Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

Justice and International Mission Unit
130 Little Collins Street
Melbourne Victoria 3000
Telephone: (03) 9251 5271
Facsimile: (03) 9251 5241
jim@victas.uca.org.au

25 July 2011

James Catchpole
Secretary
Joint Select Committee on Cyber-Safety
R1-109 Parliament House
PO Box 6021
Canberra, ACT 2600
jscc@aph.gov.au

Submission by the Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church in Australia to Inquiry into Cybercrime Legislation Amendment Bill 2011

The Justice and International Mission Unit welcomes this opportunity to make a submission to the Joint Select Committee on Cyber-Safety inquiry into the *Cybercrime Legislation Amendment Bill 2011*. The Synod of Victoria and Tasmania is actively concerned about ending both the abuse of children that occurs in the production of child sexual abuse material, and in the trafficking of children for the purpose of producing child sexual abuse material. The Unit's specific interest is in relation to addressing sexual abuse material on the internet, as this material represents serious transnational criminal activities. The Unit recognises that combating this criminal activity presents a number of substantial difficulties. Policing the online environment is in its early stages and in the case of online commercial child sexual abuse the criminal activity is hosted overseas and the victims are overseas while Australians are amongst the offenders that access and purchase the abuse material.

Most commercial child sexual abuse material is produced in countries with poor systems of enforcement to prevent the trafficking and abuse of vulnerable children and women.

UN Human Rights Council A/HRC/8/L.17 of 12 June 2008 calls for governments:

> *2(g) To establish mechanisms, where appropriate, in cooperation with the international community, to combat the use of the Internet to facilitate trafficking in persons and crimes related to sexual or other forms of exploitation and to strengthen international cooperation to investigate and prosecute trafficking facilitated by the use of the Internet.*

The Unit supports Australia's accession to the *Council of Europe Convention on Cybercrime* and the need to pass legislation giving effect to the Convention. The Unit believes that greater international efforts are required to combat child sexual abuse online, which requires greater international cooperation. Evidence suggests thousands of Australians purchase or share images of child sexual abuse electronically. Thus the Unit is supportive of legislative measures to allow for the rapid investigation of such offences and enhanced cooperation with requests for mutual assistance from law enforcement officials of other countries.

The Unit notes that Article 15 of the Convention requires that domestic implementation of the Convention complies with human rights obligations, including those contained within the *International Covenant on Civil and Political Rights*. The Unit urges that the Australian

Parliament to implement the *Council of Europe Convention on Cybercrime* in compliance with this respect for human rights standards.

Commercial Child Sexual Abuse on the Internet

The UN Office of Drugs and Crime (UNODC) report *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (17 June 2010) contains an assessment of the commercial child sexual abuse industry globally. This report estimates the online commercial child sexual abuse industry, as opposed to non-commercial peer-to-peer networks, generates an estimated 50,000 new child sexual abuse images each year and is worth about US$250 million globally. It involves thousands of commercial child sex abuse sites. Most of the victims are white and female, with the majority of the commercial child sexual abuse industry being based in Eastern Europe.

The UK based Internet Watch Foundation has identified 715 unique sources of commercial child sexual abuse websites, each with a distinct website name and brand. They found 321 of these were active in 2010. Of these, the ten most prolific 'brands' account for at least 47.7% of commercial webpages observed by the Internet Watch Foundation, with the most prolific using 862 urls. Each of the webpages or websites is a gateway to hundreds or even thousands of individual images or videos of children being sexually abused, supported by layers of payment mechanisms, content stores, membership systems and advertising frames. Payment systems may involve pre-pay cards, credit cards, 'virtual money' or e-payment systems and may be carried out across secure webpages, text or e-mail. Analysis by the Internet Watch Foundation has identified that the criminals running these operations do so in a cluster of commercial child sexual abuse 'brands' from the manner in which they share hosting patterns, payment arrangements, advertising systems and registration details as well as from the overall appearance of the websites.[1]

During 2010 a total of 14,602 webpages were featured on the Internet Watch Foundation blocking list of live child sexual abuse content. An average of 59 webpages were added to the list each day reflecting the speed at which child sexual abuse content moves online location.[2] The webpage blocking list now typically contains 500 urls at any one time, down from 1,200 in 2008.[3]

The Internet Watch Foundation found that 73% of the child victims appear to be under 10 years old and 66% of the images and videos depicted sexual activity between adults and children including the rape and sexual torture of the child.[4]

Of the sites blocked containing child sexual abuse material, 42% of the urls were hosted in North America, 41% in Russia and 17% in Asia. Only one site was found to be hosted in Australia.[5]

The 2009 analysis of online child sexual abuse images by Cybertip.ca reported they had examined 800 commercial child sexual abuse sites (representing 12.6% of all child sexual abuse sites they had dealt with) using 27 different payment types, most of which would be considered online payment systems.[6] In 55% of cases the sites claimed to be able to accept traditional credit cards for payment. For 61 of the sites payment could be made from a

[1] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[2] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[3] http://www.iwf.org.uk/resources/trends
[4] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.
[5] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.
[6] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 10, 56.

traditional bank or financial institution.[7] Nearly a quarter (23.8%) of the commercial child sexual abuse sites accepted multiple payment methods, with the average number of payment types being offered being 2.4 for those that offered multiple payment types.[8] The majority (85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (average of $53 a month). One-off membership fees (15.4% of the sites) ranged from $30 to $1,990 with an average cost of $249.[9] DVDs were also sold (5.8%) for as much as $1,900, as were a variety of packages (4.7%), image sets (3.1%), videos (1.1%) and websites (0.2%). Cybertip!ca concluded there is clearly a large consumer market for child sexual abuse images.

Cybertip.ca found that commercial websites tend to cater to a specific group of offenders, with images grouped in specific or narrow age ranges. A minority of commercial sites cater to individuals with a sexual interest in very young children, showing mainly infants and toddlers.[10]

They found that 29.7% of images on commercial child sexual abuse sites depict children being sexually assaulted, with 3.3% of images on commercial sites being of extreme sexual assaults (compared to 2.7% of images on all child sexual abuse websites).

Their analysis found the top five countries hosting urls for commercial child sexual abuse material were:[11]

- US (65.6%)
- Canada (8.7%)
- Russia (5.6%)
- Netherlands (2.9%)
- Germany (1.8%)

They found 80% of child sexual abuse sites hosted in Poland were commercial sites.[12]

They noted that in addition to the commercial child sexual abuse sites there are many sites that do not have their own commercial component but exist for the purpose of promoting commercial sites. In providing links, re-directs or advertisements for distinct commercial websites, these sites may receive payment or reciprocal linking for making child sexual abuse material available. These websites are indirectly profiting from the sale of child sexual abuse images.[13]

The UNODC argue that child sexual abuse material is available in both commercial and non-commercial domains, but the ratio between the two remains unclear.

The UNODC commented that despite their use of the internet, child pornographers and their clients are not necessarily technologically sophisticated. Only 6% of the offenders in one

[7] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 64.
[8] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 64.
[9] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 65.
[10] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 41.
[11] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 11.
[12] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 62.
[13] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 56.

sample used encryption technology. In another sample, 17% used password protection, 3% evidence – eliminating software and only 2% used remote storage systems. They note more sophisticated consumers could have evaded detection.

They estimate the upper limit of consumers of commercial child sexual abuse materials to be in the order of two million people globally.

A study of internet pornographic-related search requests by keywords in 2006 found that "teen sex" and "teen porn" were in the top 20 of such requests, with 14 million requests for "teen sex" and 6 million for "teen porn".[14] These terms related to 4 million webpages containing these keywords. However, the Unit notes the vast majority of this material would be legal, as there is a whole pornographic genre around women purporting to be 18 years old with terms such as "barely legal".

The UNODC 2010 report suggests that law enforcement efforts may be catching as little as 1% of all consumers of child sexual abuse materials.

UNICEF Philippines provided an example of Australians being involved in the establishment of commercial sites of sexual abuse material:[15]

> *In recent times, coinciding with the Internet boom, cybersex joints have opened. These are establishments that employ men, women and children to perform live sexual acts, which are then broadcast on the Internet via webcam. These sexual acts range from taking their clothes off to masturbating for the customers and doing other similar acts. It is also reported that there are cybersex joints where both heterosexual and homosexual acts are caught on webcam. Customers with Internet connections and credit cards may view these from a computer at home anywhere in the world.*
>
> *A number of these joints are found in Central Luzon. Lani (not her real name), who works full time for a local NGO, confirms the existence of numerous cybersex joints in their area. Most of these joints are operated by foreigners, mostly Australians and Americans, who have made the country their home. Usually, these foreigners have Filipino partners for their front men. She suspects that the owners of these joints have business partners abroad. Moreover, she also confirms that these cybersex joints employ children as young as 15 years old.*
>
> *The NBI [National Bureau of Investigation] also confirms that adult online entertainment providers exist in the country. These joints are offshore offices of adult online service providers in Western countries such as the United States. In May 2003, the NBI raided one of these joints, located at the plush San Lorenzo Village in Makati. According to the Inquirer (2003), the company was run by an American national. The joint's main office, however, is located somewhere in Nevada. It keeps an offshore office in the Philippines because it is much cheaper to operate here; Filipinas are paid much less than their US counterparts, and less money is spent on office maintenance. The company set up shop in a Makati mansion, which they subdivided into 10 different rooms, each room having two computers each complete with web cameras.*
>
> *The company, according to a NBI agent interviewed for the report, employed more than 20 women who went on eight hour shifts, twenty four hours a day. Not*

[14] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p.15.

[15] Arnie Trinidad, *Child Pornography in the Philippines,* Psychosocial Trauma and Human Rights Program UP Centre for Integrative and Development Studies and UNICEF Manila, 2005, pp. 48-49.

surprisingly, the company also employed teenage children. In the raid, the NBI were able to rescue two children aged 16 and 17. The women and girls who worked for the company were not regular women in prostitution, as some were found to be college students while others were waitresses who were either recruited directly by the owners or by their friends.

Evidence of the need for greater international co-operation in combating online child sexual abuse

A study by Cambridge University compared times taken to take down different forms of content.[16] It was found that Phishing sites and sites which threaten banks commercial interests are taken down very quickly. Child abuse image sites are by contrast likely to stay up for many weeks due to different jurisdictions not working together effectively, and reports being routed via local law enforcement which may not prioritise the issue or be properly trained to deal with it.

However, in their 2010 annual report the UK Internet Watch Foundation report that through activities to combat child sexual abuse material online, including blocking by ISPs, the length of time child sexual abuse images are hosted has been reduced from years to just days.[17] This outcome indicates that progress can be made against child sexual abuse material online if governments are willing to implement and resource effect laws to combat it.

An example of this was seen in late November 2010 six Virtual Global Taskforce partner agencies, including the Australian Federal Police, came together to dismantle a network of some 230 commercial child sexual abuse websites selling images and videos of children as young as three years old. Five members of an organised crime group in the Ukraine were arrested.[18]

The International Centre for Missing & Exploited Children has conducted updated research into legislation against child sexual abuse material globally.[19] They specifically examined whether national legislation:

- Exists with specific regard to child pornography, not just pornography in general;
- Provides a definition of child pornography;
- Expressly criminalises computer-facilitated offences;
- Criminalises possession of child pornography, regardless of intent to distribute; and
- Requires ISPs to report suspected child pornography to law enforcement or to some mandated agency.

They found that only 45 countries have legislation sufficient to combat child sexual abuse material (eight countries met all of the criteria above and 37 countries met all but the last criteria, pertaining to ISP reporting) and 89 countries have no legislation at all that specifically addresses child pornography.[20]

Of the countries that do not have legislation specifically addressing child sexual abuse material:

- 52 do not define child pornography in national legislation;
- 18 do not explicitly provide for computer-facilitated offences; and

[16] Moore, T & Clayton R, 'The Impact of Incentives on Notice and Take-down', (2008), www.cl.cam.ac.uk/~rnc1/takedown.pdf
[17] Internet Watch Foundation, '2010 Annual and Charity Report', p. 1.
[18] The Hon Brendan O'Connor, Launch of the Virtual Global Taskforce Conference, Opening Address, 2 December 2010.
[19] International Centre for Missing & Exploited Children, http://www.icmec.org
[20] International Centre for Missing & Exploited Children, 'Child Pornography: Model Legislation & Global Review', 6th Edition, 2010, p.iii.

- 33 do not criminalise possession of child sexual abuse material, regardless of intent to distribute.

Measures in the Cybercrime Legislation Amendment Bill 2011

The Justice and International Mission Unit acknowledges the need for the preservation of evidence in the investigation of cyber crimes. As noted by the Australian Institute of Criminology:[21]

> *The modern criminal, using the same devices as today's teenagers, communicates with Voice over Internet Protocol, video instant messaging, cellular camera phone, and text messaging in computer slang that is foreign to most police officers and parents. The trail to uncover this valuable investigation resource often starts with a forensic examination, but this trail quickly grows cold as Internet Service Providers overwrite logs and data retention periods expire. All police agencies are facing the same challenge when dealing with computer forensics. Police managers must find a way to examine an increasing number of digital devices, each containing an immense volume of data, in a timely manner and with limited resources.*

Thus the Unit strongly supports requirements for carriers and carriage service providers (C/CSPs) to preserve the stored communications and telecommunications data for specific persons when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign governments.

The Unit is concerned that in Schedule 2 relating to the amendments of the *Mutual Assistance in Criminal Matters Act 1987* Section 15B requires the offence to which the investigation relates be punishable by a maximum penalty of "imprisonment for 3 years or more, imprisonment for life or the death penalty". Given the assessment of the International Centre for Missing & Exploited Children about the paucity of laws to combat online child sexual abuse in many jurisdictions, this threshold could prevent providing assistance to law enforcement agencies in other jurisdictions in matters related to online child sexual abuse and grooming. For example, under section 160 of the UK *Criminal Justice Act 1988* possession of child sexual abuse material carries maximum penalty on conviction on indictment of a term of up to five years imprisonment, but a summary conviction of the same offence carries a maximum penalty of only six months imprisonment.[22] The Unit has scanned the legislation of other jurisdictions and notes a requirement of an offence having a maximum three year imprisonment penalty would prevent providing assistance in relation to offences under:[23]

- Article 117 of the Albanian Penal Code which carries a maximum penalty of two years imprisonment for "producing, delivering, advertising, importing, selling, publishing pornographic material in minors' premises".
- Section 207a(3) of the Austrian Criminal Code which states the possession of a pornographic depiction of a minor over the age of 14 carries a maximum penalty of only one year imprisonment and possession of a pornographic depiction of a minor carries a maximum penalty of up to two years imprisonment.
- Article 343 of the Belarus Criminal Code which has a maximum penalty of up to three months in prison for the possession of pornography (including child pornography) with the aim of its circulation or advertising.

---

[21] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p.82.

[22] Yaman Akdeniz, 'Internet child Pornography and the Law', Ashgate Publishing Limited, Surrey, UK, 2008, pp. 32-33.

[23] Taken from http://legislationline.org/documents/section/criminal-codes and http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/Default.asp

- Article 159(5) of the Bulgarian Criminal Code for the offence of keeping "a pornographic work for whose creation a minor, underage or a person with appearance of a minor or underage has been used" carries a maximum penalty of up to one year imprisonment.
- Article 191 of the Czech Republic Criminal Code which carries a maximum penalty of up to two years imprisonment for displaying or giving a child pornographic material (effectively a child grooming offence). Article 192 carries a maximum penalty of up to two years imprisonment for possessing "photographic, film, computer, electronic or other pornographic work depicting or otherwise exploiting a child".
- Section 235 of the Danish Criminal Code in relation to the dissemination of "obscene photographs or films, other obscene visual reproductions or similar of persons under the age of 18" as it carries a maximum penalty of up to two years imprisonment and possession of such material carries a maximum penalty of one year's imprisonment.
- The offence of sexual enticement under S 179 of the Estonian Criminal Code which carries a maximum penalty of one year imprisonment.
- Article 17, Section 18 of the Finnish Penal Code that carries a maximum penalty of two years imprisonment for "a person who offers for sale or for rent, distributes, or to that end manufactures or imports, pictures or visual recordings depicting children, violence or bestiality in an obscene way". Section 19 under the same Article carries a maximum penalty of six months imprisonment for possession of "a photograph, video tape, film or other visual recording, realistically depicting a child having sexual intercourse or in a comparable sexual act, or depicting a child in another obviously obscene way".
- Article 141 of the Georgian Criminal Code for "Depraved action without violence by the preliminary acknowledgement of criminality towards a person who is not 16 years old yet" carries a maximum penalty of up to two years in prison.
- Article 255 of the Georgian Criminal Code for child pornography offences carries a maximum penalty of imprisonment of up to two years imprisonment.
- Section 292 of the Indian Penal Code for the sale, circulation and advertising of child sexual abuse material which carries a maximum penalty of up to two years imprisonment for a first offence.

This only represents a sample of the offences that may be excluded. The Unit further notes that much of the commercial child sexual abuse industry is located in Eastern Europe, with the laws of many of these countries carrying less than a three year imprisonment penalty in relation to at least possession of child sexual abuse material.

The requirement of a maximum three year imprisonment penalty will exclude the issuing of stored communications warrants for foreign offences that are serious crimes under Australian law, but which carry a lower threshold of penalty in the foreign jurisdiction.

The Unit would therefore strongly recommends part (b) of Section 15B not apply to requests made by the requesting country that relate to criminal offences in relation to child sexual abuse and child grooming online. Similarly, Section 5EA of the *Telecommunication (Interception and Access) Act 1979* should include any offences related to 'child pornography' and 'child grooming' as being a serious foreign contravention.[24] The Attorney General should be able to authorise the making of an authorisation under Section 180B of the *Telecommunications (Interception and Access) Act 1979* if the offence relates to 'child pornography' in Section 15D of the *Mutual Assistance in Criminal Matters Act 1987*. Also, the ability:

- For 'Prospective authorisation';

[24] The Unit notes Australian legislation refers to child sexual abuse material as 'child pornography', which is also how it is referred to in the legislation of many other jurisdictions. Most law enforcement agencies and those working to combat such material now refer to 'child pornography' as child sexual abuse material or child exploitation material in response to the growing legitimacy of adult pornography in Western countries. It is feared that using the term 'child pornography' grants the material a level of legitimacy that is inappropriate.

- For ‘Extension of prospective authorisation’; and
- To allow disclosure to a foreign law enforcement agency

in Section 180B of the *Telecommunications (Interception and Access) Act 1979* should apply to all offences related to possession, production, trade in or distribution of ‘child pornography’ regardless of the offence having to carry at least a maximum penalty of three years in prison in the requesting country.

In the amendment of Section 15B of the *Mutual Assistance in Criminal Matters Act 1987*, the Unit would prefer the reference to the death penalty be removed. The Uniting Church in Australia has a long standing opposition to the death penalty, as does the Australian Parliament and successive Australian Governments. Making a request for mutual assistance dependent on an offence carrying the death penalty may be seen to be offering tacit support to the death penalty as a legitimate form of penalty. This concern also applies to the amendment of Section 5EA of the *Telecommunication (Interception and Access) Act 1979*, Section 15D of the *Mutual Assistance in Criminal Matters Act 1987* and Section 180B of the *Telecommunications (Interception and Access) Act 1979.*

Given the transnational nature of online child sexual abuse and its impact on tens of thousands of victims around the world, it is vital Australia assists other countries in criminal investigations where Australians have been the offenders or the victims, or where offenders have used Australian telecommunication services. Thus the Justice and International Mission Unit supports the ability of Australian agencies to obtain and disclose telecommunications data and stored communications for the purposes of assisting a foreign investigation.

To safeguard against misuse of the above measures, the Unit strongly supports the confidentiality requirements, through amendment of the *Telecommunications (Interception and Access) Act 1979*, contained within the Bill in relation to authorisations to disclose telecommunications data.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Phone: (03) 9251 5265
E-mail: mark.zirnsak@victas.uca.org.au