SUPPLEMENTARY SUBMISSION No. 86.1

SOUTH AUSTRALIA POLICE
KEEPING SA SAFE

Your Ref:	
Our Ref:	PCO 2010/4115
Enquiries:	Jim Jeffery
Telephone:	08 8172 5033
Facsimile:	08 8172 5060

Mr James Catchpole
Secretary Joint Select Committee on
Cyber-Safety
R1-109 Parliament House
PO Box 6021
CANBERRA ACT 2600

SUPPLEMENTARY SUBMISSION NO. 86.1
Inquiry into Cyber Safety

Dear Mr Catchpole,

I refer to your letter dated 30 November 2010 inviting South Australia Police (SAPOL) to provide further written submissions to the Joint Select Committee on Cyber-Safety.

The following submission is provided:

Online environment in which children are currently engaging:
The use of technology by children includes mobile phones, computers and other devices which allow for communication in a variety of means. 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. The increase in the use of devices such as mobile phones and tablets has significantly enhanced the ability of users to gain access to the Internet from any location. Current advice given to the community in having the 'Internet' computer in a family space will no longer provide a response that can ensure safety. Wireless technology freely accessible throughout the country also allows those who do not have account access to do so without oversight.

Abuse of children online:
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. SAPOL has the capacity to initiate covert investigations under the authority of an approved undercover operation. Whilst Cyber bulling is not a criminal offence, some of the associated behaviours such as cyber stalking and unlawful threats are criminal in nature and when reported are acted upon.

Breaches of privacy and identity theft:
SAPOL regularly receives reports from concerned parents relating to images of their children placed upon the social networking sites of school friends which have been posted without permission; this is not a criminal offence. Instances which do amount to criminal offences include the posting of intimate images without permission; stalking and instances of identify theft where the intent is to commit a serious offence.

Australian and international responses to cyber safety threats:
SAPOL provide details of suspicious Internet web sites and content to the Australian Communications and Media Authority (ACMA).

SAPOL provide a focal point for receiving referrals relating to cyber crime from the Australian Federal Police (AFP) and other Non-governmental Organisation (NGO) groups such as the National Centre for Missing and Exploited Children (NCMEC) based in Canada via the Sexual Crime Investigation Branch (SCIB).

A dedicated operation managed by SCIB utilises intelligence from the Internet industry to identify people who are attempting to access child exploitation material.

Internet use by children regularly requires information from sites such as Facebook in order to identify criminal activity and safe guard the welfare of children. Requests for assistance in providing information and content from overseas will require the application of domestic legislation. In cases where mutual assistance applications are required to gain access to content to obtain overseas based evidence, the processing and forwarding to other countries is counter to the requirements of timely investigations.

Since the first submission was made, SAPOL members have met with representatives from Facebook and the Attorney-General's Department on issues relating to the access of content from Facebook. Whilst Facebook have stated that they can respond to a Mutual Assistance request in 10 days, the Attorney-General's office has stated that it will take them at least 6 months to process the request before it is forwarded to Facebook. The uptake in the use of social networking dictates that law enforcement will require content from overseas providers on an ever increasing basis. There is a very real need to improve the process for obtaining information or court outcomes could likely be affected.

Access to mobile Internet Profile (IP) data which can be used to identify an Internet user is now also impacting upon law enforcements ability to investigate matters. Companies such as Optus and Telstra have informed that IP data is not available after relatively short periods of time (up to one month only). In many cases, IP data is not requested until after the expiration of such a short period. Mandated requirements for retaining information pertaining to communication would be of direct benefit to law enforcement in investigations.

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 inside and outside of the state. Materials from agencies such as ACMA and the Australian Competition and Consumer Commission (ACCC) are regularly sourced and used to assist with crime prevention initiatives.

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 and key Government Agencies.

The United Kingdom, United States of America and New Zealand have implemented centralised cyber crime reporting facilities. The roll out of the National Broadband Network (NBN) and the imminent participation of Australia in the European Convention on Cybercrime provides a timely opportunity for Australia to improve the coordination of all cybercrime security and safety activities through establishing a National Cyber Crime Coordination Centre (NCCC).

A NATIONAL CYBERCRIME COORDINATION CENTRE

The concept of a NCCC has been informally discussed within Law enforcement for some time. The recent findings and recommendations of the Standing Committee have enabled discussions of this concept to gain momentum. SAPOL has produced a draft concept paper which has been provided to the National Cybercrime Working Group chairperson.

It is timely to consider the establishment of a NCCC to deliver on four key functions across four Units, namely a Reporting Unit, Prevention Unit, Training Unit and Relations Unit (refer attachment).

Cybercrime Reporting Unit

A National Cybercrime reporting Unit could:

- Receive reports of cybercrime - preferably on-line, providing immediate preventative and security advice to the complainant and identify the origin of the offending;
- Facilitate intelligence analysis and data matching; and
- Disseminate the data and / or investigation to the appropriate agency for action.

This unit would incorporate the functions of the reporting centre concept which is being proposed by the National Cyber Crime Working Group (NCWG).

Cybercrime Prevention Unit

A National Cybercrime Prevention Unit could:

- Develop training packages and programs;
- Coordinate delivery and dissemination of prevention material;
- Operate an on-line prevention advice facility;
- Provide National media releases incorporating prevention strategies and
- Initiate prevention campaigns as required.

Cybercrime Training Unit

A National Training Unit could:

- Coordinate Tier 3 (specialist) training and deliver it when appropriate;
- Prepare Tier 1, 2 & 3 Training packages;
- Develop and administrate training requirements; and
- Develop and maintain a National capability register.

Cybercrime Relations Unit

A National Cybercrime Relations Unit could:

- Provide a contact point for outbound requests to offshore ISP's and social networking providers;
- Provide a contact point for inbound enquiries from offshore agencies and
- Assist investigating agencies with off-shore enquiries and information requests.

The NCCC would need to ensure that it is engaged to support investigations as opposed to conducting them.

What agencies should be involved?

The NCCC would need to be predominately funded by the Commonwealth and amalgamate some existing services currently provided by state law enforcement, AFP, Australian Crime Commission, ACCC, Austrac, Australian Tax Office, ACMA and Cert Australia.

The four Units would initially need to be supported by experienced representatives from the various agencies. The level and nature of involvement would be determined by the relevance of the assisting agency to each particular Unit.

An alternative option to implementing an NCCC could be to provide additional resources and / or funding to existing agencies. This option is less desirable as history suggests that it is unlikely that the existing crucial issues of coordination, equity and effectiveness, will not be efficiently resolved without all core functions being coordinated and operated by the same agency.

The effectiveness of an NCCC would be determined by the engagement of all key agencies and the establishment of functions and processes that are aligned to addressing the issues and most importantly protecting and providing effective service delivery and protection to Australian citizens.

Whilst there are concerns that the concept of a NCCC will require resourcing and funding, the risk of not addressing the current issues is that the longer that the status quo remains, the more funding and resources that will be required to rectify the issues in the future.

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.

SAPOL has also provided support and relevant information with the Coalition to decrease bullying as it relates to cyber bullying issues.

SAPOL participates in the 'Cybersmart Detectives' program, an initiative of ACMA.

Role of parents, families, care givers and the community:
Education for parents, grandparents, care givers and children is the key to addressing issues relating to cyber safety. 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 personnel have been trained in the delivery of these packages.

The Officer in Charge, Commercial & Electronic Crime Branch, Detective Superintendent Jim Jeffery, can be contacted on 08 817 25033 should you wish to discuss this submission.

Yours sincerely,

(G T Burns)
DEPUTY COMMISSIONER OF POLICE