Enhancing Online Safety for Children Public consultation on key election commitments January 2014

March 7, 2014

Department of Communications GPO Box 2154 CANBERRA ACT 2601

The Director, Cyber Safety Policy and Programs,

It is with great interest that I give some abbreviated feedback for this public consultation period looking into digital safety and children and youth. This is my specific research area at the University of Queensland and I look forward to following this evolution of policy and practice. In short, I have come across the same statistics in terms of usage, harms, and social networking practices of young people. My interest in this issue is twofold – firstly investigating the considerations that youth make when using digital media and secondly to follow the role of technology as an actor, facilitator and mediator of digital practice. The basic premise is that technology changes us in ways we often do not anticipate or consider. Ultimately, technology enables a new digital ethical landscape to negotiate with indeterminate ends. This environment is difficult to understand for adults and clearly a minefield for children and youth who are, for the most part, not actively considering the complex and unfolding impacts of their daily digital footprints.

From this assertion, that technology affords incomprehensible and unpredictable aspects of digital practice, a sensible approach for children and youth would be one of protection – as offered as part of this document. However, I believe this is a limited and unsustainable response as proposed. I would argue for a more complex and multipronged approach that includes many of the systems already set up to address this issue – most importantly the Australian Curriculum. Ultimately, online safety for children will only be ensured through a rigorous program embedded within the educational system. 'Add on' curriculum and information such is available through government and non-government websites and technological features such as filters, blocks to websites, pulling down inappropriate material and posting warnings are useful but do not solve the critical issue – ignorance in the use of digital media (evidenced by cyber bullying and sexting behaviors) and premeditated predatory behaviors.

As we have seen, technology is continually morphing to adapt to filters, barriers and blocks. The snap-chat phenomenon is a good example of how sexting was facilitated by a more ostensibly ephemeral practice (chats or photos that would be destroyed by the sender after a couple of seconds) that was subverted by permanently capturing images or words by apps or screenshots. There are numerous examples of these types of adaptations to fix cyber safety problems.

In the end, a good education is the best and most sustainable remedy. Therefore I would recommend prioritizing digital literacy and digital ethics in schools. Filters, blocks and rapid removal practices will have an impact, however the Internet is an uncontainable space. Once photos, ideas and concepts are shared it is like scattering seeds in the wind – there is no practical way to collect them all up again. The best strategy is to rigorously include digital literacy and digital ethics into curriculum and to reduce the number of children and youth who actually engage in these negative/destructive behaviors. In addition, there should be a focus on at-risk kids – as these are the most common victims and most likely to be harmed in the digital

sphere. Secondly, I would support strong enforcement of the Section 474.17 of the Criminal Code. This gives a front and back response – strong education, including the criminal penalties, and an enforced criminal code.

The last area to support for me would be for decentralized site moderation practices for social media. During my research I have witnessed very direct solicitation occurring on teen chat sites — and open requests for webcam chats. This is not a buried practice but open and common. I have also witnessed chat sites directly reconciled by moderation and having site rules and people being kicked out if they are inappropriate or do not follow site expectations.

In terms of a body that would operationalize the Child and Youth Esafety program I would not recommend an NGO. As you may already recognize, many youth and technology NGOs are biased and operate to deliver specific outcomes. As an example, the *Young and Well* group appears to simply support technology and looks towards ways of supporting positive technology use. This would prohibit this group from making and supporting any research that may question the place of technology or research that may shine light on some of the crucial and problematic elements regarding children and youths relationship with technology. Obviously, *Young and Well* has some very useful and commonly shared beliefs – respect, health and acceptance. I personally would have more faith in the ACMA approach where the preeminent focus should be health and welfare for Australian children and youth as the central concern and coupled with a more objective view to the child-youth- technology nexus.

I have just started my research so I would not like to claim I have any expertise in this area – at this point I would call it a great interest. I do think the EFA (Electronic Frontiers Australia) obviously another tech focused NGO has an interesting idea about the Bill of Digital Rights – looking at the Internet according to rights and responsibilities as something that deserves greater consideration.

In the end, I am very busy and therefore unable to give more detailed feedback.

Q1 – I do not think this report gives enough information to be able to make an assessment of the programs and powers to be assigned to the Commissioner. As this is a very complicated space with significant impacts and implications, I would suggest that a **Cross Sector Board**, rather than a single Commissioner, would be more appropriate. As cyber safety is an emerging and growing matter of concern, which has education, policing, social services, legal, communications and media (ACMA), technology and cultural dimensions it would be difficult to imagine a single person or unit that would be able to consider this issue in its entirety.

I do think there is a redundancy of cyber safety information on the Internet – although I do not know if that is a negative reality. Seeing similar messages from different organisations could lead to a greater appreciation of how important this topic is for youth and children; but I also recognize there is government spending inefficiencies with that model.

Q2 – I personally do not like any of these options. They are either too expensive or limited in their make up and application. I would recommend for a Board that creates policy, procedures and guidelines and to use the current social services, educationa and legal strucutures that are in place. Option 3 is the least optimal as I noted before.

Q3 – boyd and Ellison have done substantial work in this area and would be appropriate researchers to look for guidance for definitions of social networking sites.

Q4 By the definition given by boyd and Ellison games with conversations would apply. If communication is part of the experience there is social networking.

 $\ensuremath{\mathsf{Q5}}\xspace$  I am sure there are experts in the field who could make this assessment.  $\ensuremath{\mathsf{Q6}}\xspace$  -

Q7-10 I do not think this is a sustainable or reasonable first priority for the issue of child and youth safety. Clearly, as part of a suite of actions taking down objectionable material would be beneficial – but how would this be operationalized effectively? What happens when digital objects just move? How many complaints would this office be able to attend to? And how long would it take in the event that it was clearly established that the artifact was harmful? I don't see this as practical.

Q11 – In the end these should be legal matters and left to policing in the case of cyber bullying or child pornography (including under age sexting). These legal matters should be strongly supported through effective education. Not the marginalized tack on later educational practices that often occur now. Examples of this are the once a year 'specialist cyber safety' talk circuit at many Queensland schools.

Q20 – For the most part the law is fine – it needs to be shared through an educational context and enforced.

Q22 – No merit – it should stand – and people should be aware that it is a highly inappropriate practice and that it carries a legal punishment or fine.