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

9 July 2010

Committee Secretary
Joint Select Committee on Cyber-Safety
Department of House of Representatives
PO Box 6021
Parliament House
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 The Joint Select Committee on Cyber-Safety

The Justice and International Mission Unit welcomes this opportunity to make a submission on cyber-safety. The Unit's specific interest is in relation to addressing sexual abuse material on the internet, as much of this material is generated through human trafficking and sexual servitude and represents serious transnational criminal activities.

The Synod of Victoria and Tasmania is actively concerned about ending both the abuse of children that occurs in the production of child pornography, and in the trafficking of children for the purpose of producing child pornography. The Unit notes that most child pornography and sexually abusive pornography is produced in countries with poor systems of enforcement to prevent the trafficking and abuse of vulnerable children and women.

The Unit notes the resolution of the UN Human Rights Council A/HRC/8/L.17 of 12 June 2008 calling 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 experience of the Justice and International Mission Unit

The Unit has previously made a complaint to the Australian Communications and Media Authority (ACMA) in relation to inappropriate posting from an external source to a mainstream social justice blog site that it established, and administers. The Unit made a complaint about a post promoting commercial 'forced' and 'amateur' 'rape videos'. Following investigation of the complaint, the ACMA was satisfied that the internet content (hosted outside Australia) contained content which was 'prohibited' or contained 'potential prohibited content'. In addition to this material, the same blog site has received a similar external posting, this time promoting commercial pornographic material relating to 'incest rape'. Staff within the Synod have also been sent e-mails directly marketing commercial sexual abuse sites, including child sexual abuse material, with complaints again being submitted to ACMA. This anecdotal experience has made the Unit very distrustful of claims that exploitative and illegal pornographic material is a purely 'underground' phenomenon.

Commercial Child Sexual Abuse on the Internet

The Unit notes the recent release of the UN Office of Drugs and Crime (UNODC) report on *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010 contains an assessment of the commercial child sexual abuse industry globally. The UNODC report estimates the commercial child sexual abuse industry on-line, 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. Commercial child sexual abuse sites are more likely to involve the abuse of very young children, with the Internet Watch Foundation noting that 69% of victims appear to be younger than 10 and 24% being less than 7 years of age. Most of the victims are white and female, with the majority of the commercial child sexual abuse industry being based in Eastern Europe. However, the US holds the largest national share of the domains related to child pornography detected by groups like the Internet Watch Foundation and Cybertip.ca.

Cybertip.ca also found that most commercial websites of child sexual abuse material sell memberships, and although on-line payment systems appear to be preferred, the majority also offered credit card payment options. The average cost of subscribing to a commercial site of child sexual abuse material was US$53 per month. Commercial child sexual abuse vendors often set up fictitious businesses in order to obtain a merchant account for credit card processing. To evade detection by law enforcement, payment schemes used by commercial child pornography sites are increasingly complex. The demand for anonymous payments has led to the development of virtual payment systems and virtual currencies. Virtual currencies may not require identification and validation, thus preventing law enforcement agencies from tracing money-flows back to offenders.

The UNODC argues 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 sample used encryption technology. In another sample, 17% used password protection, 3% evidence – eliminating software and only 2% used remote storage systems. They note that it is possible that more sophisticated consumers have evaded detection.

The UNODC estimates the upper limit of consumers of commercial child sexual abuse materials to be in the order of two million people globally.

The UNODC report suggests that law enforcement efforts may be catching as little as 1% of all consumers of child sexual abuse materials. Further, in addition to the UNODC report, it should be noted that many countries do not have laws to prosecute child pornography. A 2006 study by the International Centre for Missing and Exploited Children found that of the 184 member States of Interpol, 95 had no legislation at all that specifically addresses child pornography, and of those that do, 41 countries did not criminalise possession of child pornography, regardless of the intent to distribute.

An example of commercial sites of sexual abuse material being set up in our region has been raised by UNICEF in the Philippines:[1]

> *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.*

[1] 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.

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 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.

Actions to deal with Commercial Sexual Abuse on the Internet

The Synod of Victoria and Tasmania is supportive of the broad approach that has been taken by successive Federal Governments in dealing with cyber-safety, which includes education for Australian children and parents and funding for law enforcement agencies. We note the funding for law enforcement includes pursuit of producers and consumers of sexual abuse materials in Australia and also funding for the Australian Federal Police in assisting countries in the region in dealing with sexual abuse offences including child sexual abuse generally and human trafficking. The Synod notes that these initiatives appear to have universal support from Members of Parliament and Senators.

The Justice and International Mission Unit is supportive of the Government's efforts to require ISPs to not provide a service to clients seeking to visit overseas hosted websites containing Refused Classification (RC) rated content. The Unit believes that by setting the material to be blocked as that which is rated RC is a sensible decision, placing the decision of which sites get blocked within Australia's well established classification system. It makes sense that material that is prevented from being sold and distributed in other forms of media, such as DVDs, videos, printed material and the Australian hosted internet, due to its abusive content, should also be prevented from being accessed via the overseas hosted internet.

We note that it is already illegal under Australian law to host RC content on the internet on Australian soil. Those hosting RC content are subject to take-down notices issued by ACMA and criminal prosecution in the case of child pornography. The current law suggests that Australians should not be able to access RC classified material through book, films, magazines or Australian hosted internet content, but are allowed to access the very same material if it is hosted on a server overseas (although they are subject to prosecution for accessing child pornography even when the material is hosted on a server overseas for the minority of offenders who get caught).

The reasons for supporting requiring ISPs to be required to block user access to RC classified sites are:

- Using the RC category makes sense, as this is the category that bans sale and distribution of material in all other media, including the Australian hosted internet. To limit this further, means that material that would be banned from being hosted on the Australian internet can be legally disseminated through use of a server overseas. The material that those opposed to filtering RC content seem to be objecting to filtering are sites that promote criminal graffiti activities, safe illicit drug use and instruction in how to commit suicide or assist others in committing suicide. We are not convinced that having Australians, including Australian children, access such material through the unregulated overseas internet serves any worthwhile social purpose.
- With reference to sexual abuse material, including child pornography, blocking has a crucial role to play both in preventing the domestic consumer stumbling across the materials by accident and in preventing those who do not know how to access the material but who are curious, or who are at an early stage of developing or feeding their sexual interest in children.
- The implementation of blocking helps to undermine the whole commercial trade of child abuse images and actively disrupt its success. The more countries that use blocking systems the less successful and active this US$250 million market will become. It is the commercial industries in sexual abuse materials that are impacted by mandatory filtering. It has minimal benefits in dealing with peer-to-peer sharing of sexual abuse images and their production.
- It protects the vast majority of Australians who do not wish to view RC classified content accidentally stumbling across sites hosted overseas containing this material (for the sites that are on the blocked list).
- It is reasonable to expect ISPs to accept some responsibility for what their clients seek to view and the material they provide access to. Such action is consistent with Australia's commitments to fight transnational criminal activity, as outlined in the *UN Convention Against Corruption* and the *UN Convention against Transnational Organised Crime.* Australian ISPs have shown a great reluctance to voluntarily take any action to prevent their clients accessing child sexual abuse material, compared to the UK where 95% of ISPs have voluntarily adopted such measures and where UK human rights groups are calling for legislation to deal with the recalcitrant 5% that have not been willing to comply. ISPs being required to take some responsibility in relation to what their clients access to help combat transnational criminal activity is similar to the positive obligations that the Federal Government has introduced on banks and other financial institutions. Obligations on financial institutions require them to know their clients and report suspicious activity by clients who may be involved in transnational criminal activity such as money laundering, corruption and financing of terrorism.

The Unit does not see placing obligations on ISPs as a replacement for education and awareness programs and law enforcement, but as another complementary measure as part of a wider cyber-safety strategy. The requirement of taking social responsibility and not facilitating transnational criminal activity by ISPs would be largely designed to assist in providing cyber-safety to the children who would otherwise become victims of the demand for commercial child sexual abuse materials.

To that extent the Unit's position is similar to that of the European NGO Alliance for Child Safety Online (eNACSO). eNACSO campaigns for governments to introduce mandatory requirements on ISPs to not provide a service for their clients to access child sexual abuse sites. eNACSO has the following members:

- Save the Children Denmark
- Nobody's Children Foundation Poland
- Save the Children Italy
- ISPCC Ireland
- Save the Children Finland
- ECPAT Austria
- Action Innocence Belgium
- Estonian Union of Child Welfare
- Instituto de apaia a Crianca
- Kanner Jugendtelefon Luxemburg
- NSPCC UK
- Protegeles Spain
- Action Innocence France
- ECPAT Netherlands
- KEK VONAL Foundation Hungary
- Our Child Foundation Czech Republic
- Innocence in danger Germany
- Save the Children Romania
- Children Support Centre Lithuania

It is clear that Save the Children branches in Europe adopt a very different position on requiring ISPs to not provide service to those clients seeking to access commercial child sexual abuse materials compared to Save the Children in Australia.

The Unit notes that Italy already has a law to require ISPs not to assist clients in accessing child sexual abuse sites. France reached an agreement with ISPs in June 2008 for ISPs not to provide a service for their clients to visit sites containing child pornography and some other forms of content. Several of the large US-based search engines deploy the Internet Watch Foundation list. In the UK every mobile phone operator uses the Internet Watch Foundation list to block access to known sites via mobile handsets. The fact that so many ISPs and mobile phone operators are already blocking child abuse images shows that there are no reasonable technical arguments against implementing such a policy.

The Unit is highly supportive of incorporation of international lists of overseas-hosted child sexual abuse material provided by highly reputable overseas agencies. While the processes used to compile the lists should be reviewed by the ACMA before such lists are used, the agency in question should also be given the opportunity to discuss a decision with the ACMA where the ACMA decides not to use such a list because of process concerns it has.

Sites added to the RC content list from highly reputable overseas agencies should simply be treated the same as sites added by the ACMA through complaints made by Australian citizens.

From the Unit's point of view it would be desirable for ISPs to be required to report clients that attempt to access sites containing child sexual abuse materials to the appropriate authority for investigation, in the same way financial institutions and casinos are required to report suspicious transactions by clients to AUSTRAC.

The Unit notes that Australia could seek to play a greater role in international co-operation on take down notices for child sexual abuse sites. A study by Cambridge University compared times taken to take down different forms of content.[2] It was found that Phishing sites and sites which threaten banks' commercial interests are taken down very quickly. The child abuse sites are by contrast likely to stay up for many weeks due to the complexities of the fact that different jurisdictions do not work together effectively, and reports are routed via local law enforcement which may not prioritise the issue or be properly trained to deal with it.

In the area of law enforcement Australia should encourage more police forces to be part of the Virtual Global Taskforce to tackle child sexual abuse on-line, as currently only the police forces from Australia, New Zealand, Canada and Italy are part of this network.

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Phone: (03) 9251 5265

[2] Moore, T & Clayton R, 'The Impact of Incentives on Notice and Take-down', (2008), www.cl.cam.ac.uk/~rnc1/takedown.pdf