERT

The website your Internet Browser is attempting to connect with has been Refused Classification under Australian Law and may contain illegal images of child exploitation.

If you believe that this site has been blocked in error, please contact ACMA on XXXXXXX

If you were purposively seeking access to images of child exploitation and would like to speak to someone about your thoughts or behaviours towards children, please contact Stop It Now on XXXXXX

We believe, given the data from Stop It Now (US & UK) (provided earlier), that it is important to provide individuals who are attempting to access these sites the opportunity to seek help. Stop It Now is a program being adopted by Phoenix House in Bundaberg.

6. Bravehearts recommends an alert page replace blocked websites and provides options for the user to contact should they believe the site should not be blocked, or in the event that they wish to seek assistance with their behaviour or thoughts.

Help Button

On-line reporting and monitoring systems are important tools in responding to child exploitation. The use of reporting hotlines provides an alternative to reporting to law enforcement agencies, as many people may be reluctant to report illegal content directly to the Police.

As part of the Federal Government Cyber-Safety Consultative Working Group, Bravehearts is aware of the development of a Cyber-Safety Help Button. We thoroughly support this initiative and advocate that this be mandatory on computers in schools and libraries, as well as being marketed towards families and businesses.

7. Bravehearts supports the development of a Cyber-Safety Help Button, and advocates that the Help Button be made mandatory in schools and libraries.

Legislative Responses

Australian Commonwealth and State legislation plays a vital role in protecting vulnerable children from sexual exploitation. The need to legislate for offences that lead to child sexual assault or child exploitation cannot be underestimated.

Legislating for grooming and preparatory offences allows authorities to step in, in order to protect children before they come to any physical or sexual harm, that is it will enable action to be taken before any sexual activity takes place when it is clear this is what the adult intends. For example, there are concerns that offenders convicted for indecent image related offences who may be assessed as 'low risk' may actually constitute a higher risk in terms of their propensity for contact abuse.

For paedophiles on-line technologies have presented alternative avenues of operation, including the opportunity to organise informal networks on a global scale. There is little doubt that the explosion in Internet accessibility and other communication carriage devices (including mobile phones and traditional postal services) and improved usability of these in recent years has made child sexual assault material more available to more people, has given offenders more opportunity to share more images, and has enabled these and other individuals to contact children previously unknown to them as never before. While most Australian jurisdictions have legislation in place that criminalises on-line child grooming, there remains a lack of consistency, both in relation to covering substantive offences as well as in sentencing.

These problems in legislative consistency are even greater when considering that on-line offending often occurs across countries. The Australian Government needs to actively engage on an international level; although we have relatively comprehensive legislative frameworks, disparities with and among countries will continue to create risks.

8. Bravehearts advocates that the Australian Government actively engage with overseas Governments to work towards consistency and strengthening of responses to a crime that knows no boundaries.

Consultative Working Group

The collaboration of Government, industry, child protection specialists and policing bodies is fundamental to ensuring and holistic and effective response to cyber-safety.

9. Bravehearts advocates for the continuation of the Federal Government Consultative Working Group on Cyber-Safety.

Law Enforcement

Bravehearts believes that it is crucial that law enforcement and policing and security researchers contribute to a safer on-line environment. Adequate resourcing must be prioritised to specialist police units to respond to and address on-line child exploitation threats.

Partnerships between police jurisdictions must be strong to ensure cooperation and free flow of information between agencies. Groups such as the Cospol Internet Related Child Abusive Material Project (CIRCAMP) and the Virtual Global Taskforce

are examples of collaboration between international policing agencies. A similar Taskforce consisting of representatives from specialist units from each of the Australian jurisdictions would assist in better communication and collaboration across the country, strengthening Australia's response to cyber-crime.

10. Bravehearts recommends a National Law Enforcement Cyber-Safety Taskforce be established to strengthen current jurisdictional responses to cyber-crime.

In conclusion, we thank the Committee for the opportunity to provide comment to the Joint Select Committee on Cyber-Safety and look forward to hearing the outcome of this process. Please contact us if further information or clarification is required. Bravehearts would be happy to consult further around these issues if requested.

Warm Regards

Hetty Johnston
Founder & Executive Director

Carol Ronken
Criminologist, BA (psych), MAppSoc (social research)
Research and Policy Manager

References:

Australian Bureau of Statistics (2009). *Children's Participation in Cultural and Leisure Activities*. Canberra [ACT]: Australian Bureau of Statistics.

Australian Media and Communications Authority (2008). *Internet Use and Social Networking by Young People*. Canberra [ACT]: Australian Media and Communications Authority.

Bourke, M. & Hernandez (2009). The 'Butner Study' Redux: A report of the incidence of hands-on child victimisation by child pornography offenders. *Journal of Family Violence, 24*(3): 183-191.

Bryant, C. (2009). Adolescence, pornography and harm. *Trends and Issues in Crime and Criminal Justice* (no. 368).

Child Exploitation and On-line Protection Centre (2007). Available: http://www.ceop.gov.uk/ [On-line].

Choo, Kim-Kwang Raymond (2009). *On-line Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences*. Canberra [ACT]: Australian Institute of Criminology Research and Public Policy Series (no. 103).

Clough, J. (2008). Now you see it, now you don't: Digital images and the meaning of 'possession'. *Criminal Law Forum, 19*: 205-239.

Galbreath, N.W., Berlin, F.S., & Sawyer, D. (2002). Paraphilias and the Internet. In A. Cooper (Ed.), *Sex and the Internet: A guidebook for clinicians* (pp.187-205). New York: Brunner-Routledge.

Griffith, G. & Simon, K. (2008). *Child Pornography Law*. NSW Parliamentary Library Research Service Briefing Paper No. 9/08.

i-SAFE Inc (2006). Available: www.isafe.org [On-line].

Kingston, D.A., Fedoroff, P., Firestone, P., Curry, S., & Bradford, J.M. (2008). Pornography use and sexual aggression: the impact of frequency and type of pornography use on recidivism among sexual offenders. *Aggressive Behaviour, 34*(4): 1–11

Marshall, W.L. (2000). Revisiting the use of pornography by sexual offenders: implications for theory and practice. *Journal of Sexual Aggression, 6*: 67-77.

National Center for Missing and Exploited Children, Crimes Against Children Research Center and Office of Juvenile Justice and Delinquency Prevention (2006). *On-Line Victimisation of Youth: Five years later*.

National Society for the Prevention of Cruelty to Children (2003). Available: http://www.safefamilies.org/sfStats.php [On-line].

Protect Your Children On-Line *(*Undated). Available: http://www.privateclienttechnologies.com [On-line].

Seto, M.C., Cantor, J.M., & Blanchard, R. (2006). Child pornography offenses are a valid diagnostic indicator of pedophilia. *Journal of Abnormal Psychology, 115*: 610-615.

Stop It Now! (2000). *Four-year Evaluation: Findings reveal success of Stop It Now! Vermont*. Stop It Now! Report (May 2000, no.5).

Stop It Now, UK & Ireland. (2009). *Stop It Now! News*. (Spring, Issue 11)

Taylor, M. & Quayle, E. (2003). *Child Pornography: An Internet crime*. Brighton [UK]: Routledge.

Wolak, J., Finkelhor, D. & Mitchell, K.J. (2005). *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile On-line Victimization Study.* Washington [DC]: National Center for Missing and Exploited Children.

Ybarra, M., Espelage, D. & Mitchell, K. (2007). The co-occurrence of internet harassment and unwanted sexual solicitation victimisation and perpetration: Associations with psychological indicators. *Journal of Adolescent Health, 41*(6): s31-s41

ATTACHMENT 1
CIRCAMP INFORMATION SHEET

CIRCAMP

Cospol Internet Related Child Abusive Material Project

Policing the Internet

The Internet is a perfect vehicle for child sexual abusive material distribution, with its perceived anonymity, high speed, wide availability and low entry price. Since the introduction of this technology in the mid-1990s, and with the high penetration of digital imaging devices in the population, the amount of child abuse material available on the Internet is growing, and growing fast. The police cannot control the Internet by itself; there is a need for extensive cooperation on the varied arenas that make up the Internet, like the Internet industry.

Law enforcement agencies face significant hurdles when investigating online child exploitation. The production of child exploitation material often takes place in foreign countries with lacking legislation and limited resources for investigation or prosecution of child abuse. Criminals design distribution networks to hinder and delay investigation, for instance by placing servers hosting child abusive material sites in different countries or countries with strident privacy laws.

What is the CIRCAMP network?

In response to the need to facilitate international coordination against cross-border crime, the European Police Chiefs Task Force (EPCTF) established the Comprehensive Operational Strategic Planning for Police (COSPOL) initiative in 2004. Under COSPOL, the EPCTF is able to identify pressing cross-border needs to form international operational cooperative networks amongst law enforcement agencies in Europe. The EPCTF identified online child exploitation as one of the areas that required COSPOL support, and this led to the formation of CIRCAMP.

The overall aim of the CIRCAMP network is to combine the resources of and improve coordination between law enforcement agencies in Europe on the topic of online child exploitation cases. The CIRCAMP network has three primary goals:

- detect, disrupt and dismantle networks, organizations or structures used for the production and/or distribution of child abusive files, and to detect offenders, identify children and stop abuse
- through cooperation create a common understanding towards global policing of the Internet
- reduce harm on society by attacking the distribution of child abuse material on a European level, and disrupt the methods used by organized crime groups responsible for illegal pay-per-view sites

Currently, the National Criminal Investigation Service (Kripos) in Norway serves as the “driver” (i.e. program manager) for CIRCAMP, while the United Kingdom’s Child Exploitation and Online Protection Center (CEOP) serves as a co-driver. The other forerunner member states and organizations in the CIRCAMP network are:

Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Malta, the Netherlands, Poland, Spain and Sweden.

In addition, the project receives operational and analytical support from Interpol and Europol.

CIRCAMP is currently operating under an Action Plan published in 2006. The Action Plan has three main elements:

- block access to child abusive material as a preventive measure and according to national legislation by introducing the Child Sexual Abuse Anti Distribution Filter (CSAADF)
- identify, investigate and close down payment systems used/abused by criminals disseminating child sexual abusive material commercially on the Web
- identify, investigate and arrest those responsible for the commercial distribution of child sexual abuse material on the Web

CIRCAMP will cooperate and share information with any law enforcement agency, anywhere in the world.

By blocking access to domains distributing child sexual abusive material, several effects are achieved:

- prevent the re-victimization of children
- prevent the illegal distribution of files
- prevent the illegal display of abuse material and reduce the harm to the general population while informing the public of the extent of the problem
- prevent access to child abuse material and thus limiting the "market", reducing the need for new production

The Child Abuse Anti Distribution Filter (CSAADF) focuses on blocking on domain level. Currently, six CIRCAMP countries are blocking the distribution of child sexual abuse material in addition to two non-CIRCAMP countries.

International "worst of"-list of domains

The availability of child abuse material is global and needs a global approach. Although CIRCAMP believes that the list of domains that are blocked in any given country should be based on national legislation, CIRCAMP also acknowledges that there are countries that lack the resources and necessary laws to implement it. At the same time, our experience is that the Internet industry in many countries wishes to limit the amount of child sexual abuse material that is available through their networks, based on Terms of Service or policy, but has limited possibilities to find and define such material themselves. As a response to this need, CIRCAMP has agreed to develop a list of domains that contain the most severe child sexual abuse available on the Web, with content that is illegal to distribute and possess in most countries. This list is meant to be a starting point for local police forces willing to actively police the Internet in their country, and access providers that wish to limit child sexual abuse in their systems.

This list should also be made available to IPSs to enable them to block domains on policy basis, even if they are not provided with a national blocking list, as defined by their authorities. A generic "stop page" will also be provided by CIRCAMP and can be used and modified according to the access providers' own discretion. An example of a national "stop page" is shown at the end of this document.

Interpol, as a central and important partner in the CIRCAMP network, will disseminate the list of those domains that publish the most severe child abuse material through the I-24/7 network to all NCBs. The NCBs will be in a position to ensure that the updated lists are continuously distributed within their country, to all parties they see fit. CIRCAMP believes that this will encourage a constructive relationship between law enforcement and the internet industry. The General Secretariat's dedicated unit will assist the NCBs and others in any questions related to this.

The criteria for being added to the list are very strict, and reliability of the list is of paramount importance. The criteria will be further refined, but will include the following considerations:

- The child must be a real child. Computer-generated, morphed, drawn or pseudo images will not be included
- The age of the child must be younger than 13 years of age or perceived to be less than 13
- There must be severe abuse depicted in the files.
- The domain must have been alive within the last three months

The Internet is global in nature, and partnering with a global organization like Interpol is of upmost importance in order for this type of policing to work. Blocking access to child sexual abusive files is a cheap and simple preventive method for both the Internet industry and the police, and will be a powerful tool in our efforts to avoid that children end up as commercial goods on the Internet for the rest of their lives.

Example CSAADF "stop page"