AFP
AUSTRALIAN FEDERAL POLICE

Australian Federal Police
High Tech Crime Operations (HTCO)

Submission to the Joint Committee on Cyber Safety

25 June 2010

Introduction

The key message underpinning the Australian Federal Police (AFP) ThinkUKnow prevention program articulates the primary cyber safety concern – that the Internet and its many and varied applications and platforms offers a veil for a diverse array of criminality. The most insidious of which is the predation of children by adults driven by degrees of sexual motivation.

There are numerous crime prevention, education and awareness programs actively endeavouring to raise awareness of parents, carers, teachers and children. In the context of the change that characterises the online environment, the AFP invite the Committee to consider a number of strategic issues that it and partner agencies are working through to ensure the effectiveness of these programs :

- Most programs tend to be targeted at mainstream audiences; an almost safe harbours approach. This potentially leaves the more vulnerable children at heightened risk and could explain some children unwittingly exposing themselves to significant risk in the face of numerous safety programs and extensive messaging.
    - It may be therefore a fundamental although well founded error to approach cyber safety in isolation without considering the wider spectrum of behavioural issues that are driving the criminality.
- Are Governments, law enforcement agencies and other stakeholder organisations (such as Non Government Organisations (NGO's) and communities more generally making the necessary linkages to the wider suite of anti social behaviours that are impacting on our societies and developing more holistic policy responses?
    - As an example, we are questioning why younger boys and adolescents are so willing to demonstrate a fundamental disrespect for girls in readily encouraging and disseminating inappropriate, often sexualised, images. The issue is wider than technology or the cyber world.
    - Equally as important is to question why young girls and teenagers may deem it as acceptable to take sexualised photos of themselves and to send them using a carriage service. .
- Criminal behaviour is by nature fluid, flexible and adaptive; the cyber spectrum is an almost perfect enabler for those attributes.

Criminality may commence in the cyber world but quickly move to the real world.

i. The online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers);

Some Australian children are growing up in a world without a clear demarcation between online (virtual) and offline (real) world; to them, the two coexist symbiotically.

The Internet and new and evolving technologies open up a world of exciting possibilities and benefits for young Australians. Whilst the Internet and mobile technologies provide many benefits, they also pose some risks.

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 clear that understanding how to navigate the online world safely is an important element in the development of digital literacy. It is important that teachers and parents are able to provide the right advice and assistance to their students and their children, and it is important for education departments and their schools to use appropriate methods to address cyber-safety within their communities.

Understanding how to navigate the online world safely is an important element in the development of digital literacy and a focus of awareness programs that the AFP is involved in. It is as equally important that adults are able to provide the right advice and assistance to children, as it is that education systems use appropriate methods to address cyber-safety within their communities.

We inform parents, carers, teachers and children of the risks and how to manage those risks.. Online risks include bullying, stalking, exposure to inappropriate content, 'grooming' by online sex offenders, sexual solicitation, child pornography, identity theft, fraud, breaches of privacy and online scams.

We believe that there must be a degree of responsibility commensurate with care taken in the real world. It is critical also that all internet users exercise a prudent degree of caution in their transactions, be it social, commercial or mere curiosity. .

It is important to acknowledge that everyone has a responsibility to protect children online and there are many prevention avenues which each stakeholder can take. For example, from a law enforcement perspective, it is vital that information about trends, offenders' modus operandi derived post each operation is linked into current prevention strategies. This ensures prevention and awareness raising campaigns are targeting the vulnerabilities in which online child sex offenders have identified and pursued.

There are numerous prevention and awareness raising campaigns in existence in Australia targeting cyber-safety. The messaging regarding cyber safety is not new; numerous awareness campaigns are in their second or third iterations. For that reason we are questioning whether awareness is reaching across the entire community through all socio economic and culturally and linguistically diverse aspects and therefore reaching the most vulnerable. Few programs have been evaluated for their impact. There is also an absence of evidence-based prevention programs. We are looking at what works in raising awareness and what works in changing behaviour.

Research suggests that in order for there to be changes in behaviour, there needs to be a prolonged period of exposure to the material seeking to change behaviour (Homel & Carroll 2009; Nutbeam 2000; Ajzen 1985)[i]. This also refers to short term behaviour change and long term behaviour change.

Cyber-safety prevention and awareness raising campaigns need to be underpinned by sound research, and longitudinal research. Unfortunately, such research is not completed within a few months, but can take years. That is one of the challenges associated with requiring an evidence based approach to cyber-safety that we are seeking to address.

ii. The nature, prevalence, implications of and level of risk associated with cyber-safety threats, such as:

- **abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);**
- **exposure to illegal and inappropriate content;**
- **inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);**
- **identity theft; and**

- **breaches of privacy;**

The AFP's High Tech Crime Operations (HTCO) portfolio aims to build a highly technical investigative capability for the AFP by anticipating and identifying emerging technology challenges for law enforcement and to develop response strategies for these challenges through engaging with domestic and foreign law enforcement agencies, government, industry, academia and the public.

In collaboration with its Australian and international partners, the AFP, through Child Protection Operations, has a focus on serious and organised crime in the online sexual exploitation of children. During 2009-10, the AFP has successfully identified and charged numerous offenders for child sexual exploitation and child sex tourism offences in accordance with the broader organisational direction.

Internet safety encompasses many areas. Online financial fraud, child exploitation material, malicious software, viruses and identity theft are just some of the issues that the AFP's High Tech Crime Operations teams deal with every day.

Cyber-bullying involves the use of information and communication technologies (ICT) to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others (Bill Belsey, cyberbullying.org).

This form of bullying is often committed using mobile phones or the Internet and includes such activities as:

- Posting hurtful messages on social networking sites.
- Sending repeated unwanted messages either by SMS, instant messaging (IM) or email.
- Excluding someone from an online group.
- Creating fake social networking profiles or websites that are mean and hurtful.

An act of cyber-stalking is defined as when a person stalks another person by publishing on the internet or by an email or other electronic communication to any person, a statement or other material with the intention of causing physical or mental harm to the victim, or of arousing apprehension or fear in the victim for their own safety.

Legislation does not specifically refer to cyber-stalking. There are however, telecommunications offences in the *Criminal Code 1995* dealing with threats and menacing, harassing or offensive behaviour conducted online (see sections 474.15 and 474.17). Additionally, state/territory legislation covers stalking, for example section 35 of the *Crimes Act 1900* (ACT). There are many other offences that may also cover 'stalking' type behaviour such as offensive behaviour, and assault.

There is no distinct offence of cyber-bullying. Depending on the circumstances of the incident, in serious cases of cyber-bullying, where there is a specific threat to the physical safety and well-being of a young person, state and territory laws relating to threatening and harassing behaviour might be used. However, there is a reluctance of law enforcement to use this legislation, as there are more appropriate avenues for responding to this behaviour.

The death of Nona Belomesoff on 14 May 2010, who apparently met the man charged with her murder through social networking sites Facebook and Bebo, is a shocking reminder of the importance of internet safety.

Additionally, it is of grave concern that people would use social networking sites to post inappropriate material on the internet, particularly in such tragic circumstances as the deaths of Trinity Bates and Elliot Fletcher, where memorial sites in their honour were defaced.

The AFP has forged relationships with Content Service Providers (CSPs) such as Facebook, and will continue to work with CSPs into the future to tackle the growing prevalence of threats to internet safety.

However a balance needs to be reached between the overall purposes of social networking sites – that is, the sharing of information - and the privacy of the users. Privacy settings need to be simple to follow and users need to understand exactly what information they are allowing strangers to view about themselves.

For example, in response to growing criticism over its privacy controls, Facebook has announced an overhaul of its privacy settings which will be rolled out in mid 2010. Some of the major changes include simplified controls for who users share content with.

Users need to familiarise themselves with the changes and exercise caution before selecting the 'Recommended' privacy settings by Facebook. This option spreads out the sharing of content across the three groups of 'Everyone', 'Friends of Friends' and 'Friends Only'. Under this option, users status updates, posts and relationship status are made available to Everyone and users photos, videos and birthday are made available to 'Friends of Friends'. This means that this significant amount of personal information is shared with strangers.

Another identified vulnerability in terms of risks posed to young people is the fact that there is no age verification on social networking sites. Whilst most social networking profiles set the minimum age of thirteen years to set up a profile, it is common knowledge that children are lying about their age, and setting up profiles pretending to be older than who they are. The opposite is also prevalent with older people purporting to be younger to engage with young people online. This may make young people more vulnerable to fall victim to online child sex offenders.

When it comes to removing offensive or illegal online content, the AFP works with the Australian Communications and Media Authority (ACMA). Where the posting of the online content amounts to an alleged serious criminal offence, the AFP assesses the information on a case by case basis and decides whether an investigation should be commenced.

The ACMA is the primary agency for removing online content (where that content is prohibited under the *Broadcasting Services Act 1992*). The ACMA responds to community concerns about offensive and illegal material online by administering a national regulatory scheme that includes the investigation of complaints about prohibited online content.

If content is hosted in, or provided from Australia and is prohibited, or is likely to be prohibited, the ACMA will direct the CSP to remove or prevent access to the content from their service. If the website is hosted offshore, the AFP and ACMA are limited in what they can do.

Technology reliance, combined with the reach and speed of the internet, allows criminal elements to operate from international regions with limited regulation or legislation. In this environment, the sharing of information internationally between industry, private sector, government and third-party organisations in an open and timely manner enables law enforcement to protect the community and develop safe strategies against technology enabled crimes.

Child sexual exploitation can involve possession, making and distributing child pornography, online enticement of children for sexual acts, child prostitution, child sex tourism and child sex molestation. Every image of child sexual abuse is a crime and reflects the abuse that child received.

Child sexual exploitation and abuse is not just a law enforcement issue. The victims are children, including Australian children, and the challenges posed and solutions required need to be shared by everyone. The nature of the exploitation and abuse defies human logic and reasoning and affronts our values and norms. Sophisticated and caring communities simply cannot tolerate such exploitation and abuse. Hence the need for a holistic approach to policy making and delivery.

The evolution of technology including encryption and converging technologies present challenges for law enforcement. Similarly, the volume of data and its retention by Internet Service Providers (ISPs) for potential use as evidence in police investigations also presents challenges in this environment.

The AFP has fostered working relationships with a number of industry partners to overcome some of the technological challenges that currently face law enforcement in this area. We also work very closely with Australian government agencies in relation to policy development and legislative reform to address the numerous challenges emerging in this environment.

The National Broadband Network (NBN) is a case in point. The AFP with other Australian Govenrment agencies is working to minimise the criminal exploitation of the NBN. The inherent risk of the NBN is that it could facilitate the continual growth and sophistication of online criminal syndicates' ability to commit cyber offences against online systems due to the attractiveness of the increased speed. Increased bandwidth available via the NBN may result in increased bandwidth available for committing or facilitating computer offences.

The NBN will likely create an environment in which relatively small Retail Service Providers (RSPs) operate offering a range of services including voice, data and media, internet TV, social networking, music, video messaging, games, text, email and internet browsing. Unless smaller RSP's are required to comply with the same 'licensing' arrangements as other 'carriage service providers' as defined by the *Telecommunications Interceptions Act 1979*, it is likely that many RSPs will have limited capacity to assist law enforcement (due to limited size or technical capabilities).

The proliferation of a large number of RSPs has the potential to increase the difficulty law enforcement has to obtain telecommunications data. Australian government agencies are in consultation with NBN Co to address this particular issue.

Identity Theft

Identity theft associated with the compromise of personal information in the online environment is a current and ongoing threat. Risks of compromising identity are the same across all age ranges. The use of a computer by one person who inadvertently downloads malicious software onto the computer will have an impact on every other user of that computer. Malicious software downloaded onto a computer can now also be used to remotely access files, webcam or microphone on the compromised computer.

There should be an onus on online users to protect their personal information.

Data compromised in the online environment may include personal financial information, other personal information such as emails, identity data and photographs. Young person's details may be used to identify their parents or adult contacts and be subsequently used to attempt to give legitimacy to communications designed to compromise the adults computers or obtain personal and financial details.

The 2007 Australian Personal Fraud survey, undertaken by the Australian Bureau of Statistics indicated that the impact of online identity theft in the previous twelve months equated to approximately $970 million. The impact of identity theft in 2010 is expected to be significantly higher than the 2007 estimates.

iii. Australian and international responses to current cyber-safety threats (education, filtering, regulation and enforcement) their effectiveness and costs to stakeholders, including business;

Cyber-Safety Initiative

The Government's Cyber-Safety initiative is part of a whole-of-government initiative involving the Department of Broadband, Communication and the Digital Economy (DBCDE), The ACMA, the Commonwealth Director of Public Prosecutions and the AFP. The Cyber-Safety initiative is a continuation of the former Government's 'Protecting Australian Families Online' initiative implemented in 2007-2008. Funding for the Cyber-Safety initiative is $49 million over four years (2009-2012).

The role of the AFP is to:

- Target and investigate technology crime including child pornography and paedophile behaviour in the online environment;
- Provide a police presence in social networking sites; and
- Contribute to broader prevention strategies such as educational campaigns.

Specific AFP objectives are to enhance the AFP's contribution to combating technology crime impacting Australian families by:

- Proactively targeting the production and distribution of online child sex exploitation images;
- Creating a hostile environment on the internet for online offenders through the development of proactive and innovative methods of informing potential offenders of the risks involved in their activity;
- Increasing research into the evolving digital landscape and emerging threats to better predict trends and capabilities and develop proactive targeting, prevention and disruption strategies for online crimes, especially those involving child victims;
- Promoting community awareness through active liaison with government and non-government organisations such as educational agencies and community groups;
- Developing and implementing an Australian National Victim Image Library (ANVIL); and
- Developing and implementing a training and welfare strategy to deal with identified risks associated with teams working within the online child sex exploitation arena.

The AFP is responsible for the development and implementation of a covert capacity to proactively identify, target and investigate online predators including:

- The purchase of software similar to that used by offenders;
- The purchase of evidence collection software;
- The implementation and maintenance of a *covert* and an *overt* police presence on the internet;
- The purchase of non-government specification hardware from non-government suppliers;
- Online presence including warnings in chat rooms relating to potential predatory behaviour, utilising the Virtual Global Taskforce (VGT) as appropriate; and

- Deterrence initiatives such as redirection of all ‘take down’ sites to warning sites. This will require the development, implementation and installation of necessary software.

Examples of Operational Activity

The AFP HTCO investigative capacity focuses on high risk organised, networked and/or commercially orientated on line sexual exploitation of children and child sex tourism. The AFP has now moved toward the upper level offending and focus on disrupting the source of the material whilst the states and territories build capacity and capability in policing their digital citizens consistent with how they police their real world communities. To that end, the AFP suggest that cyber safety now needs to be considered in the context of overarching policing strategies, particularly those targeted at anti social behaviours.

Incumbent in this refined direction is some degree of move from quantitative to qualitative analysis. Complex investigations into multi jurisdictional criminality are resource intensive.

The AFP value sustainable and positive relationships with our national and international partner agencies. This extends from the initial referral and evaluation processes to intelligence collection and sharing and investigation. Through those processes the AFP has an impressive record of operational outcomes, including:

- Operation Centurion commenced in mid 2008 and was one of the largest investigations ever conducted into online child abuse with 141 people arrested nationally. The technology the offenders used is a peer to peer (P2P) application which allows internet users to share files without accessing a central network server, making it more difficult for content to be monitored by ISP filters and shutting out those not invited into the network. This application is a common way for transferring child sexual exploitation material. The operation was triggered after a legitimate European website was hacked into and 99 degrading and explicit images were placed on it;

- Operation Resistance commenced in December 2007 with a referral from Brazil’s Departamento de Polícia Federal (DPF) via Interpol that led to twenty-four people charged nationally for downloading and sharing child abuse material. This operation saw more than 15,000 videos and 500,000 images of child abuse seized;

- Operation Glatton is a current investigation into offenders using a popular P2P application. To date there have been seventeen arrests;

- Operation Kickshaw was a covert online operation involving a globally-networked group of offenders trading child exploitation material. The operation stared with the arrest of a United States (US) offender based on AFP information and further proactive investigations in conjunction with overseas partners resulted in thirty-four further arrests in Australia, the US, United Kingdom (UK) and Europe. Operation Kickshaw illustrates the covert operations the AFP conduct on a daily basis on the Internet. The AFP identify offenders using the Internet to network and trade child exploitation material and who are committing sexual assault or sexual exploitation offences against children;

- The AFP provided assistance to the Royal Thai Police (RTP) investigation into the activities of child sex offenders in Pattaya, Thailand. The RTP sought the assistance of the UK, Child Exploitation and Online Protection Centre and the AFP Child Protection Operations Team. The multi-agency investigation, led by the RTP and supported by the AFP, resulted in a dual Australian-United Kingdom citizen being arrested in Pattaya in March 2009. This operation also identified over thirty known and suspected Australian national child sex offenders with connections to Pattaya, Thailand; and

- Operation Ramillies is a Child Protection referral from Europe to the AFP in which 1,768 unique Australia based IP addresses were identified. An IP address is a unique identifier, assigned to a computer while connected to the Internet, and on this matter to date, 726 suspects have been identified. This example highlights a number of issues:
    - The volume of offending generated through technology ;
    - The need for international, state and territory law enforcement to develop the best response strategy (in this case to identify and protect any children at risk);
    - The specialist skills needed by police (and technicians) to investigate and to provide expert evidence to courts through computer forensics;
    - Understanding that industry are key players in this new environment;
    - The existence of a complicated legal framework to obtain evidence for court to prosecute offenders; and
    - The ability to successfully educate and develop crime prevention strategies to empower the community to have safe and secure experiences in using technology.

Legislation

Since the early 1990's the Commonwealth has pursued a range of legislative and regulatory initiatives to enhance cyber-safety.

The Commonwealth has enacted offences for the misuse of computers and telecommunications systems in the *Criminal Code Act 1995* and created specific offence regimes to address the online sexual abuse of children in the *Criminal Code Act 1995* and spam communications in the *Spam Act 2003*.

Commonwealth law enforcement have been given specific powers for the examination and seizure of computers under the *Crimes Act 1914* search warrant powers including the ability to move a computer off-site for examination, compel the provision of passwords and access data held at another premises via the on-site computer. In addition to more traditional investigative methods Commonwealth legislation enables cybercrime investigators to access telecommunication interception under the *Telecommunications (Interception and Access) Act 1979*, surveillance devices under the *Surveillance Devices Act 2004* and controlled operations incorporating undercover operatives under the *Crimes Act 1914*.

The Commonwealth regulates Internet content through the national classification scheme and the *Broadcasting Services Act 1992*. Internet content that is deemed 'prohibited content' can be added to the Designated Notification Service, colloquially known as the black list. In addition, law enforcement may request carriage service providers to block access to sites suspected of being used to commit offences against Australian law under the *Telecommunications Act 1997*.

The Commonwealth legal and regulatory framework is under constant review. Law reform in this area presents a number of challenges due to the rapidly changing digital environment and the transnational and highly adaptable nature of online criminality.

Online crime is borderless and evidence can be transitory, highly perishable and located overseas. 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 to underpin the strong working relationships the AFP has developed with overseas partners. The current scheme provided by the *Mutual Assistance in Criminal Matters Act 1987* (MACMA) can be cumbersome and is not suited to the online environment. MACMA is currently under review by the Attorney-General's Department. The AFP is engaged in the review process and supports reforms that streamline the MACMA process.

The Attorney-General also recently announced Australia's intention to accede to the Council of Europe Convention on Cybercrime. The convention provides benefits to law enforcement and contains procedures to make investigations more efficient and provides systems to facilitate international co-operation, including:

- helping authorities from one country to collect data in another country;
- empowering authorities to request the disclosure of specific computer data;
- allowing authorities to collect or record traffic data in real-time;
- establishing a 24/7 network to provide immediate help to investigators; and
- facilitating extradition and the exchange of information.

However, the Convention is not a quick solution to a difficult problem to the issue of international evidence and criminal intelligence sharing. As the cyber criminal environment operates in a very fluid and rapidly changing environment more work needs to be done on ensuring that international law enforcement has the ability to quickly exchange evidence and intelligence in a timely fashion.

The AFP works closely with government departments, particularly the Attorney-General’s Department to ensure the Commonwealth legal framework remains robust. An example is the ***Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010*** (the Act) which effectively bridged the perceived gap between online sexual exploitation and child sex tourism.

In summary, the Act:

- introduces new offences for dealing in child pornography and child abuse materials overseas, as well as for using a postal service for child sex-related activity;

- recognises the growing convergence between online crimes against children and child sex tourism, and also the link between online offenders and contact offenders;

- strengthens the existing child sex tourism offence regime, and enhances the coverage of offences for using a carriage service for sexual activity with a child or for child pornography or abuse material; and

- allows for materials to be forfeited to the Commonwealth. This is critical to ensuring effective policing in the online environment. The scheme will build community confidence that the AFP will deal decisively and effectively with hardware that contains child exploitation materials.

In terms of how the legislation affects the AFP, the Act:

- will strengthen the AFP's ability to investigate and prosecute Australians who offend against children off-shore, while working to build the capacity of local agencies;

- will improve the operation of existing offences and increase the AFP's ability to successfully prosecute these matters, including the creation of a new legislation presumption for all carriage service offences; and

- will enable the AFP to adjust its business structures and processes, upskill its investigators, intelligence and support resources to consider sexual offences against children more holistically.

Of note is the introduction of a new forfeiture scheme which will significantly improve the AFP's capacity to deal with seized child pornography and child abuse materials.

In Australia, responsibility for enacting and enforcing child sex offences is shared between the Commonwealth and the states and territories. The states and territories have criminalised conduct occurring domestically, while the Commonwealth has criminalised conduct occurring across Australian jurisdictions (eg using the Internet) or outside Australia (eg child sex tourism). Table 1 sets out an overview of Australia's laws criminalising child sexual exploitation, and the relevant jurisdiction responsible.

Table 1 – Overview of Australia's child sexual exploitation laws

Conduct	Jurisdiction
Child pornography offences	
Possession, production, distribution*	States and territories
Using the Internet	Commonwealth
Child sex offences	
Sexual intercourse/other sexual conduct*	States and territories
Procuring/grooming*	States and territories
Exposure to indecent material*	States and territories
Child prostitution*	States and territories
Child sex tourism**	Commonwealth

Internet procuring and grooming	Commonwealth

* Applying domestically ** Applying extraterritorially

The Commonwealth has enacted the following criminal laws directed at the sexual exploitation of children:

- child pornography and child abuse material offences involving the use of a carriage service (such as the Internet or mobile phone) – carrying maximum penalties of ten years imprisonment; and
- offences for using a carriage service for grooming or procuring children – carrying maximum penalties of up to fifteen years imprisonment.

Australia's child sex tourism offence regime is now articulated in Division 272 of the *Criminal Code Act 1995 (Cth),* including:

- Section 272.8(1) - Engages in Sexual Intercourse with Child outside Australia - Penalty has increased from seventeen years to twenty years imprisonment.

- Section 272.8(2) - Causing Child to engage in Sexual Intercourse in presence of Defendant - Penalty has increased from seventeen years to twenty years.

- Section 272.9(1) - Engage in Sexual Activity with Child outside Australia - Penalty has increased from twelve years to fifteen years.

- Section 272.9(2) - Causing Child to engage in Sexual Activity in presence of the Defendant - Penalty has increased from twelve to fifteen years.

iv. opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues;

Engagement and cooperation remains a strong focus for all law enforcement agencies.

The AFP works closely with law enforcement agencies, government agencies, industry and NGOs to help keep young people safe online. This includes CSP, banks, education agencies and community groups as community education remains one of the most important elements of crime prevention.

The AFP has enhanced strategic alliances within the Australia and New Zealand Police Advisory Agency Child Protection Committee (ANZPAA CPC) to combat online child sex exploitation.

The AFP has also developed a regional capacity through joint investigations and learning events at the Jakarta Centre for Law Enforcement Cooperation located in Semarang, Indonesia.

In October 2009, the AFP hosted an inaugural child sex tourism symposium in Melbourne with representation from across law enforcement, government and NGOs to better consolidate a strategic approach to child sex tourism.

In February 2010, the AFP deployed members to the Association of Southeast Asian Nations region to enhance criminal intelligence about Australian residents and occupants who sexually offend against children.

The AFP, through its international network, is able to facilitate enquiries offshore. However, in the current dynamic environment, investigation and evidence collection still remains difficult. It is for these reasons that relationships with the private sector are crucial in ensuring law enforcement maintains an effective capability to combat technology enabled crime.

Virtual Global Taskforce (VGT)

In December 2009, the AFP officially assumed the position of Chair of the VGT. The VGT includes representation from Australia, the US, UK, Italy, Canada Interpol, United Arab Emirates and New Zealand. This is a significant appointment for the AFP which will serve to further strengthen Australia’s law enforcement efforts in globally combating child exploitation online.

The VGT is made up of police forces from around the world 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. The objectives of the VGT are to make the internet a safer place, to identify, locate and help children at risk, and to hold perpetrators appropriately to account.

The AFP, in conjunction with the VGT will host the 4th biennial VGT Conference on 2-3 December 2010 in Sydney. The AFP and the global VGT membership look forward to facilitating this event, which will bring a range of international stakeholders together to address child safety in the online environment.

The AFP attends key international fora to promote investigation best practice and address emerging technology issues, including:

- The Interpol Specialist Groups Crimes Against Children Workshop;

- The Annual Dallas Crimes Against Children Conference held in Texas — the pre-eminent US event relating to issues concerning the physical and online abuse of children and the international trafficking of children. Participants include law enforcement counterparts from US and Canadian Federal and local agencies as well as representatives from key NGO's and private industry.

- The Annual US Internet Crimes Against Children National Conference — this conference is restricted to law enforcement investigators and prosecutors who manage Internet Crimes Against Children related cases.

- The AFP is a member of the National Cyber Security Awareness Week (NCSAW) Steering Group. NCSAW (6 June – 11 June 2010) is an initiative led by DBCDE in partnership with other Australian Government Departments, state and territory governments and many leading business, industry and community organisations.

- The AFP participates in the Consultative Working Group (CWG) on Cyber-safety that provides advice to Government on priorities for action. The CWG is made up of experts from industry, community organisations and Government.

- The AFP hosts the annual Australian High Tech Crime Conference bringing together leading academics, government representatives, law enforcement, members of the judiciary and industry to discuss emerging technology crime issues, building knowledge and experiences.

- The AFP will continue to work closely with industry, Government and local and international law enforcement agencies to protect children online through education and by targeting online sex offenders.

Content Service Providers (including Facebook)

The AFP has made significant contact with Facebook on behalf of the Australian law enforcement community in attempting to find a resolution to enforcement issues highlighted in recent media reporting.

The AFP's High Tech Crime Operations continues to work in partnership with CSP's including Facebook, who are receptive to approaches from law enforcement agencies. The development of relationships with CSP's is crucial to the AFP's ability to investigate and combat crime in this increasingly complex and dynamic environment.

Legal mechanisms for compelling CSP's to remove content are limited, and are unlikely to succeed due to the costly and lengthy process involved. Even where a legal remedy was successful, it would likely be detrimental to the AFP's future relationships with that CSP where assistance of an even more critical nature is required. (for example: Cloud Computing - as Google hosts more and more information, the AFP will need its consent to obtain specific types of data in a timely manner).

The awareness of the limitations as to what content can and cannot be removed from sites such as Facebook is paramount. The content has to be considered prohibited or illegal as determined under regulation through the *Broadcast Services Act 1992* or through various state and Commonwealth legislation. Facebook want to protect its members from illegal content but retain its commercial advantage through member privacy and self regulation. Importantly, material hosted in the US is not bound by Australian statute and as such there is no legislative basis for enforcing compliance.

The development of a framework for CSP liaison in emergent situations that is agreed and understood by all Australian law enforcement is essential. AFP Commissioner Negus recently proposed that the current Child Protection Committee convene to consider a process that will work for all agencies, including the development of relevant documentation and terms of reference.

The development of the aforementioned framework will be a positive move forward to ensure a consolidated, collaborative approach for engaging with CSPs in the future.

The AFP's primary concern is to ensure that all social networking sites maintain the privacy and safety of Australian users.

The AFP urges Facebook to have in place a prominent report abuse button on each profile page, better privacy settings and a dedicated law enforcement liaison presence in Australia to efficiently and effectively deal with requests for assistance.

The ability to work closely with other law enforcement agencies, domestically and internationally, industry, academia and the community is critical to ensuring capabilities and capacity of police is enhanced. By sharing information and intelligence, expertise and specialist skills and by building solid training programs in support of law enforcement efforts, many challenges can be met.

v. examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised;

The very existence of HTCO is testimony to the commitment of Australian law enforcement to maximising the potential of technology within the law enforcement spectrum. The coalescing of nearly all technologically focused policing aspects under 'one roof' was innovative and certainly set best practice levels.

In conjunction with the AFP Information Communications Technology area, HTCO has an ongoing scanning capability complimented by its emphasis on industry and academic relationships and partnerships. That collective force has the ability to forecast what is over the horizon and take necessary steps to be in a position to respond.

An example is the ANVIL project. The project has two objectives; firstly to more efficiently identify and rescue children who are the subject of online sexual exploitation, and the second to minimise police employee exposure to exploitation material (both image and video).

These objectives will be met through a platform known as CETS; the Child Exploitation Tracking System, developed by Microsoft through ongoing collaboration with international law enforcement.

ANVIL is a truly national project, hosted by CrimTrac and governed by the ANZPAA Child Protection Committee.

vi. ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying including by:

- **increasing awareness of cyber-safety good practice;**
- **encouraging schools to work with the broader school community, especially parents, to develop consistent, whole school approaches; and**

- **analysing best practice approaches to training and professional development programs and resources that are available to enable school staff to effectively respond to cyber-bullying;**

There are a broad spectrum of prevention programs through both Government and non government agencies. The cyber safety 'space' has the potential to become quite congested. At this stage, few if any of the programs have been evaluated in a longitudinal perspective; that is, it is difficult to make an authoritative assessment of the extent of achieved behavioural change. The AFP believes such analysis should inform future policy and program development. This type of assessment needs to be a priority. As will be indicated below however, the community cannot stop and wait for such findings to be delivered; the awareness raising must continue although an enhanced level of coordination is desirable.

It is also desirable that cyber safety prevention and awareness policy also be cognisant of wider social disjoints. We should question why young people, particularly males, are so willing to take or encourage young women to pose for or in fact make inappropriate images or videos, only to disseminate that material via mobile telephone, e-mail, peer to peer platforms or other technological means. There appear to be linkages to deterioration of basic societal norms including respect and sanctity of relationships.

The AFP's HTCO portfolio has been innovative in Australian policing by establishing a Team dedicated specifically to address cyber safety and security. The aim of the Team is to implement crime prevention strategies which seek to raise awareness and empower Australians to protect themselves online.

ThinkUKnow

Based on a proven (as in evaluated) program in the United Kingdom, and utilising the relationship which the AFP has through the VGT, the AFP localised for piloting in Australia, the UK's Child Exploitation and Online Protection (CEOP) Centre's ThinkUKnow cyber-safety program.

In Term 1 2009 the AFP, in conjunction with Microsoft Australia and the ACMA, piloted ThinkUKnow in three states in Australia, the Australian Capital Territory (ACT), New South Wales (NSW) and Victoria (VIC).

As part of the pilot the AFP and Microsoft volunteers delivered forty-six ThinkUKnow presentations in the ACT, NSW and VIC. Over 2,100 parents, carers and teachers were educated on how to keep young people safe online.

The pilot was evaluated by the Australian National University. Results from the evaluation indicated that - following attendance at a ThinkUKnow presentation – eighty-eight percent of parents, carers and teachers felt they better understood how children are using technology.

Furthermore, ninety-six percent found they better understood the safety issues associated with its use, and ninety-one percent reported they were motivated to take action on improving cyber security at home.

Based on the successful pilot of the ThinkUKnow Australia initiative in 2009, the national roll out continued in Term One, 2010, and was officially launched in Queensland on 19 February 2010 by the Minister for Home Affairs, the Hon Brendan O'Connor MP.

ThinkUKnow Australia aims to educate parents, carers and teachers about the risks faced online and how to create a safe online experience for young people.

Through initiatives such as ThinkUKnow, the AFP works with the private sector to educate the Australian public on how to conduct themselves safely online. Initiatives such as this are essential to combat crime in this increasingly complex and dynamic environment.

Young people need to be able to recognise inappropriate or suspicious behaviour online and parents need to be aware of what their children are doing online.

Personal information should not be posted or shared over the Internet. Young people need to be aware of what messages they are sending out about themselves and should only accept online friend requests from friends they know in real life.

It is hoped that by providing parents, carers and teachers with the knowledge and skills on cyber-safety and security, we can protect our children from the rise in technology crime, particularly those focused on exploiting or harming children.

ThinkUKnow involves presentations delivered by trained volunteers and a comprehensive website which provides additional information and resources.

The three themes of 'Have Fun', 'Stay in Control', and 'Report' form the focus of ThinkUKnow, both in the face-to-face sessions and the website.

ThinkUKnow aims to open the lines of communication between parents and children so that the Internet is as much a topic of discussion as what happened at school that day.

We know that young people will not tell their parents if something makes them feel uncomfortable online, for fear of having their Internet privileges confiscated.

By helping start a dialogue between parents and children, we hope that young people will be more confident going to their parents when they have a problem, and that their parents will better understand how to deal with these issues.

The ThinkUKnow program also advises Australians on where to report when something goes wrong online, affirming that there is an online policing presence.

The program also includes a YouTube channel that hosts a range of internet safety videos promoting the work of ThinkUKnow, as well as educational information to assist in preventing online child abuse.

Youth Education Program

In addition to educating parents, carers and teachers, HTCO’s Crime Prevention Team also embarks on a program of cyber-safety awareness amongst children and young people through attendance at schools in the ACT, regional NSW and VIC to deliver presentations.

The youth education program is designed to make young people think of the possible consequences of the things they do online. For example, many teenagers don't realise that once something is published on the Internet it can never be permanently deleted and may cause problems for them in the future.

The presentations are also backed up through the provision of Fact Sheets which are made available in hard copy and on the AFP website.

The program also makes young people aware of the need to protect their image and reputation by being careful of who they communicate with, and how they communicate. The Team has also delivered a series of ‘Protecting your reputation’ sessions to young sports players, including to Tennis Australia and the Toyota Cup National Rugby League rookie players.

Cyber-safety is not only about protecting children and young people. Senior computer users are also at risk online, and as a result the AFP has also partnered with the Australian Senior Computer Clubs Association to deliver sessions to senior users on how they can protect their personal and financial information, secure online banking and securing their wireless connections.

The AFP participates on a yearly basis in National Cyber Security Awareness Week, and in 2010, was involved in over fifteen different awareness raising activities with a number of other stakeholders. This demonstrates the importance of working together to achieve a safe online experience for all.

The AFP has a commitment to preventing online crime and education is an important part of that commitment. Australians need to take some responsibility for their online experiences, as they do in the offline environment. This should ensure they are better equipped and empowered to enjoy their cyber experience. Cyber-safety requires a multi-faceted approach; law enforcement; policy and legislation; education and some level of user vigilance.

vii. analysing information on achieving and continuing world's best practice safeguards;

The AFP promotes the following safeguards to children, parents and carers to ensure best practice protection online:

- Install security software and update it regularly;
- Turn on automatic updates so that all your software receives the latest fixes;
- Get a stronger password and change it at least twice a year;
- Stop and think before you click on links or attachments;
- Stop and think before you share any personal or financial information - about yourself, your friends or family;
- Know what your children are doing online. Make sure they know how to stay safe and encourage them to report anything suspicious; and
- Visit www.staysmartonline.gov.au for further advice and information.

Other cyber safety related safeguard messages promoted by the AFP include:

- Don't believe everything you read – make sure you know its coming from a reliable source;

- Don’t provide any private information about you, your family, friends or other people you know over the Internet;
- Make sure your social networking profile is set to private;
- Only accept friend requests from people you know – even if it is a friend of a friend it is not a good idea to add them as friends unless you know them personally;
- Tell your friends to ask for your permission before uploading and/or tagging photo’s of you on social networking profiles; and
- If you ever see content online that is inappropriate or upsetting, tell someone you trust and contact your local ISP and law enforcement agency.

viii. the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues;

The AFP does not see a demonstrated need for a further reporting point or investigative structure dedicated solely to cyber safety.

Rather the need is to consider an enhanced coordination, longer term evaluation and policy synergies of existing or proposed cyber safety programs.

[i] Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action-control: From cognition to behavior* (pp. 11-39). Heidelberg, Germany: Springer.

Homel, P & Carroll, T. (2009). Moving knowledge into action: applying social marketing principles to crime prevention. *Trends and Issues in Crime and Criminal Justice*. No. 381. Australian Institute of Criminology: Canberra.

Nutbeam, D. (2000) Health literacy as a public health goal: a challenge for contemporary health education and communication strategies into the 21st Century. *Health Promotion International*, 15, 259–267.