SUBMISSION No. 86

SOUTH AUSTRALIA POLICE
KEEPING SA SAFE

Your Ref:
Our Ref: PCO2010/4115
Enquiries: Detective
Superintendent Jim Jeffery
Telephone: 08 8172 5034
Facsimile:

Mr Jerome Brown
Acting Committee Secretary
Standing Committee on Communications
PO Box 6021 Parliament House
CANBERRA ACT 2600

SUBMISSION NO.86

Inquiry into Cyber-Safety

Dear Mr Brown,

I refer to your letter dated 14 May 2010, inviting South Australia Police (SAPOL) to provide a submission to the Joint select Committee on Cyber safety issues affecting children. The following information outlines SAPOL's response to the issues identified for comment.

Online environment in which children are currently engaging

The South Australia Police provides a law enforcement response to members of the community who report having been the victims of crime. Those reports indicate children are increasing using mobile phones, computers and other devices as a means of communication subjecting them as a victim of a crime and/or a perpetrator. Incidents have included, approaches to children for sexual purposes, production and dissemination of child pornography, unlawful threats and stalking. Whilst children have access to computers in schools and cyber cafes the majority of reported matters involve the use of personal devices. The use of mobile devices in particular has and does lead to almost instantaneous sharing of information including the recording of what amounts to electronic evidence where the images, postings and videos depict the commission of crime.

Abuse of children on line

Online predatory procurement and grooming of children for prurient purposes is policed by reactive response to reported crime and through identification of offending behaviour by covert means. Legislation provides significant penalties for people who incite or procure indecent acts involving children, communicate with children with the intention of procuring sexual activity or making children amenable to sexual activity.

The laws do not specifically mention the online environment however, they were designed to deal with the opportunities that the Internet and other telecommunication media provided to facilitate predatory criminal behaviour.

SAPOL has a number of means for policing suspicious communications between adults and children including covert and under cover operations to referring the matter to other Law Enforcement Agencies where a jurisdictional nexus exists.

Cyber bullying is not a criminal offence although some of the associated behaviours such as cyber stalking and unlawful threats are criminal in nature and therefore investigated accordingly. Whilst SAPOL regularly receives complaints regarding cyber bullying, statistics are not maintained as it is not a criminal offence. Anecdotal evidence identifies instances of bullying is rising with the increasing use of technology in society.

Breaches of privacy and identity theft

SAPOL regularly receives reports of breaches of privacy generally from concerned parents who have become aware of images of their children placed on the social networking sites of school friends without permission. Most of these incidents do not amount to criminal behaviour due to the restrictive provisions in current legislation. Incidents of criminal behaviour including the posting of intimate images without permission, stalking and instances of identity theft where the intent is to commit a serious offence are investigated by SAPOL.

Australian and international responses to cyber safety threats

SAPOL provides details of suspicious Internet web sites and content to the Australian Communications and Media Authority (ACMA) via the online reporting facility where it is suspected that the source of evidence is offshore.

SAPOL's Sexual Crime Investigation Branch (SCIB) provides a focal point for receiving referrals relating to cyber sex crimes from the AFP and other NGO groups such as the National Centre for Missing and Exploited Children (NCMEC) based in Canada. A dedicated operation managed by SCIB utilises intelligence from the Internet industry to identify people who are attempting to access child exploitation material. Referrals have been provided to Law Enforcement agencies globally.

The advent of social networking use by children regularly requires law enforcement to obtain information from sites such as Facebook, in order to identify criminal activity and safe guard the welfare of children. The manner in which this occurs is not always timely and the regulatory frameworks applied in many cases are those of foreign countries. The current process for administration of mutual assistance applications rarely produces timely investigative outcomes.

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

SAPOL regularly cooperates with stakeholders in other agencies both within and outside of the State. Materials from agencies such as ACMA and the Australian Competition and Consumer Commission (ACCC) are regularly sourced and used. The resources available from these bodies are of a high standard and SAPOL gains leverage from their use in providing information to the public. Of late there appears to be more agencies developing their own strategies and resources. This can result in key messages of safety and security becoming confused. As identified in the House of Representatives Standing Committee on Communications Report of the Inquiry into Cyber Crime, there is a need for greater coordination between law enforcement agencies.

Ways to support schools to change their culture to reduce incident and harmful effects of cyber bullying

SAPOL through the WatchSA program works with the community to reduce and prevent crime. Each of the Local Service Areas within South Australia have crime prevention personnel who have been trained in aspects of internet safety including issues for parents, adolescents, scams and computer security. These members in turn are able to deliver a consistent safety message to the community.

SAPOL has also worked with both government and non government education bodies to develop educational materials. The cyber bullying and e-crime document was distributed through Government, catholic and independent schools in 2009 is an example.

SAPOL participates in the 'Cybersmart Detectives' program, an initiative of ACMA, by providing an interactive virtual training environment between police and primary school children highlighting the dangers of cyber relationships.

Role of parents, families, care givers and the community

It is believed education is a key strategy in addressing issues relating to cyber safety. Education for parents, grandparents, care givers and children assists in reducing the digital divide. Whilst parents and care givers have an understanding of issues relating to personal safety generally, their lack of knowledge of technology can be restrictive in the personal safety discussion. SAPOL supports initiatives aimed at increasing the level of knowledge of members of the community and have developed a number of packages on topics relating to the use of technology (Internet safety, scams, security and respect). Members from each of the Local Service Area crime prevention sections have been trained in the delivery of these packages.

I trust that this submission is useful to the Select Committee and invite you to contact Detective Superintendent Jim Jeffery, Officer In Charge, Commercial & Electronic Crime Branch on 08 8172 5034 should you have any queries relating to this submission.

Yours Sincerely,

(Malcolm A Hyde)
COMMISSIONER OF POLICE

30/ 6 /2010