Submission to the
Cyber Safety Policy and Programs
Department of Communities

Enhancing Online Safety for Children

Bravehearts inc.
Educate. Empower. Protect.

March 2014

About the Authors

Carol Ronken is Bravehearts' Research and Policy Development Manager. After seven years at Griffith University as a casual researcher and Associate Lecturer in the School of Criminology and Criminal Justice, Carol joined Bravehearts in early 2003. Carol has a Bachelor of Arts (psychology) and Masters in Applied Sociology (social research). In 2011 she received an award from the Queensland Police Service Child Protection and Investigation Unit for her contribution to child protection. Carol has also co-authored *The Bravehearts Toolbox for Practitioners: working with Child Sexual Assault* (Australian Academic Press, 2011). A member of the Australian and New Zealand Society of Criminology and the International Society for the Prevention of Child Abuse and Neglect, she is currently studying for her doctorate through the Faculty of Law at Queensland University of Technology.

Hetty Johnston is the Founder and Executive Director of Bravehearts Inc. Hetty is the author of the national awareness campaign, 'White Balloon Day', 'Sexual Assault Disclosure Scheme', 'Ditto's Keep Safe Adventure' child protection CD-Rom and her autobiography, 'In the Best Interests of the Child' (2004). Hetty has been a contributing author to various books including, 'Crime on my Mind', and 'Women on Top'.

In 2005, Hetty was announced as a finalist for the 2006 Australian of the Year Awards – she is the recipient of two Australian Lawyers Alliance Civil Justice Awards (2003, 2004) and was named a finalist in the 2008 Suncorp Queenslander of the Year Awards. She was awarded a Paul Harris Fellowship in 2010 and is a Fellow of the Australian Institute of Community Practice and Governance (March 2010). In early 2009, Hetty was recognised as one of approximately 70 outstanding leaders throughout the world, receiving the prestigious annual Toastmasters International Communication and Leadership award. In 2013 Hetty was awarded Northern Australia's Ernst & Young Social Entrepreneur of the year. Hetty is a member of the International Society for the Prevention of Child Abuse and Neglect and sits on the Federal Government's Cybersafety Working Party.

This submission has been prepared by:
Bravehearts Inc
PO Box 575
Arundel BC, Qld 4214
Phone: 07 5552 3000
E-mail: research@bravehearts.org.au
Web: www.bravehearts.org.au

Table of Contents

About Bravehearts Inc.

Our **Mission** is to stop child sexual assault in our society.

Our **Vision** is to make Australia the safest place in the world to raise a child.

Our **Guiding Principles** are to at all times, do all things to serve our Mission without fear or favour and without compromise and to continually ensure that the best interests and protection of the child are placed before all other considerations.

Bravehearts has been actively contributing to the provision of child sexual assault services throughout the nation since 1997. As the first and largest registered charity specifically and holistically dedicated to addressing this issue in Australia, Bravehearts exists to protect Australian children against sexual harm. All activities fall under 'The 3 Piers' to Prevention; Educate, Empower, Protect – Solid Foundations to Make Australia the safest place in the world to raise a child. Our activities include but are not limited to:

EDUCATE

- Early childhood (aged 3-8) 'Ditto's Keep Safe Adventure' primary and pre-school based personal safety programs including cyber-safety.
- Personal Safety Programs for older children & young people and specific programs aimed at Indigenous children.

EMPOWER

- Community awareness raising campaigns (Online and Offline) including general media comment and specific campaigns such as our annual national White Balloon Day.
- Tiered Child sexual assault awareness, support and response training and risk management policy and procedure training and services for all sectors in the community.

PROTECT

- Specialist advocacy support services for survivors and victims of child sexual assault and their families including a specialist supported child sexual assault 1800 crisis line.
- Specialist child sexual assault counseling is available to all children, adults and their non-offending family support.
- Policy and Legislative Reform (Online and Offline) - collaboration with State Government departments and agencies.

Bravehearts Inc. is a National organisation, it is a registered Public Benevolent Institution, registered as a Deductible Gift Recipient, operates under a Board of Management and is assisted by State based Community Regional Committees, Executive Advisory Committees and a Professional Finance Committee.

Introduction

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 continued to grow, 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.

We note that the current discussion paper, *Enhancing Online Safety for Children*, focussed heavily on the issue of cyber-bullying.

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.

Additionally we note that 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.

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.

1. **What existing programmes and powers should the Commissioner take responsibility for?**

Bravehearts thoroughly supports the establishment of a single body to take the responsibility in relation to online safety of children. The Commission should be focussed on:

- Improving the safety and protection of children and young people in the online environment;
- Oversight and coordination of online safety programs;
- Ensuring that complaints are dealt with in a timely and appropriate manner;
- Reviewing legislation, policy and practices relating to the online safety and protection of children and young people;
- Conducting and coordinating research;
- Initiating reviews and inquiries;
- Fostering effective relationships with, industry, sector organisation and program providers;
- Establishing and coordinating a think tank on online safety; and
- Providing opportunities through which children and young people are engaged in issues and matters that affect them and provide an avenue through which their voices and views are heard and considered.

Bravehearts recognises that current responses to online safety are uncoordinated and spread across government and non-government agencies. We would advocate that as a first role the Commission would conduct an audit of which agencies are currently providing online programs and work to minimise duplication and ensure consistency in messaging to children, young people and the community in relation to online safety.

2. **Considering the intended leadership role and functions of the Commissioner, which option would best serve to establish the Commissioner?**

Bravehearts supports Option 2, whereby the Commissioner would be set up as an independent office within an existing government agency. It is our position that the Commissioner should fit within the office of the National Children's Commission.

3. **Are these definitions of 'social networking sites' suitable for defining 'social media sites' for the purposes of this scheme?**

Bravehearts supports the definition of social networking sites as provided by the Office of the Australian Information Commissioner. However we would recommend the addition of two additional components:

- That social media sites can be constructed as public or semi-public
- That social media sites can include the activity of online gaming.

4. **Should the proposed scheme apply to online games with chat functions?**

Bravehearts believes the inclusion of online games in the proposed scheme, along with the definition of social networking, is vital. Online gaming provides opportunities for potentially harmful interactions between users, including, but not limited to, grooming of children and young people and exposure to inappropriate material.

5. **What is the best criterion for defining a 'large social media site', and what available sources of data or information might be readily available to make this assessment?**

We would support the defining criterion for assessing a 'large social media site' as the level of usage, specifically the number of active Australian users.

6. **Is the coverage of social media sites proposed by the Government appropriate and workable?**

Bravehearts believes that the coverage of social media sites proposed by the Government, as outlined in the Discussion Paper, is appropriate and workable for this scheme.

7. **Should the scheme allow children who are unsupported by adults to be active participants (either as complainants or notice recipients)? Having regard to the vulnerability of children, what procedural safeguards should be in place?**

Bravehearts believes that it is important that children and young be allowed to be active participants, particularly as complainants. We know that, just as in offline sexual exploitation of children, there are a raft of barriers to children and young people disclosing to an adult. The level of shame, silence and secrecy (and in relation to online risks, fear of losing access) surround sexual exploitation of children, either online or offline, means that we need to ensure that children's participation in notifying of harms and concerns is sensitively handled.

Bravehearts supported the promotion of the current Help Button, and additionally that children and young people be provided with information on accessing support, including anonymously, to ensure their safety and wellbeing (for example through organisations like Bravehearts and KidsHelpLine).

8. **What type of information would it be necessary to collect from complainants in order to assess their eligibility under the proposed scheme (including age verification) and also to adequately process complaints with minimal investigation required?**

As outlined in the Discussion Paper, Bravehearts believes that basic information including:

- Clear identification of material, for example web address or screen shots
- Identification of relevant social media site or platform
- Any relevant usernames or contact details (e-mail address, social media profile) of 'offending' individual
- Copy of any reports to the social media site, for example screen shot or copy of receipt of notification

It is our position that if we wish to encourage children and young people to notify and overcome the known barrier to disclosure, there must be the option to report anonymously.

9. **How would an eligible complainant demonstrate that the complainant has reported the content to the participating social media site?**

Reporters can demonstrate that a complaint has been forwarded to the participating social media site through the provision of a copy of any reports to the social media site, for example screen shot or copy of receipt of notification

10. **What should the timeframe be for social media sites to respond to reports from complainants? Is 48 hours a reasonable timeframe, or is it too short or too long?**

Bravehearts supports a 48 hour timeframe for social media sites to respond to complainants' reports.

11. **What level of discretion should the Children's e-Safety Commissioner have in how he/she deals with complaints?**

While there should be a level of discretion in how the e-Safety Commissioner responds to complaints, it is our position that there must be clear policy around decision and a process be in place to ensure consistency and transparency of decisions. If a decision is made that complaint is frivolous, vexatious or not made in good faith, this should be reviewed internally to ensure that there is consensus that the complaint does not warrant investigation.

12. **What is an appropriate timeframe for a response from the social media site to the initial referral of the complaint?**

Bravehearts supports a 48 hour timeframe for social media sites to respond to an initial complaint referral.

13. **Are the nominated factors, the appropriate factors to be taken into account when determining whether the statutory test has been met? Should other factors be considered in this test?**

We note that factors outlined in the Discussion Paper include:

- That the material which is the subject of the complaint would have to relate directly to the child in question;
- A reasonable person would consider that the material would be likely to cause harm or distress to the child. In making this assessment, the Commissioner would be able to take a range of factors into account, such as:
    - the occasion, context and content of the material;
    - the circumstances under which the material was placed on the social media site;
    - the risk of triggering suicide or life-threatening mental health issues for the child;
    - the age and characteristics of the child; and
    - any other matter which the Commissioner may consider relevant;
- The material would have to be on a participating social media site; and

- The material would have to have been placed on the participating social media site by a third party.

In relation to the nominated factors, Bravehearts supports these in principal, however we would suggest that in relation to the first dot point clarification is needed in terms of 'how' the material subject to complaint would have to "relate directly to the child in question". In the case of cyber-bullying this may be easily understood, however if a child is exposed to inappropriate material or grooming behaviours it is less clear.

Additionally, the second dot point states that consideration would include whether the "material would be likely to cause harm or distress to the child", Bravehearts would advocate that this should be broadened to "likely to cause harm or distress to the child or children generally".

14. Is the test of 'material targeted at and likely to cause harm to an Australian child' appropriate?

Bravehearts supports the test of appropriateness, however, as noted above we would advocate that this should be broadened to "likely to cause harm or distress to the child or children generally".

15. What is an appropriate timeframe for material to be removed?

Bravehearts would suggest that once a notice to remove material has been issues, social media sites should be provided with a maximum timeframe of 24 hours.

16. What would be the best way of encouraging regulatory compliance by participating social media sites that lack an Australian presence?

Bravehearts supports an incentive scheme similar to the 'safe harbour' provision in New Zealand, providing security to social media sites that comply with their responsibilities.

We would also suggest that social media sites that comply receive a 'safe site' compliance logo.

17. Should the proposed scheme offer safe harbour provisions to social media sites which have a complying scheme, and if so, what should they be?

We support a legislative protection for complying social media sites in line with the New Zealand scheme.

18. Is merits review by the Administrative Appeals Tribunal the most appropriate review mechanism and if so, which parties and in relation to which types of decision is it appropriate? What are the alternatives?

In relation to this question, Bravehearts would like to emphasise that at all times, in all decisions the best interests of the child must be paramount.

19. What do industry representatives consider are the estimated financial and administrative impacts of compliance with the proposed scheme? How are these estimated impacts derived?

As a non-industry representative Bravehearts is unable to comment.

20. In light of the Government's proposed initiatives targeting cyber-bullying set out in Chapters 1 and 2; do the current criminal laws relating to cyber-bullying require amendments?

As identified in the paper, current criminal laws relating to cyber-bullying provide adequate coverage of serious cyber-bullying instances.

At this point we would like to introduce issues around legislative responses to the issue of sexting, which can often be a component of cyber-bullying.

Much of the concerns around sexting and the law is focused on child pornography offences under criminal laws. However, sexting also may have repercussions under civil law such as defamation law, privacy law etc. It is suggested that, to understand how the law regulates *sexting*, it is necessary to effectively address sexting under our laws we need to take into consideration a range of factors such as (a) the intent of the person who sent the original image, (b) how those images came into the possession of the person who has them and (c) how those images or videos are subsequently used and/or redistributed.

Legislation responses need to be carefully constructed to ensure the protection of young people. It may be argued that an appropriate approach may be to ensure the inclusion of sexted images under child pornography legislation, with an available defence for young people who voluntarily self-produce and distribute such images to other minors. The availability of such a defence could protect young people who self-produce images and some minors who receive them, for example if they can show that they did not exert pressure on the producer and did not further distribute the images.

This approach would facilitate effective prosecution of adult offenders while protecting the interests of the minors who are depicted in the images.

Additionally, and particularly in relation to first and objectively less serious (ie. low-mid range) 'offences', a more effective consequence for young people involved in sexting would be a diversionary program focussed on awareness and education. It would be preferable that young people realise the severe moral, personal and social costs of their actions before they commit an act that may have serious legal consequences.

21. Is the penalty set out in section 474.17 of the Criminal Code appropriate for addressing cyber-bullying offences?

See response above (Question 20). Particularly in relation to first and objectively less serious (ie. low-mid range) 'offences' Bravehearts would support a diversionary program, such as youth justice conferencing to assist young people understand the moral, personal and social costs of cyber-bullying.

22. Is there merit in establishing a new mid-range cyber-bullying offence applying to minors?

See response above (Question 20 and 21)

23. Is there merit in establishing a civil enforcement regime (including an infringement notice scheme) to deal with cyber-bullying?

See response above (Question 20 and 21)

24. What penalties or remedies would be most appropriate for Options 2 and 3?

See response above (Question 20 and 21)

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 A: Further Recommendations

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.

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.

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.

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.

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.

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.

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

Education and Awareness

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.

A more appropriate preventative approach would include a school-based 'Social Studies' education approach that would teach young people about the dangers – legal and personal – associated with safe mobile phone and internet usage.

Bravehearts recommends a curriculum-based approach to educating children and young people about the legal and personal risks aligned with unsafe online practices. Additionally, we support greater general awareness and education programs targeted to the community.