Australia New Zealand Policing Advisory Agenc
ABN 61 537 811 305
Level 6, Tower 3, World Trade Centre
637 Flinders Street, Melbourne Victoria 3004
PO Box 415, Melbourne Victoria 3005
T +61 3 9628 7211 F +61 3 9628 7253
secretariat@anzpaa.org.au www.anzpaa.org.au

D/11/2904

20 April 2011

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

Joint Select Committee on Cyber-Safety Submission

Dear Mr Catchpole,

Thank you for the invitation to make a submission to the Joint Select Committee on Cyber-Safety. This submission is made on behalf of the Australia New Zealand Policing Advisory Agency (ANZPAA), noting that several police jurisdictions (South Australia Police, Australian Federal Police, Western Australia Police and Tasmania Police) have made submissions directly to the Committee.

ANZPAA is a joint initiative of the Australian and New Zealand Police Ministers and Commissioners and provides strategic policy advice to the ANZPAA Board on cross-jurisdictional policing initiatives that enhance community safety and security.

The cross jurisdictional nature of cyber-crime requires a coordinated response by all agencies. ANZPAA facilitates collaboration within policing and the development of effective relationships with other stakeholders.

This submission will focus on three key aspects of the Inquiry's Terms of Reference:

- The online environment in which Australian children engage.
- Australian and international responses to current cyber-safety threats.
- Opportunities for cooperation across Australian and international stakeholders.

The Online Environment

With the online environment becoming an integral aspect of our lives, it has exposed all its users but particularly children, to a number of dangers. Continuing technological breakthroughs fuelled by an ever increasing worldwide demand for fast and massive data transfers and unlimited connectivity options will only exacerbate these dangers in the future.

With an exponential increase in volume, speed, content and users, historical conventions have been significantly challenged to adapt. The propensity for evidence to be captured electronically has stretched the forensic examination capability of most law enforcement agencies world wide to capacity.

Challenges for Law Enforcement

There are a number of strategic issues from a law enforcement perspective that are critical to this inquiry:

- The reach and speed of the internet allows criminal elements to operate internationally with limited regulation. As a result a key legislative issue for law enforcement is an effective and efficient legal framework for the exchange of information and evidence with overseas agencies. The risks for cyber-safety without such a framework are continued and significant delays in investigations and the potential for some matters not to proceed to prosecution.
- The volume of data and its retention by Internet Service Providers (ISPs) for potential use as evidence in police investigations presents challenges for law enforcement as there is currently no mandatory data retention requirement in Australia or New Zealand.
- The introduction of the National Broadband Network (NBN) is likely to see further growth and sophistication of online criminal syndicates' ability to commit cyber offences and enable greater and quicker access to child exploitation material (CEM) on the internet.
- The volume of data and the expense incurred by its storage will soon prompt difficult decisions about what information to keep and how it is to be managed to ensure its accessibility.
- There is no comprehensive preventative framework in place to combat cyber-crime and thus enhance cyber-safety. Any such framework would need to be cognisant of both the educational and technical preventative tools available.
- Most programs aimed at mitigating child exploitation tend to target mainstream audiences only. If awareness programs are to reach across the entire community more tailored approaches are required.
- Cyber-safety cannot be approached in isolation from wider behavioural issues that drive criminality and, therefore, more community-wide responses are required.
- Criminal behaviour is often fluid, flexible and adaptive and the cyber spectrum provides an almost perfect enabler for those characteristics.
- Some Australian children are growing up in a world without a clear demarcation between online (virtual) and offline (real) world; to them, the two seem to symbiotically coexist.
- It is crucial that children and young people using these technologies have the necessary information and skills to make informed decisions online and to become good digital citizens. It is also crucial that parents have an understanding of the risks associated with the technologies and the knowledge to be able to take reasonable steps to reduce that risk.

Responses to Cyber-Safety Threats

Cyber-crime and related efforts on cyber-safety are a high priority for Police Commissioners across Australia and New Zealand. ANZPAA and ANZPAA forums such as the ANZPAA Child Protection Committee (ACPC) and the ANZPAA e-Crime Committee (AeCC) contribute to a multi-faceted set of initiatives aimed at mitigating cyber-crime.

ANZPAA Child Protection Committee

The ACPC is comprised of the Heads of Child Protection from all policing agencies in Australia and New Zealand. Through the collective efforts of the ACPC, Australia and New Zealand law enforcement has established a collaborative relationship that enables joint investigations and the timely sharing of information within Australia and, to the greatest extent possible, with New Zealand.

A primary focus of the ACPC is the protection of children from the more insidious elements of the internet. The online environment has seen the proliferation of CEM, while the popularity and accessibility of social networking sites has become a rich environment for sexual predators to locate and groom children.

As part of its charter, the ACPC is actively developing partnerships with key external stakeholders including telecommunication companies, internet service providers and pioneers in the technological field. It is envisaged that such an approach will engage those that have the greatest capacity to make an impact.

The ACPC is engaged in the following initiatives designed to mitigate cyber-safety threats:

- The utilisation of hash set values as a means of identifying previously seized CEM and to block the further transmission of these images through technological solutions such as the Global File Registry (GFR).
- The standardisation of CEM categorisations and the sharing of hash sets internationally.
- Implementation of the Child Exploitation Tracking System (CETS) and the Australian National Victim Image Library (ANVIL) across all jurisdictions.
- The establishment of information sharing practices and national training packages across the jurisdictions.
- The development of national guidelines for evidence presentation of CEM.
- The development of a framework for content service provider liaison in emergent situations that is agreed and understood by all Australian law enforcement.
- The development of cooperative relationships with relevant stakeholders including internet service providers.

ANZPAA e-Crime Committee

The AeCC plays a central role in the strategic development of e-crime capabilities within law enforcement and as such, is a key player in the national response to cyber-safety. The AeCC is involved in work currently being undertaken by the National Cyber-crime Working Group (NCWG) including:

- Development of national guidelines for digital analysts and technology crime investigators.
- Undertake a scoping study to formally assess law enforcement capabilities across jurisdictions.
- Development of a national cybercrime protocol to enhance information sharing and clarify responsibility for investigation of cyber crime between law enforcement agencies.
- Developing a simple and consistent message for all jurisdictions to assist internet users to prevent cyber crime, and be consulted on a broader draft communications strategy.

National Cyber-crime Working Group

ANZPAA is also a member of the NCWG, a newly appointed body comprising State, Territory and Commonwealth law enforcement agencies, justice departments and Chaired by the Commonwealth Attorney-General's Department. The NCWG has conducted a scoping study of existing domestic and international mechanisms for reporting online crime and prepared a discussion paper on options to improve current reporting arrangements. These options include the creation of a centralised national online reporting facility.

The NCWG has also progressed work on measures to improve coordination and information-sharing in cyber crime investigations, ensure appropriate training for police and judicial officers on electronic evidence and enhance consistency in education and prevention strategies relating to cyber crime.

Opportunities for Cooperation

The borderless environment the internet creates extends beyond the response capacity of a single jurisdiction. Establishing and maintaining stakeholder networks are therefore paramount. ANZPAA's primary role is to facilitate collaboration and cooperation between all agencies both within and beyond law enforcement. In addition to the collegial initiatives outlined above, ANZPAA and law enforcement more generally is contributing to the holistic response to cyber-safety through various cross-jurisdictional and multi-agency forums.

Virtual Global Taskforce (VGT)

The Virtual Global Taskforce (VGT) of which the Australian Federal Police (AFP) is currently the Chair, has demonstrated the value and importance of working collaboratively with other countries in sharing information and breaking down barriers that prevent timely cooperation. The VGT includes police representation from Australia, the US, UK, Italy, Canada Interpol, United Arab Emirates and New Zealand working together to fight online child abuse. Its aim is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse.

Council of Europe Convention on Cyber-Crime

The need for international law to effectively facilitate global co-operation for the investigation of cyber crime offences is urgent. The Council of Europe Convention on Cyber-Crime is the first international treaty on crimes committed via computer networks. Its primary objective is to pursue a common criminal policy aimed at the protection of society against cyber crime, by adopting appropriate legislation and fostering international co-operation.

The Convention requires certain conduct to be criminalised, appropriate powers to be available to law enforcement agencies and the availability of procedures to facilitate information sharing and greater multilateral access to information.

The Cybercrime Convention is not limited to European nations and as such the Federal Attorney-General's Department of Australia has proposed to accede to the Convention. Acceding to the Convention would ensure Australia's laws and arrangements are consistent with international best practice and improve Australia's ability to engage internationally in the fight against cyber-crime. It would also complement the broader policy agenda in the development of a national approach to combat cyber-crime.

United Nations Commission

In April 2011, the United Nations Crime Prevention and Criminal Justice Commission will take place and for the first time an Australian law enforcement officer has been invited to be a keynote speaker. The prominent theme for the twentieth session of the Commission will be "Protecting children in a digital age: the misuse of technology in the abuse and exploitation of children". The Commission will focus on two primary subthemes:

- Nature and scope of the problem of misuse of new technologies in the abuse and exploitation of children.
- Responses to the problem of misuse of new technologies in the abuse and exploitation of children.

Children: A Resource Most Precious Conference

In November 2011, Western Australia Police in conjunction with the Government of Western Australia's Department of Child Protection and Edith Cowan University will host the *Children: A Resource Most Precious Conference.* The Conference has a focus on collaborative prevention strategies, initiatives and programs for minimising harm to children.

Please contact this office if you seek further information on any of the matters mentioned in this submission.

Kind regards

Jon White
Chief Executive Officer