Submission to the

Joint Select Committee on Cyber-Safety

By Civil Liberties Australia

Introduction

The first thing to consider when discussing children and young people is to have a clear understanding of what it means to be young.

Childhood is a time in all our lives for learning, developing and growing. It isn't accurate to consider children as innocent, 'lesser' adults, but perhaps better to consider children as inexperienced people. Part of growing up is understanding how to cope with the full range of human emotion, passion and hardships that a full life will bring.

A parent's role is not about shielding their child from the reality of the world, but rather about providing digestible exposure to the full wonders and horrors that are reality. Most people's goal is to equip their child with a complete emotional and intellectual toolbox to tackle any problem as an adult, while providing a safe, and supportive, environment to allow the child to explore and experiment.

Of course, part of the trouble for children and young people is that their inexperience means they will sometimes lack the knowledge and wisdom to make the best decisions. This can often manifest in not having a clear understanding of the value, power and responsibility of the technologies we give them. Noted therapist Dr Marty Klein[1] said this well:

> *"[We] put the world's most powerful communication tools into the hands of children, and expect children to use them thoughtfully, safely, wisely. Then parents are outraged when kids do with digital technology what they also do with magic markers, French fries, and rollerblades: use them carelessly, selfishly, casually, and stupidly. You expect your kid to be more thoughtful with her cellphone than with her sweater?"*

A large part of the cyber-safety concerns that children encounter are a result of parents putting extremely powerful technology into their hands before they have the wisdom and maturity to understand the responsibility that brings. Today's mobile phones are more powerful and provide greater communication options than high-end desktop machines of as recently as 10 years ago, yet are readily given to many children before their teenage years.

---

[1] http://sexualintelligence.wordpress.com/2009/11/17/my-new-digital-camera-sexting-in-middle-age/

The power this technology brings is hugely important for Australia's industry, business and innovative future. Government should not be trying to limit this power: even best- intentioned limitations will have unintended consequences, and could make Australia less competitive. Instead government should aim at helping parent's to better present this powerful technology into portions that children and young people will be able to benefit from, while still learning about its value.

Technology

There are core principles of living in a free society: they include a presumption of innocence, and also freedom of choice. Measures that assume Australians are criminals or incompetent should be looked on with disdain; freedom of choice also means the freedom to make bad choices, especially where 'bad' is a subjective quantity.

The recently released Cyber-Crime Report contained a number of good suggestions, but also some rather shocking ones. Interestingly, examining the list of witnesses and submissions shows almost all are from big business, law enforcement and government departments. There are few from end-users groups, or indeed end users themselves. End users are one of the largest groups affected by online crimes, but will also be the ones largely monetarily affected by suggestions (such as 7.65) requiring the installation of anti-virus software. A new code of practice could indeed encourage ISPs to inform clients about security issues, but the requirement would assume Australians to be incompetent to make their own decisions.

Another thing to keep in mind is that all technology products are going to ship with bugs. Software projects are very complex. It is no longer practical for even the simplest software developments to test all eventualities and still be competitive.

Civil Liberties Australia certainly agrees that government needs to encourage greater technical literacy in all areas of the country. Law enforcement in particular could certainly benefit from 'Internet street smarts'.

It is also important that the government should be seen to have a high level of technical competence. Hearing comments from the responsible Minister referring to 'spams and scams' coming out of the 'portal' is the equivalent of hearing the Education Minister claiming that the Earth is 10,000 years old, or the Health Minister proposing a Medicare subsidy for phrenology. Any technically-literate Australian hearing such comments coming from government can only be worried about the competence of the technological decisions made by that Minister.

In this vein, the suggestion (11.27) in the Cyber-Crime report that a mandatory Internet filter will do anything to combat online crime is preposterous, not least because – as the government's own reports reveal – circumvention of the filter will be a trivial matter, able to be done in a trice by anyone with just above basic skills.

Further, blacklisting malicious websites could be considered counter-productive, particularly in relation to Cyber-Crime. Blocking websites that deal with detailed instruction to crime keeps the innocent ignorant, as well as affecting the potentially guilty: how are people to know to suspect a person purchasing a large quantity of fertiliser if they can't know that fertiliser can be used to manufacture explosives?

Cyber Safety

Online Environments

The Internet and cyber technology are rapidly becoming a utility, a basic of life, like electricity and water. The Internet is intrinsically integrated into the lives of many (and probably most) Australians. It is hardly an ungovernable 'wild west', and largely does not require specific laws or regulation. Fraud, for example, is a crime regardless of whether it is committed online or offline...as would be fraud committed in relation to an electricity account.

Internet-enabled equipment is increasingly expected rather than the exception. The Internet itself is unlike anything we've seen before. It supports a huge and growing number of protocols, each of which have their own peculiarities and concerns.

This all means that the Internet, as a whole, is highly volatile and dynamic. Attempting to legislate to any particular incarnation will result in the legislation quickly being outdated and could prevent exciting new opportunities from launching in Australia until the law is changed.

Typically, what people tend to think of as 'The Internet' is the World Wide Web. This consists of the web pages that are served through browsers that most people are familiar with. It should be noted that this is not even the majority of the traffic that travels over the Internet.

In non-home environments where children are likely to have access to the Internet, their access is likely to be restricted to the Web. Most other protocols require separate applications that any decent system administrator could prevent.

Online Abuse

Governments are good at creating new words and phrases for things that already exist and are already a problem. 'Cyber-bullying' is one such phrase. Bullying is certainly a problem, and has been a problem in schools for a long time. Cyber-bullying is simply using modern technology to make attacks quicker and easier. The underlying problem that bullying exists hasn't changed. Bullying is going to be aimed at someone familiar, which means, in most cases, someone who goes to the same school as the bully. That is the core problem that needs to be addressed, not the means of delivery of a message.

Inappropriate Social and Health Behaviours

It is certainly true that there are online places that do advocate undesirable behaviour. Certainly young people also engage in undesirable behaviour online. One recent example is that the filming and uploading of school fights isn't uncommon. As with bullying, one has to consider though, is it the filming and uploading that is undesirable, or the fact that a fight occurred in the first place?

The promotion of particular unhealthy behaviours online should not be considered greatly different taen the messages delivered through other media channels. Web pages do not just jump out at users; you have to actively browse to reach a web page. This means that when a young person is getting unhealthy messages from particular sites they would have to be already leaning in that direction, and sought it out to get confirmation that they weren't alone, or someone else brought that particular site to their attention.

For example, there is a fair amount of social pressure to be unhealthily thin. Are we really to blame a website for a child's eating disorders, when a child searches for information on becoming thin? Isn't the fact that the child was searching for that information in the first place the bigger problem?

Another large subset of concerns centres around access to online 'pornography'. Children, young people, are certainly going to seek – and find – information and pictures related to sex. It is now simply technologically impossible to delete or block all such information on the Internet. The reality is that people, and particularly teenagers, have a great curiosity about sex. It is a major part of the human experience, yet one that many adults refuse to discuss seriously. In the absence of decent answers to the questions young people have, they turn to other sources, including the Internet.

There was a recent study in Australia into the usage and demographics of people who employ pornography in their lives, called *The Porn Report*. This is a large percentage of the Australian population, and a surprising and growing number of women. Adolescents are not asexual beings who only think of engaging in sexual relations upon turning 18. Indeed, many children discover masturbation in their pre-teen years. A view of children as completely asexual is unrealistic, and potentially harmful in the long term.

What is required is age-appropriate sex education, through the school system, right from the beginning. Mechanics is not necessary until children are older, but the names of all body parts, the importance of privacy, and dangers of abuse are critical from an early age. Additionally, what makes for good relationships, communication and the importance of being comfortable and ready before any sexual acts are engaged in, are also important topics. Given the prevalence of pornography, it is probably also a good idea to diffuse some of the less healthy messages given, such as lack of condom use. Parent's should also be encouraged to discuss sex and relationships with their children.

This, together with 'sexting', leads into child pornography laws as they are currently written in many states. While it may make parents unhappy, young people are going to be in relationships, and some of these may involve sex. As such, and given that young people are now in possession of camera-equipped mobile phones, it is inevitable that some will choose to send sexual pictures to each other. Whilst the sexual education above should discourage this behaviour, no minor involved in a healthy relationship should ever be considered a "child pornographer" nor in possession of "child pornography" for such behaviour. About the worst thing we can do to our young people is brand them as sex offenders: the current laws turn experimenters into criminals. The real issue is when and how the images are made publicly available. The person(s) who makes the images publicly available should be made responsible for that act.

Breaches of Privacy

It is a little rich for the Government to claim to show concern for breaches of privacy, given the recent revelations from the Department of the Attorney-General of its plans for a new Data Retention policy which would be the single greatest breach of privacy by government in Australia's history. The Government's tendency towards secrecy is of great concern, shows a profound lack of understanding of technology and the Internet, and demonstrates a casual disregard for the rights and privacy of citizens.

Having said that, there are certainly concerns for children and young people's privacy online. For the time being, at least, this is largely the result of children, young people and even parents not taking appropriate precautions with the details they choose to make available online. Research appears to indicate that a change in culture is under way, where privacy is no longer a major concern for the populace, particularly younger people (although, that is not an excuse for government to ride roughshod over everyone's privacy). The more likely scenario is that many

people simply do not realise that the Internet never forgets, and information posted online in the heat of the moment may come back to haunt him/her at a later date.

The privacy issue has the same cause as many of the other problems encountered in relation to Cyber Safety; there isn't a high level of technology literacy among the general population.

Australian Responses

The government should not give Australian parents a false sense of security on these issues. The proposed mandatory Internet filter, for example, is being sold in a way that will do just that. It will do absolutely nothing to:

- stop bullying,
- prevent access to age inappropriate material,
- eliminate spam, or indeed
- prevent a single child from being abused.

It will increase the economic gap between well-off and less well-off families, as the cost of access increases, preventing some parents from being able to provide for their children. It may indeed increase the problems associated with children and young people's online safety as a false sense of security will mean even more parents will grant their children <u>unsupervised</u> Internet access.

Every expert agrees that the best form of security over children's use of the computer and associated technology is a close involvement and supervision by one or two parents. A mandatory Internet filter will stop or reduce that happening in Australian families.

Supporting Schools

One major point to keep in mind is that there will always be a subset of school children and young people who take any security measures put in place as a challenge rather than for their protection. Some of these children will be more technically competent than the people responsible for the security in the schools. Partly this is a result of schools simply not having the resources to hire people who have the necessary security literacy, but it is also a result of some children having a natural aptitude for technology and the dedication and drive to learn more. Such dedication and drive should be encouraged, because these children could have a lot to contribute to Australia if it can be productively channeled, but it does cause a short-term problem, which could be turned into an opportunity. Such children are technically competent enough to avoid online issues themselves, but they could leave holes open that would allow other, less technically literate children access to age-inappropriate material. The opportunity exists to enlist the help of technically literate young people to help protect the technically illiterate, teaching responsibility to both.

As discussed above, the focus should be on learning responsibility, just like it is far more important to work on solving the problem of bullying rather than just 'Cyber-Bullying'.

Role of Parents, Family and Carers

Governments and ISPs can certainly do their part to raise technical literacy and provide help and support in dealing with online concerns. Ultimately, it has to be a parental responsibility to raise a child with the values and principles that the particular parents believe in. Families should be given options on how best to protect their own children to their own standards. A one-size-fits-all approach is not going to be appropriate and – as outlined above – will in fact be counter-productive to expanding the number of parents who monitor and moderate their children's use of technology.

The solution to the problem of Cyber-Safety should encourage closer child-parent-teacher involvement, not discourage it.

Governments operate best when they facilitate and encourage responsible community behaviour, rather than browbeat and corral society into group-think. The days of control freak behaviour are over.

Governments are not like churches or religions, which must impose hard and fast 'commandments' applying to all to ensure uniformity of belief and action. Governments preside over vastly different belief sets belonging to families of all – and no – religious persuasion.

Where there is a dichotomy between presumption of innocence and freedom of choice – as opposed to pre-allocating guilt and curtailing options – governments should always trust their people more and let them choose for themselves the best course of action for their individual circumstances.

Australians deserve to be trusted by the Australian Government. If we trust people to elect our Government by an exercise of free choice, our Government should trust the good judgement of Australians in return to choose appropriately to look after the best interests of their own children.

ENDS