Australian Federal Police
To fight crime together and win

SENATE LEGAL AND CONSTITUTIONAL COMMITTEE

Inquiry into the provisions of the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004

Introduction

The Australian Federal Police (AFP) welcomes the inquiry by the Senate Legal and Constitutional Legislation Committee (the Committee) into the provisions of the *Crimes Legislation Amendment* (*Telecommunications Offences and Other Measures) Bill 2004* (the Bill).

Aim of this Submission

The AFP submission supports all the provisions of the Bill, however this submission only focuses on the proposed amendments to telecommunications offences.

Role of the Australian Federal Police

The AFP is the major instrument of Commonwealth law enforcement and the chief source of advice to the Commonwealth Government on policing issues. Its role is to enforce Commonwealth criminal law and protect Commonwealth and national interests from crime in Australia and overseas. The AFP is also Australia's international law enforcement and policing representative.

The AFP maintains a very strong focus on fighting transnational crime. The Committee would be aware that the AFP has an important role in investigating serious offences, including sex offences against children and offences which are facilitated through the use of a telecommunications service.

The AFP appreciates the opportunity to comment on the Bill.

Telecommunications Offences

One of the key outcomes of the Bill will be to introduce new telecommunications offences in the *Criminal Code,* which will replace outdated offences in the *Crimes Act 1914.* The proposed new offences and amendments are essential if the AFP is to continue fighting contemporary criminal activity in the face of new and emerging technological developments.

Of particular note are the proposed provisions which will:
- introduce offences for using the internet to groom and procure children under 16 for sexual activities;
- create offences to use a telecommunications service to produce, distribute and collect child abuse and child pornography material;
- create offences for rebirthing of mobile phones and other communication devices (altering an IMEI) and for cloning mobile phone SIM cards; and
- introduce the offence of using a telecommunications service to commit a serious offence.

Grooming and Procuring, Child Abuse Material and Child Pornography Material

The production, distribution and collection of child pornography is known to be only one aspect of child sex offending. It is imperative to recognise that children have been abused during the production of the material, and furthermore, the abuse of those children continues every time the material is viewed.

The Internet has provided child sex offenders with a means to not only trade in such material, but more importantly, to abuse children. The Internet (for example, chat channels) provides offenders with a vehicle to access children, to identify potential victims, to "groom" them, and then to arrange for committing offences against children in the physical world.

The Internet has also provided a means for child sex offenders to form support and offender networks, or 'clubs', and to exchange information.

Commonwealth response

Where there have been obvious deficiencies in the legislative environment the Commonwealth has acted to ensure the appropriate criminalisation of acts that society finds harmful. The amendments to the *Criminal Code Act 1995* as described by the *Cybercrime Act 2001* have demonstrated the Commonwealth's willingness to intervene where required.

In response to this need, Police Ministers and Commissioners agreed in 2003 to the establishment of the Australian High Tech Crime Centre (AHTCC). The AHTCC, hosted by the AFP, brings together police representatives from all Australian Police jurisdictions in a joint effort to combat high-tech crime. By its very nature, the AHTCC is a national focal point for coordination and expertise in all matters involving technology and serious criminal offending. Furthermore, the AHTCC enhances AFP international relationships as it partners with comparable foreign high-tech crime centres to combat the global aspects and challenges of this crime type.

In the current legislative environment, the AHTCC effectively investigates various types of computer and networked based offending such as hacking, denial of service, and malicious software as expressed in the *Cybercrime Act 2001*.

The AHTCC takes a leading role in combating online child sex abuse. However, without effective legislation that targets the most serious aspect of Internet child pornography - the actual assault and abuse of the child – the AHTCC is hampered in its efforts to combat what is clearly serious criminality involving technology.

Given the borderless nature of the Internet, cross jurisdictional issues in relation to online child sexual abuse are inevitable. It follows that effective outcomes will only be achieved through nationally consistent legislation.

It is on these bases that the AFP strongly supports the proposed offences and their related provisions that:

- will outlaw using a carriage service for child pornography, child abuse material or to groom or procure a person under 16 years age for sexual activity;
- will outlaw possessing, controlling, producing, supplying or obtaining child pornography or child abuse material for use through a carriage service;
- places a positive obligation on Internet Service Providers and Internet Content Hosts to refer known services dealing in child abuse or child pornography material to the AFP; and,
- will authorise the officers of the AHTCC and other relevant law enforcement personnel to lawfully conduct necessary covert operational activities to bring offenders to justice.

Law enforcement powers

Given the seriousness of the proposed child sex offences, the AFP welcomes the consequential amendments to the *Telecommunications (Interception) Act 1979* and to section 15HB of the *Crimes Act 1914* which will provide law enforcement officers with capacity to obtain telecommunications interception warrants and controlled operations authorities when investigating offences proposed under the Bill.

Rebirthing of mobile telephones and SIM cloning

The AFP supports the proposed offences and the related provisions that prohibit the 'rebirthing' (modification of a telecommunications device identifier) of mobile phones and the copying of mobile phone SIM cards (copying an account identifier), as well as possessing, producing, supplying or obtaining a device or data with intent to 'rebirth' a mobile phone or copy a SIM card.

A law enforcement exception has been necessarily included in these provisions. This will allow law enforcement to forensically examine mobile telephones and SIM cards for data recovery purposes without breaching the provision.

Using a telecommunications network with intention to commit a serious offence

The creation of an offence for using a telecommunications network to commit a serious Commonwealth, State, Territory or foreign offence is a positive step to effectively and efficiently deal with crime across jurisdictions. Telecommunications have enabled people to commit crimes in jurisdictions where they are not physically present, the investigation of which would ordinarily be complex given differences in the law between jurisdictions, both procedural and in offences themselves.

In particular recognition of the complexity of fraud offences, and the proliferation of fraud facilitated through the Internet, the AFP welcomes the inclusion of proposed section 474.14 in the Criminal Code which will make an offence of using a telecommunications network to commit such fraud.

Recent money laundering amendments were introduced under the *Proceeds of Crime Act 2002* in recognition of the investigatory and prosecutorial difficulties associated with proving a predicate offence. This is particularly so with complex fraud matters where it is often difficult to establish what offence and what geographical limitations may apply.

United States legislation was considered an appropriate model. Section 1343 of Title 18 of the United States Code makes it an offence (punishable by a maximum term of 5 years imprisonment) to use a telecommunications network to commit a fraud of any kind.

Conclusion

The AFP supports all the provisions of this Bill and acknowledges the importance of the measures that will be implemented. The AFP also acknowledges the excellent consultation that has occurred with major stakeholders, including the AFP, during the development of the Bill.