SUBMISSION No. 78

WESTERN AUSTRALIA POLICE

OFFICE OF COMMISSIONER OF POLICE
POLICE HEADQUARTERS
6TH FLOOR
2 ADELAIDE TERRACE, EAST PERTH
WESTERN AUSTRALIA 6004
TELEPHONE : (08) 9222 1256
FACSIMILE : (08) 9222 1717

Your Ref:
Our Ref: 0136410FV001
Inquiries: Detective Inspector Bob Kirby

Mr Jerome Brown
A/g Committee Secretary
Joint Select Committee on Cyber-Safety
R1-109, Parliament House
PO Box 6021
Canberra ACT 2600

Dear Mr Brown

Thank you for your letter dated 14 May 2010 inviting submissions from the Western Australia Police on Cyber-Safety. I will individually address each of the topics you raised.

1. The online environment in which Australian children currently engage

Social networking and peer-to-peer sites provide an opportunity for adults to exploit children with some degree of anonymity. Adult offenders often engage with children through chat rooms and other social network programs, using computer technology to both procure children to commit sexual acts as well as using them as a mechanism to transmit both video and digital images of themselves performing indecent explicit acts.

The use of text messaging and sending photos by mobile phone is becoming more common and creating an environment in which offences are being committed. Mobile phones offer communication connectivity and mobility that makes it easier for children to communicate with others without appropriate supervision. It therefore allows offenders to communicate with children thereby enabling an increase in the risk of offending.

2. Abuse of children online, particularly cyber-bullying

The practice known as "sexting", whereby explicit photographs and videos of children are forwarded via mobile phone to other children is becoming more prevalent. These images are often spread amongst children and the ramifications to the child who initially sent them are enormous.

The use of social networks to groom and commit offences against children is increasing. Children are often coerced into sending photos and using webcams to expose themselves to adults or other children. Covert operatives posing as children online, often identify offenders exposing themselves and committing explicit sexual acts.

Another practice we have seen increasing recently is "bots" or software programs that engage people via social networking sites and are, therefore, often engaging children. These programs try to encourage the user to enter websites with adult content.

Cyber-bullying appears to be a significant issue. Whilst not dismissing the significance and the impact of "playground" bullying, it is generally limited to a small cohort (within the school).

With cyber-bullying, the audience and potential offenders are infinite and the outcomes can be enduring. Also, young people engaging in cyber-bullying have a sense of anonymity, feeling that they will not be caught and do not have to face their victim. Because there is no physical contact, the physical attributes and characteristics can go against what we might see in the "playground". That is, the victim could be a person who might otherwise be more likely to handle themselves in the playground, and the offender could be a person who might otherwise be less likely to be an offender in the playground.

There is no specific "cyber-bullying" legislation in Western Australia. However, depending on circumstances, there may be scope for police intervention. For example, "threats" is covered in Chapter 33A of the Criminal Code and "Stalking" is covered in Chapter 33B of the Criminal Code.

3. Inappropriate social and health behaviours in an online environment

Due to their anonymity, social networks provide an environment where inappropriate behaviour can flourish. From a policing perspective, the long term mental and physical impact to children may lead to offending behaviour, however, further research would be required to identify and measure any link between offending and the use of social networking interaction.

4. Identity theft

Although not specific to children, the Criminal Code Amendment (Identity Crime) Bill 2009 - Bill Number 104 has been passed by both Houses of Parliament in this State and is awaiting Assent.

This Bill addresses the unlawful use of another person's identity.

5. Breaches of privacy

The WA Police do not investigate privacy breaches.

6. Australian and international responses to these cyber-safety threats

WA Police currently chairs the Australian and New Zealand Police Advisory Agency - Child Protection Committee (ANZPAA-CPC). Through this committee, strategies are being developed to prevent, detect and disrupt the distribution of child exploitation material (CEM).

The use of technology known as Global File Registry (GFR), which uses hash values (digital numbers used to identify images) to prevent the distribution of known images on peer-to-peer networks, is currently being explored through the ANZPAA-CPC. This initiative will require the cooperation of Internet Service Providers (ISPs) across Australia if it is to be successful. If the technology is adopted, ISPs will have the capacity to automatically filter out known CEM as it travels through their servers.

The identification of child pornography and exploitation material is also being addressed through a national information technology project known as "CETS / ANVIL". Once implemented, CETS / ANVIL will allow law enforcement to automatically compare seizures of suspected CEM against a known data-base. This will speed up the process for assessing images, and allow more time for law enforcement agencies to assess unknown images, potentially identify victims and contact offenders.

The Australian Government is currently undertaking a project to filter known URL sites that contain child exploitation material. This strategy is also supported by WA Police.

7. Opportunities for cooperation across Australian and international stakeholders in dealing with cyber-safety issues

Opportunities exist to have both social network and internet service providers (ISPs) develop a code of conduct for the operation of their sites to either filter or block CEM being distributed through their networks or servers.

There is already some level of cooperation in regard to law enforcement nationally and internationally with specialist software being provided to identify the distribution of CEM on peer-to-peer networks. WA Police use these tools on a regular basis.

With the availability of GFR technology, ISPs have an opportunity to block all known CEM images being distributed on internet networks. This will require significant cooperation and agreement between ISPs.

One challenge currently being experienced by the WA Police is obtaining quicker and easier access to companies' information (Facebook, MySpace, Microsoft etc) either for a law enforcement purpose or when bullying needs to be reported. Advice is often provided to users on reporting abuse / bullying to the companies, however, it often takes many weeks before the companies resolve the issues reported.

8. Ways to support schools to change their culture

Robust policies on the use of computers and the internet need to be developed and embedded at an early stage by education providers. At present, the Australian Communications and Media Authority and Australian Federal Police provide support to education providers on request (e.g. Think U know program). These are positive initiatives which need to be built upon.

9. The role of parents, families, carers and the community

Parents and carers play a significant role in preventing cyber-bullying and on-line child sexual abuse.

Steps such as having computers in a public area, supervision and appropriate blocking software will reduce the risk to young users.

I trust that the information I have provided will be of assistance to your Committee.

Yours sincerely

KARL J O'CALLAGHAN APM
COMMISSIONER OF POLICE

29 June 2010