
A submission in response to

**Joint Select Committee on cyber-safety**

July 2010

## OVERVIEW

Microsoft Australia welcomes the opportunity to provide this submission to the Joint Select Committee on cyber safety.

Although the Internet opens a new world of information, socialising and entertainment for children and young people it also presents new risks. These include online predators, personal information disclosure, exposure to inappropriate content and emotional and psychological attack by others connected to the internet.

Consumer security and safety are a top priority for Microsoft. Eight years ago, the company launched its Trustworthy Computing Initiative, a companywide top-to-bottom commitment to delivering secure, private and reliable computing experiences for everyone. In addition to improved software development practices, Trustworthy Computing includes support for strong laws addressing criminal online conduct; support for law enforcement training, investigations, coordination and prosecutions; and guidance for customers on adopting security and privacy best practices.

More recently, Microsoft has established the Digital Crimes Unit. A worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer through strong enforcement, global partnerships, public policy and technology solutions.

Our corporate privacy policies—including a set of privacy principles released in 2007 related to search and online advertising—reflect our long-held commitment that consumers should have the ability to control the collection, use and disclosure of their personal information. This is nowhere more crucial than in the area of young people's Internet use. From social networking sites to e-mail to online gaming, responsible user practices and technology safeguards should be applied to help keep young Internet users—and their personal information—safe.

Microsoft Australia focuses its submission in the following areas:

- Cyber bullying;
- Breaches of privacy;
- Opportunities for cooperation;
- Ways to support schools; and
- The role of parents, families and carers.

## CYBER BULLYING

Australian parents are challenged in how to deal with cyber bullying incidents involving their children.

Research commissioned by Microsoft Australia in 2008 found that 83 percent of parents did not know what to do if their child was being cyber bullied and two out of three parents said that they were unsure about the best alternative to help their children. While almost all surveyed parents said they were aware of the issue, three quarters said they are more concerned about cyber bullying than they were a year ago.

Changing patterns in computer use, an increase in SMS texting as well as classic signs like a child becoming withdrawn or becoming anti-social are all possible indicators of cyber bullying.

Microsoft provides the following recommendations to parents and carers to identify and respond to cyber bullying:

- Communicate: Discuss cyber bullying with children and encourage them to report bullying to a trusted adult.
- Block: Block communications with cyber bullies through filtering technologies and encourage children not to respond to bullies. Children should be educated as to the importance of refusing to pass along bullying messages and they should be encouraged to tell friends to do the same.
- Investigate: Know what children are talking about. Investigate what they do online.
- Use Family Safety Software. This can supply parents with an activity report on their child's computer usage, which in turn provides a starting point for parents to discuss online activities with their children.
- Report: Know who to contact if a child is being cyber bullied, e.g.:the child's school, the site service provider where the bullying material is located, and the local police.

In our submission to the House of Representatives Standing Committee on Communications during its inquiry into cybercrime we called on the Australian Government to consider a more expansive strategy and create a "Cyber Tzar," located in Prime Minister and Cabinet and a strategy that engages all elements of national power. We continue to commend this proposition as in our view there is a need to have an officer at the Federal level who can look across the nation into activities that assist children and young people in the online environment.

**BREACHES OF PRIVACY**

Research commissioned by Microsoft in December 2009 found that 79 percent of hiring managers and job recruiters surveyed reviewed online information about job applicants. Most of those surveyed considered what they found online would impact their selection criteria. In fact, 70 percent of hiring managers in the study said that they have rejected candidates based on what they found.

It is important for young people in particular to recognise that their personal profiles online may be available to persons who will have an impact on their future.Online content can surface years after it has been posted. Microsoft provides the following recommendations to young people to be proactive in protecting their privacy and online reputation:

- Safeguard personal information. A basic strategy to avoid identity theft and online fraud is to keep personal information private online. Just as individuals need to be careful about sharing information offline they should not provide information to an organisation unless they know how that organisation will use that information. Before giving information to an organisation online, individuals should ask why the organisation would need that personal information. Where the information is not needed for the transaction being undertaken online, individuals should think twice before making it available.
- Use privacy settings. Most social networking and photo-sharing sites allow users to determine who can access and respond to their content. If a site doesn't offer privacy settings, we recommend users find another site.
- Don't mix public and private lives online. Use different e-mail addresses for different online activities to help keep public and private lives separate.
- Choose photos thoughtfully.  A photo, like a picture, says a thousand words. Photos uploaded by friends can be damaging to a reputation – vigilance is needed.
- Language and content. It is best to assume that anyone can read anything that is written online.
- Take action. If you find information that is unflattering, embarrassing, or untrue, contact the Web site owner or administrator and ask them to remove it. Most sites have policies to deal with such requests.

Young people have a complex understanding of online privacy and the consequences of shared information. This understanding is related to their developing concepts of trust. It is not possible to 'protect' young people from the consequences of every action they take. It is possible however for parents to discuss these issues with their children on a regular basis and to encourage their children to consider the consequences of their online actions – just as they do their actions in the physical world.

**OPPORTUNITIES FOR COOPERATION**

Microsoft Australia is of the view that there are many opportunities for industry and Government to work collaboratively to manage cyber safety issues.

**Child Exploitation Tracking System**

Microsoft Australia has been working with the Australian Federal Police (AFP) to roll out the Child Exploitation Tracking System (CETS) and other technological tools to help more effectively identify victims of sexual exploitation and abuse and track down online pedophiles.

CETS is a unique software tool that enables the AFP to work with law enforcement agencies throughout Australia and around the world, to share and track information relating to online child exploitation and abuse. According to the AFP, CETS increases the effectiveness of AFP investigations by enabling officers to store, search, analyse and link large quantities of evidence and match cases under investigation by Australian and international law enforcement agencies.

**ThinkUKnow**

Microsoft is also involved in a range of partnerships including *ThinkUKnow* (with the Australian Federal Police and Ninemsn). ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers in primary and secondary schools across Australia using a network of accredited trainers.

The credentials of ThinkUKnow have been supported by a 2009 evaluation of the pilot, which identified strong support for the program and the empowering knowledge it provides. This included how to report online sexual exploitation, inappropriate content, cyber bullying, spam, scams and provided advice on other safety and security issues.

Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia.

The program is already operating in New South Wales, Victoria and the ACT and will roll out in Queensland, Western Australia, South Australia, Tasmania and the Northern Territory throughout 2010.

**PhotoDNA**

Globally, Microsoft has been working with law enforcement agencies, child protection groups and ISPs to look at what can be done via technology to help reduce the spread of child pornography, help track and trace on-line predators and educate the community about what can be done to protect children online.

The technology, called PhotoDNA, was initially created by Microsoft Research, to help the US based National Center for Missing & Exploited Children (NCMEC) in its efforts to find hidden copies of the worst images of child sexual exploitation. Once NCMEC assigns PhotoDNA signatures to known images of abuse, those signatures can be shared with online service providers, who can match them against the hashes of photos on their own services, find copies of the same photos and remove them. Also, by identifying previously "invisible" copies of identified photos, law enforcement may get new leads to help track down the perpetrators.

Microsoft Australia is examining opportunities to work with Australian law enforcement agencies in using this technology in Australia.

**Age verification technology**

Microsoft has also outlined a proposal to the Consultative Working Group on Cyber Safety for an Australian pilot of its digital age verification technology.

The Group's digital age verification sub-committee was established to consider the proposal for such a pilot, using schools to verify the ages of the children that would be involved. The sub-committee intends to develop the proposal for the Group's consideration, in the first instance, with Microsoft and other industry members of the Group providing a lead in the sub-committee.

**Other partnerships**

Other partnerships that Microsoft Australia is involved in include the *Smart Online Safe Offline* initiative (with the National Association for the Prevention of Child Abuse and Neglect—NAPCAN) and the Cybersafety and Wellbeing Initiative (with the Alannah and Madeline Foundation).

Microsoft has also worked with Interpol and the International Centre for Missing & Exploited Children (ICMEC) to sponsor worldwide training sessions for law enforcement personnel on computer-facilitated crimes against children. As of February 2008, more than 2,600 law enforcement officers from more than 100 countries have been trained in methods of identifying suspects, investigating offences and dealing with victims of online child predators.

**ROLE OF PARENTS, FAMILIES, CARERS**

Earlier this year, Microsoft commissioned “For Safety’s Sake” research. The survey found that two thirds of Australian parents were concerned about the safety of their kids online, and more than 60 percent of parents allowed their children to surf the net unsupervised and unrestricted at home.

Alarmingly, one fifth of all Australian parents surveyed had caught their children looking at inappropriate material online, almost one third had found their children chatting to strangers, 36 percent had caught their kids downloading software without permission and another 12 percent had found their children handing over personal details.

Despite two thirds of parents surveyed allowing their children free reign to the web at home, most believed that online danger was more likely to occur at a friend’s house (52 percent).

The survey revealed that in spite of concerns for online safety not enough was being doneto educate and help protect children.

- More than two thirds of Australian parents admited they knew only a few of their children’s online friends;
- Another 11 percent admited they were totally in the dark, knowing none of their children’s online friends;
- Only half of all parents (58 percent) housed the computer in a public area of the home;
- 20 percent of parents had not discussed online safety with their children;
- More than 60 percent of parents were aware their computer had parental control software available – yet less than a third of all parents monitored their children’s activity online.

The Internet opens a new world of information, socialising and entertainment for children - it also presents new risks. Protecting children while they are using computers can be quite challenging.

Microsoft recommends numerous steps that can be taken by parents to foster a safe online experience for children including using a form of parental control software.

Microsoft has built such controls into its computer operating systems. For example, Windows 7 Parental Controls are designed to put parents' minds at ease and give them confidence in their ability to manage what their children can do on the computer. Parental Controls in Windows 7 help parents determine which games their children can play, which programs they can use, and which websites they can visit—and when. Parents can restrict computer use to specific times and trust that Windows 7 will enforce those restrictions, even when they're away from home. Other features include::

- Web Restrictions – Using an online service, a parent can restrict what types of web sites their child can visit, either by category or specific URL to determine what sites are allowed and which are not. These restrictions will work automatically with any web browser.
- Game Restrictions – Partnering with Computer Game rating systems from around the world, Windows 7 allows a parent to restrict the types of computer games their child can play.
- Application Restrictions – If a parent chooses, they can apply limits so their child can only run the applications that the parent has approved.
- Time Limits - Parents can decide when children are allowed, or not allowed, to use the computer by choosing the specific times and days to block. The child then receives a 15-minute and a 1-minute notification that their time is about to expire, and if their time ends before they log off the computer, Windows 7 suspends their session and displays the logon screen so another user can use the computer. The child's session stays active in the background, however, so the next time they log on, they can pick up where they left off without losing any of their work.

Microsoft recognises that parental controls are only useful when a parent can understand how to deploy the controls. Microsoft has as a consequence sought to make the deployment of parental controls as easy as possible for parents with every level of computer appreciation.

**CONCLUSION**

Microsoft Australia has long been committed to helping protect children online. We take a comprehensive approach to online safety that includes the development of family safety technologies, guidance and education for families and children, and partnerships with industry and law enforcement to combat online crime.

Online child safety is directly in line with Microsoft's overall commitment to promoting greater trust online and to offering products and services built with consumer safety in mind. Microsoft will continue to invest in programs, technologies and partnerships that advance the goals of safe computing for children and families.

As stated in our submission, we recommend the Government take additional steps to help protect children and young people online, these include:

- Appoint a "Cyber Tzar," located in Prime Minister and Cabinet and adopt a national strategy that incorporates activities and education to assist children and young people in the online environment.
- Examine opportunities for bringing PhotoDNA technology to Australia.

- Further promotion and education for parents regarding the deployment and use of parental controls on computers.
- Continue to work with Government in the development of digital age verification technologies.

Microsoft Australia looks forward to working with the Joint Select Committee on cyber safety in implementing these initiatives to further protect children and young people online.

**CONTACT**

Please address any questions regarding this submission to:

Sassoon Grigorian
Manager, Government Affairs
Microsoft Australia
1 Epping Rd
North Ryde NSW 2113