ninemsn Submission to the Joint Select Committee on Cyber Safety

Thank you for inviting ninemsn to prepare a submission on the important issue of cyber safety.

The internet has become an integral part of Australian society and the economy. It offers unparalleled opportunities and benefits to the Australian community including tools for learning via the use search engines, new channels for entertainment such as catch up television and video on demand as well as a new means of social interaction via social networking sites, email and messaging products. Our current generation of young Australians will be the first raised in the internet era and their lives will continue to become increasingly "Web-based".

Advances in internet technology have undoubtedly been accompanied by new and challenging risks to the safety of online users increasingly of concern to governments, law enforcement agencies and industry participants globally. Importantly, these include risks to which children are particularly vulnerable such as exploitation by online predators, exposure to age-inappropriate material, cyber bullying and misuse of private information.

This submission will provide an overview of the ninemsn business and technologies. We will then provide our thoughts on the appropriate approaches to protecting children from the critical risks posed by internet and mobile technologies, with particular emphasis on improving education and public awareness, consumer initiated technology measures and cooperation with law enforcement agencies.

1. About ninemsn

ninemsn was incorporated in 1995, and is a 50:50 joint venture between Microsoft Corporation (Microsoft) and PBL Media Holdings Pty Ltd (PBLM). The joint venture combines the content and expertise of PBLM in the broadcasting and publishing areas and the expertise of Microsoft in the technology, software and interactive areas.

The ninemsn business employs over 350 staff and operates over 80 websites targeted at Australian and New Zealand markets. The business includes the following components:

(a) Websites devoted to news, entertainment, finance, fashion, travel, leisure, shopping and sports. These sites are rated PG or G save for http://www.zooweekly.ninemsn.com.au/ which is rated M. Entry to M-rated content on this site is only granted to registered members who have verified that they are 18 years of age or above;

(b) Streaming of video and 'catch-up' TV content on ninemsn's FixPlay website, the majority of which are rated G or PG.

(c) ninemsn's mobile site http://m.ninemsn.com.au which provides a limited version of the content on the network, adapted for viewing via mobile devices.

(d) Windows Live, ninemsn's social networking product featuring Windows Live Messenger and Windows Live Hotmail

(e) Bing, the search engine.

2. Key Cyber Safety Issues

(a) Education and Public Awareness

ninemsn believes that the internet industry should play a pivotal role in enabling safe and responsible use of internet technologies, particularly by children. We believe education and public awareness programs are one of the best methods for increasing cyber safety and should be the foundation of the Government's approach on the issue. While it is important that parents and their children have access to technological control tools that can help minimise exposure to cyber safety risks, technology will not provide a complete or even nearly complete means for making the internet safe, particularly given the rapid pace with which the internet is growing and changing. This is why ninemsn is committed to providing education to parents, educators and children to increase current levels of knowledge and control over children's online environment.

To be effective, educational programs and public awareness campaigns should be responsive to developing social and technological tends in internet usage. Some of the most serious online dangers faced by children include:

1. Cyber stalking and 'grooming' via social networking platforms and services;
2. Cyber bullying (peer to peer harassment is the most frequently reported incident);
3. Exposure to inappropriate and harmful material including pornographic, violent and hateful content;
4. Misuse of personal information including information posted on social networking sites which are accessed and abused by strangers.

Although more research about these risks is required, what is clear is that current programs should give priority to children's home online usage and mobile usage. The available research indicates that much of Australian children's internet usage is at home. There are an estimated 91400 Australian children aged 6 to 11 using the internet from home, approximately 12 times per month.[1] 96% of 14 to 15 year olds online primarily access the internet from home. 27% of children have a computer in their own bedroom and 24% of teens claim that their parents are never around when they are online (yet only 6% of parents claimed that they were never around when their children were online).[2] Consequently children are most likely to be exposed to inappropriate material in their home environment. The available research also shows that 42% of internet users aged 10 to 14 have viewed pornographic images online, with 79% of this exposure occurring in the family home.[3] There is also an increasing tendency for teens to access the internet by mobile devices, with 21% of all 14 to 15 year olds having accessed the internet via a mobile phone in the surveyed four week period (higher than the general population at 13%).[4]

[1] Nielsen NetView home/work panel May 2010
[2] Girls beat boys at Internet safety - Media Release by NetAlert 29 March 2007
[3] Online Victimization of Youth: Five Years Later, 2006
[4] *Source; Roy Morgan Single Source Apr 09 – Mar 10*

While parents are aware that online dangers exist, it seems many remain unsure how best to address those concerns.[5] We would agree with the views of the United States StaySafeOnline Campaign that, "just as we don't teach children to drive by giving them the keys to the car and expecting them to be "self-taught," similarly, we shouldn't let children sit down at the computer without training and supervision."[6] The difficulty with internet use, however, is that there appears to be a generational gap between parents and children, which results in a significant disconnect between what parents think children are doing or exposed to online and the reality of the situation. For instance, two independent surveys conducted by ninemsn and NetAlert (undertaken by parents and children separately), confirmed that parents believe they know what their children are up to when online; yet children are telling a different story. 71% of the parents surveyed believed their children use the internet for research, while only 23% of teens said that was the case. Further, 50% of parents said they always know what sites their children visit, yet only 46% of the children surveyed believed their parents set rules when it came to internet usage[7] and 43% of teenage boys have downloaded files that they didn't want their parents to know about.[8]

In Australia, ninemsn has partnered with the Australian Federal police and Microsoft to address cyber safety through its promotion of the ThinkUKnow[9] nationwide initiative on the ninemsn network. ThinkUKnow is aimed at educating parents, teachers and carers by hosting school-based seminars and by developing a user-friendly website. The ThinkUKnow website has a host of user-friendly resources, such as video resources (see http://www.youtube.com/watch?v=FGF146WJ22M) aimed at educating parents and children on how to avoid these risks and report incidents when they occur.

There are many simple steps that parents can take to protect their children's exposure to these risks. For example, ThinkUKnow recommends to parents that they:

- Encourage children to only upload pictures that you as their parents / carer would be happy to see – anything which is not acceptable to be passed around the dinner table should NOT make it on to the internet. It's also not a good idea to post pictures which can identify the school which your child attends since this could help someone locate them.
- Tell your children not to post their phone number or email address on their homepage.
- Help your child to adjust their account settings so that only approved friends can instant message them.
- Check if your child has ticked the "no picture forwarding" option on their social networking site settings page – this will stop people sending pictures from their page around the world without their consent
- Encourage them not to disclose too much information in a blog. Friends can call them for the address of the latest party rather than read about it on their site.
- Ask them to show you how to use a social networking site - getting involved will encourage them to share the experience with you.

In relation to information searching, parents have the option of applying a 'safe search' filter on the Bing search engine which is specifically designed to prevent inadvertent exposure to sexually explicit images. In addition, the ninemsn

[5] Recent research commissioned by Microsoft
[6] http://www.staysafeonline.org/content/protect-your-children
[7] Girls beat boys at Internet safety - Media Release by NetAlert 29 March 2007

[8] 'Online Safety for Teens' survey conducted by NetAlert and Ninemsn
[9] http://www.thinkuknow.org.au/site/index.asp

homepage houses links to ninemsn's Online Safety Hub[10] which provides information on cyber bulling, cyber crime, protecting email privacy, user-friendly tips for children and parents as well as links to various government and community safety and filtering sites.

Finally, ninemsn believes that cyber safety needs to become an integral part of every school curriculum. This is important given the close relationship between online harassment and offline bullying in the schoolyard, with a large proportion of those who engage in cyber bullying also engaging in face-to-face bullying behaviors.[11] Ideally, cyber safety lessons would begin with primary age students and would continue throughout schooling, adapting appropriately as students mature and online behaviors change. Further, the curriculum should maintain pace with technical and social change in this area, such as encouraging responsible use of mobile phone applications. Again there is an opportunity for the Australian internet industry to play a supporting role. Many best practice educational and awareness campaigns around the world have involved public-industry partnerships. We note, for example, that of the 80 European countries which have provide cyber safety lessons in their schools, in the majority of cases, the curriculum was developed by some form of collaborative public-private partnership between schools, the private sector and Government.[12]

(b) Consumer-initiated Technology Controls

The Australian Government has positioned Mandatory ISP Level Filtering as a key component of its approach to addressing the issues posed by the accessibility of RC classified content on the internet. ninemsn acknowledges that RC content should not be published to Australian audiences in any online media. We would support a voluntary ISP filtering, system rather than a mandatory approach. ninemsn is concerned that the proposed mandatory filtering system:

- may result in the over blocking of lawful and valuable educatory information surrounding topics of legitimate political and ethical concern ;
- is inconsistent with approaches in other jurisdictions, where limited levels of ISP filtering have remained *voluntary* and only applied to a highly restricted range of content. For example, Britain, Canada and several Scandinavian countries have implemented *v*oluntary filtering schemes but prohibited content has been specifically limited to child pornographic material;
- has the potential to result in over-reliance by parents on mandatory filtering as a means of safeguarding children, shifting responsibility out of the home; and
- is not supported by any data concerning the cost or effectiveness of a mandatory program over a voluntary program or other technological control methods.

Further, a mandatory filter will not capture unwanted material disseminated via peer-to-peer networking, instant messaging, direct emails and chat rooms. This is concerning as most child pornography is not openly displayed on websites but is covertly exchanged via such peer file sharing networks. It also exemplifies why it is important to encourage a sense of individual responsibility for cyber safety through education and public awareness campaigns.

[10] http://www.windowslive.ninemsn.com.au/onlinesafety.aspx
[11] Review of Existing Australian and International Cyber-Safety Research, Child Health Promotion Research Centre, Edith Cowan University May 2009.
[12] Education on Online Safety in Schools in Europe: Summary Report, Eurydice, December 2009.

ninemsn notes that while the Government has focused on ISP filtering there are array of consumer initiated technology protection controls which are freely available for many internet based services. ninemsn believes that these user-initiated, customised controls have many advantages because they are user-controlled, cost effective, specifically targeted to each user's particular needs and are able to be readily adapted and upgraded to changing technologies and user-behaviors.

Consumer initiated controls can assist parents provide their children with a safer user experience, for example by allowing them to block access to material which they believe is inappropriate or to monitor their child's usage. On Windows Live Messenger, parents are able to restrict/monitor contact lists, block messages from people not on that list and receive alerts when incoming messages are potentially fraudulent or malicious. There are also options which enable the contents of conversations in Windows Live Messenger to be retained, as well as a suite of user-privacy controls on Hotmail[13] and Messenger.

Again, we believe that education and awareness about the availability of these controls is critical. Parents need to be adequately informed as to what products are available and how best to configure and use them in a way most appropriate for their family. ninemsn believes this presents a valuable opportunity for industry and government to work collaboratively on promoting the availability of these tools. There are some helpful examples of best practice of this cooperative approach emerging from the US[14] and UK.[15]

(c) Law Enforcement

Ultimately, no single measure can fully protect children from all online predators who choose to willfully and covertly disseminate, trade in and access offensive material or engage in inappropriate online behaviors. Therefore, it is vital that industry members engage with and support law enforcement agencies to prosecute those responsible.

ninemsn continues to cooperate with its shareholder, Microsoft, to investigate user complaints and supports Microsoft's collaboration with the Australian Federal Police and international law enforcement agencies (such as Interpol) regarding the development of the Child Exploitation Tracking System (CETS) software and other technological tools such as PhotoDNA to help identify victims and online paedophiles. Further, ninemsn promotes the work of the Virtual Global Taskforce, which is a network of police forces from around the world working together to combat online child abuse.

(d) The Need for More Research

As noted in the most comprehensive review in Australia of the research to date, there are significant gaps in cyber safety research in Australia, where research is notably less extensive than in other countries.[16] For example we do not have any data regarding the level of cyber-grooming in Australia. ninemsn believes more Australian-based research into cyber safety risks is needed so that we are better informed about the prevalence of particular risks and the

[13] http://www.windowslive.ninemsn.com.au/hotmail/article/1068021/spamandhotmail
[14] StaySafeOnline.org http://www.staysafeonline.org/content/cyber-safety-materials
[15] UK Council for Child Internet Safety http://www.dcsf.gov.uk/ukccis/

[16] Review of Existing Australian and International Cyber-Safety Research, Child Health Promotion Research Centre, Edith Cowan University May 2009.

specific contexts in which they arise. Further studies are also needed to evaluate various educational and public awareness programs, filtering and other technologies to minimise and control such risks. This will help to make better informed choices as to what risks should be prioritised, what programs and methods will be most effective in combating those risks and how we can cost effectively target our resources.

(e) Proposed Ombudsman

ninemsn would need to be supplied with more information on the operation of the proposed online ombudsman to offer a complete opinion on the relative merits of establishing one. Our preliminary view is that an ombudsman would duplicate the reporting mechanism already in place by ACMA in relation to inappropriate content. In terms of the more pernicious online offences, ninemsn believes that the Australian Federal Police remains the most appropriate forum for investigation and prosecution.

In conclusion, ninemsn believes the Government's primary cyber safety focus should be on educational and public awareness campaigns including promoting the use of consumer-initiated technology controls, on law enforcement and generating more Australian based research of cyber safety issues and methods for combating cyber safety risks. In order to maximise the potential benefits of the internet, the industry, government, law enforcement agencies need to be well informed as to the extent of these risks and work collaboratively to develop best practice cyber safety strategies.

Contact
Please direct any queries regarding this submission to:

Jennifer Duxbury
Compliance, Regulatory and Corporate Affairs Director
ninemsn Pty Ltd
Level 7, 264 George St
Sydney NSW 2000