SUBMISSION No. 140

As a parent - and as a former convenor of the Classification Review Board – I have been aware of the issues around cyber safety for some years. My daughter was seven when she first encountered pornography online. Her school (she was in Year 2) participated in the online maths practice program Mathletics. One day when she clicked on the link to Mathletics, it took her to a pornography website and she called me saying "Mummy the computer has done something funny and there are strange people on the Mathletics site". Some hacker or virus had attached itself to the Mathletics address and was taking children to a porn site. Fortunately, it was one that needed you to accept that it was an adult site and you had to click a link to access the more graphic content

As a sophisticated computer user, I immediately ran a virus scan, removed the cache, deleted any shortcuts to the site on our computer and created a new link to the Mathletics site after having turned the computer off and logged on again with all the refreshed settings. However, apart from the concern I felt for my innocent daughter being subject to this inappropriate material, my concern was for all the other parents who may not have known how to stop their children seeing these images repeatedly or for those of older children who may not have even told their parents about the images and accessed them "voluntarily". The images would have been classified as images of full frontal male and female nudity in sexualised depictions and have been at least in the MA15+ classification range.

More recently, my daughter and her friends took photos of each other on the beach when they were wearing their bikinis. There were five girls involved and they were aged 12 to 13. They posted these images to their Facebook pages. As I am a friend of my daughter on Facebook I soon saw the images and was concerned that – although what for them were innocent enough pictures – such images were available to the broader Facebook community through each girl's hundreds of "friends". Within two hours of posting (I hadn't seen them until about three hours after upload) there were comments from Melbourne, Western Australia, Hong Kong and within NSW about these images.

Again as a sophisticated Facebook user, I immediately deleted them from my daughter's page, went to the source computer and deleted them from that and deleted them from the camera on which they were taken. I spoke to the parent of each girl and told them of the pictures and suggested they look at them. I had to explain to several how to access Facebook, how to look at images and how to remove posts. Some parents didn't have access to the internet at home. I also had my husband visit the parents of a teenage boy who had made some comments about the photographs during the window in which they were uploaded.

These photos were taken by the girls without thinking about the consequences. They hadn't thought at the time they were doing anything inappropriate. They could not foresee the dangers of uploading such content to the internet and thought only their "friends" would see the pictures. The fact that combined they had more than 1500 "friends" and that for several of the girls their "friends' friends" could see the images meaning a legitimate audience of several thousand – let alone the people who can hack into anyone's Facebook account - never occurred to them; and this despite the girls having received training on cyber safety at their school that very week.

Several of the parents couldn't log onto Facebook let alone understand the privacy settings that could/should be set to protect their daughters. They didn't understand that the profile pictures (some of the girls changed their profile pictures to those taken on the beach) could be seen by anyone on the internet. Some of the girls had their school listed on their profiles, some had their home addresses and/or phone numbers. Neither the girls nor most of the parents could foresee any of the issues that could potentially arise because of the availability of this material.

My daughter and her friends have all had cyber safety training at school. I have looked at what was covered and the method used and it seems to be comprehensive, informative and engaging. However, what they learned in the classroom did not translate to their own experience. Much of what is covered is about bullying, being exploited by others or the online "stranger danger" that children face.

These children put themselves in danger through innocence. They thought they were pushing the boundaries a little but didn't understand the consequences despite them believing that they were well aware of what they were doing. Their parents – all of them – were ignorant of the girls' online activities and of how the material could be accessed or how it could be used by those with little concern for the girls' best interests and by those of ill will. One parent berated me for "making such a fuss" about "after all what every girl in high school is doing".

My submission to date explores the issues facing well-meaning and supportive parents with ordinary, every-day children. The issues for children whose parents aren't engaged or – worse – are engaged in exploiting their children are so much greater.

Recommendations

- Cyber safety education and training needs to start with parents of pre-school aged children.
- It needs to be undertaken in a way that empowers parents.
- It needs to be undertaken at a time when parents still might know more about the online world than their child does.
- Parents should understand what they are giving permission to when allowing children to access internet sites – from Club Penguin to Facebook and everything in between.
- Ignorance by parents should not be accepted as an excuse – if you have a child you have to protect that child regardless of whether the

- Parents of older children need regular scenario-based access to information.
- The Bark brothers' film Best Enemies (2009) is relevant and appropriate for parents and teens (although this is more about bullying).
- Parents need support in engaging with online media such as Facebook, Skype and Twitter right throughout the school years – not just voluntary sessions provided by the local council and youth service
- It needs to be part of the requirement of educating children in Australia and be attended by at least one parent of all pre-school aged and school aged children.
- There needs to be consequences for parents who allow their underage child to access these sites before they are supposed to have them (they fake their birthdates)
- Parents need to be made responsible for their children's actions.
- This is a societal issue and needs a societal response – it is not enough to leave it to schools and the police who are far too overstretched to be engaging with anything but the worst of cyber crime.
- If the Federal government is to fund computers for all high school students, then it needs to go hand in hand with online training for the parents of these children.
- Community service obligations are part of Australia's telecommunications history. This model could be adopted for ISPs, social media sites and other sites that attract children. These providers could be obligated to provide or fund this training.
- Such training could be provided online for parents. And while some children might "complete" the training on behalf of their parents, just because some people will always attempt to rort a system is no reason to avoid doing anything.