SUBMISSION No. 40

I welcome the opportunity to make a submission to the Joint Select Committee on Cyber-Safety.

Before addressing the committee's terms of reference in detail, I would like to make the following general comments.

1. Cyber-Safety is by no means exclusively an issue for children. The terms of reference should have allowed for dealing with cyber-safety as it applies to any Australian internet user.
2. While acknowledging that "unsafe" things do occur on the internet, it is important not to exaggerate the frequency or risks.
3. Up to now, the Rudd government has taken a very confrontational approach to the internet. I would like to emphasise that `(a)(iv)` specifically uses the word "cooperation".

```
(a)(ii) the nature, prevalence, implications of and level of risk associated with cyber-safety threats
```

There must be significant uncertainty as to what the prevalence of those threats is.

It would probably be better not to group sexual grooming with the other threats under "abuse of children online". Lumping bullying in with potential sexual abuse reduces the gravity of the latter.

Similarly "illegal and inappropriate content" reads oddly. In the context of viewing by children, the distinction between "illegal" and "inappropriate" probably doesn't matter much. The boundary between "illegal" and "legal" is a long way from the boundary between "inappropriate" and "appropriate". Consequently, this item should probably just be "inappropriate content".

However "inappropriate" is not easy to pin down. A household may have children with a range of ages, and children of the same age may have different levels of maturity and worldliness. Likewise households may have different views about what is appropriate, given children of the same maturity.

Regarding "identity theft", there is already software available to run on a PC that attempts to protect against identity theft.

There may be a role for government in requiring Australian banks to strengthen internet banking. Some current weaknesses are:

- secure web site is accessed by navigating from insecure web site
- login security is limited to keyboard entry of a username and a password
- a single transaction amount limit applies to all transactions

However this is straying somewhat from identity theft to general fraud, and may more of a problem for adults than children.

Certainly children may exercise poor judgement about what identity information is appropriate to disclose. On the other hand, society is changing. We should be careful not simply to impose our values on younger people.

Regarding "breaches of privacy", it would be ironic if the government, in its excessive response to perceived cyber-safety issues, itself created the greatest breach of privacy. The government should drop plans for ubiquitous internet surveillance e.g. recording all web sites visited, or recording of all email sent and received etc.

Cyber-stalking is not limited to children. Ditto technology addiction. Ditto identity theft. (If anything, identity theft is likely more of a problem for adults.)

```
(iii) Australian and international responses to current cyber-safety threats (education, filtering, regulation,
enforcement) their effectiveness and costs to stakeholders, including business
```

It is important to note that there are some limits to the effectiveness of Australian government responses i.e. where some stakeholders are based overseas. The internet does not recognise national borders. Where it is sufficiently important that there be a government response, this may require international cooperation. However governments should not overreact.

Fortunately the most effective response is education, and this is not dependent on international cooperation. This can be relatively cheap. It doesn't matter whether a social networking website has a "panic button" if the child is not sufficiently aware to recognise that "panic" is the appropriate thing to do.

The next most effective response is supervision. Likewise this is not dependent on international cooperation and likewise this is relatively cheap. There is no substitute for _parental_ supervision. Not software on the PC. Not software in the ISP. Not regulation or legislation. To this end, the physical location of the computer should be considered carefully. It should be located where supervision will occur incidentally, as well as deliberately.

It would be difficult to overstate the importance of education and supervision.

PC-based filtering should be considered as an adjunct to education and supervision. It's true that a sufficiently motivated child can bypass a PC-based filter however the focus of filtering should be on preventing *accidental* access to inappropriate content, so bypass is not so much an issue. PC-based filtering offers high flexibility. There are already a range of free and commercial offerings.

The government should *drop* any plans for requiring ISPs to *offer* ISP-based filtering (and *drop* any plans for requiring ISPs to *impose* ISP-based filtering i.e. internet censorship). The government has created a toxic environment of mistrust that is unhelpful towards cooperative approaches to

improving cyber-safety. ISP-based filtering is also easier to bypass than PC-based filtering, less flexible and more expensive. ISP-based filtering, in any form, presents a tempting avenue for abuse by government.

Parents should exercise discretion about buying handheld *direct* internet access devices (e.g. the more advanced mobile phones and e.g. tablets) for their children.

(v) examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised

To maximise the benefits of the internet, the government

- should encourage the greatest availability, and
- should not take steps that will increase the cost.

Therefore the government's NBN approach could be construed as unhelpful, with its high cost effort to ensure high speed internet is available to 90% of the population, whereas for much less money the government could ensure that *reasonable* speed internet is available to almost all Australians.

Clearly requiring ISPs to filter the internet or conduct ubiquitous surveillance imposes costs that reduce the economic benefits of the internet and could even compromise availability.

Technological aspects are only part of the story however. To maximise benefit, Australians must approach the technology with confidence and perceive it positively. Here education plays a role too.

(vi) ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying

I would like to note that bullying predates the internet. It has probably been around as long as humans have. As such, schools should be working on reducing all forms of bullying. Indeed the mere use of the term "cyber-bullying" distracts attention from the underlying problem (and causes) by focussing on the mechanism.

Schools can play a role in education on cyber-safety. Curriculum sessions should be delivered by schools, so that children are given formal instruction regarding the risks that they may face online, and the practices that they should adopt to reduce those risks. This is a part of computer literacy. Clearly this would involve cooperation with state governments, and also engagement with the private education sector.

(viii) the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues

I support this proposal. If nothing else, it will offer a central collection point for real data about cyber-safety issues, so that future government policy can be based on good information about what cyber-safety issues arise and with what frequency.

Parents and/or children may be more comfortable reporting an incident to an Ombudsman rather than to the police, which may be more intimidating or may be perceived as an overreaction.

However procedures would need to be developed that cover whether the Ombudsman would forward the issue to the police. Likewise, procedures should be in place so that issues reported to the police are forwarded to the Ombudsman (at an appropriate time and with an appropriate level of detail).

The Ombudsman can advocate with online service providers but any attempt at enforcement is likely to be unhelpful. (Any breach of actual law should be left to law enforcement and the justice system.)

Statistical information about number and type of issues notified to the Ombudsman (via whatever mechanism) should be reported annually to the public, and to the parliament.