SUPPLEMENTARY SUBMISSION NO. 93.2

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

10 May 2011

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

Second Supplementary 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 second supplementary submission on cyber-safety. As noted in the previous two submissions 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 representing 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 sexual abuse material.

This supplementary submission seeks to provide further information around global measures to combat the commercial child sexual abuse industry and the human trafficking that feeds it. It draws on current research and experience of internationally recognised organisations which specialise in this field: Cybertip.ca - Canada's national tipline for reporting the online sexual exploitation of children; the UK Internet Watch Foundation (IWF) which in partnership with the police, government and the online industry, has had a major impact in successfully removing child abuse from the internet; the International Telecommunications Union of which Australia is one of 192 member states, and Interpol.

The Unit supports a number of the recommendations that have been made by Cybertip.ca to combat child sexual abuse online including:

- That governments should work together to establish international standards for the personal information a registrant is required to provide when registering a new domain name. This could include proof of name and address, residency in a particular country and contact information. This information could be valuable in the event of an investigation, assisting in determining the owner of a child pornography website, and potentially rescuing children from ongoing sexual abuse.[1]
- Governments should require domain name registrants to discard from use domains hosting illegal content. This would prevent new website owners from purchasing domains known to host child sexual abuse material and reusing them for the same purpose. Due to the fact that the domain names become important marketing tools, and become well-

[1] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 48.

> known to consumers of child sexual abuse images, steps need to be taken to remove them permanently from circulation.[2]

The Unit continues to stress that requiring ISPs to block unrestricted access for clients to child sexual abuse material acts as an effective disruption strategy against commercial sites, keeping their profitability low and therefore helping to dissuade organised criminals from seeing this as a source of easy revenue. Secondly, blocking should be seen as an educative tool for offenders and potential offenders in the non-contact category. Informal discussions with law enforcement officials who work to combat child sexual abuse online indicate they believe that education of offenders and potential offenders is a vital tool in this fight. However, the Unit is unaware of there being in Australia any wide scale education campaign targeting this group. Such a campaign could be mounted through legal pornography sites, given this is a common pathway for non-contact offenders to escalate to child sexual abuse material. The Unit suspects that legal pornographers would be unwilling to host such a campaign on their sites, not wishing to acknowledge that their sites are often a pathway for consumers to escalate to child sexual abuse material.[3] However, blocking of known child sexual abuse sites provides a potential educative moment for an offender or potential offender. With the right message it can remind the offender what they are attempting to do is illegal and may help undermine the process of normalisation and cognitive distortion offenders use to justify their behaviour.

The Unit notes that on 15 October the Board of Directors of the International Centre for Missing & Exploited Children passed a resolution stating:

> *Resolves that, given the global scope of ICMEC's work, ICMEC should encourage a multi-faceted approach and advocate for the combined recourse to all available solutions – including but not limited to blocking, filtering, notice-and-takedown, and other appropriate proactive measures – to identify and remove illegal content (involving the sexual exploitation of children) from the Internet.*

Based on reports of the volume of attempts to access child sexual abuse material online blocked by ISPs in other OECD jurisdictions, the Unit accepts that it is not helpful to have all these reported to the Australian Federal Police for investigation. Simply, there are likely be too many offenders and potential offenders for the AFP to investigate with its limited resources and it already must prioritise which reports of offenders accessing child sexual abuse material it will investigate. However, the Unit believes that the Australian Crime Commission would be interested in data on how many offenders and potential offenders are seeking to access child sexual abuse material, so ISPs could collect such data for the benefit of the ACC.

Interpol's Limited Blocking

The INTEROPOL General Assembly passed a resolution in 2009 (AG-2009-RES-05) stating that it:

> *Encourages member countries to promote the use of all the technical tools available, including access-blocking of websites containing child sexual abuse images, in order to intensify the fight of their national specialised units against the dissemination of child sexual abuse images on the internet;*
>
> *Encourages member countries to systematically provide the INTERPOL General Secretariat with updated lists of websites containing child sexual abuse images for*

[2] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 49.

[3] The Unit acknowledges that it is likely to be a small minority of consumers of legal pornographic material that progress to accessing child sexual abuse material.

> *dissemination to INTERPOL member countries, so as to enable them to take appropriate action;*
>
> *Tasks the INTERPOL General Secretariat to maintain and disseminate to the National Central Bureaus a worldwide list of URLs (Internet addresses) which contain those websites that publish the most severe child abuse material.*

INTERPOL has promoted a limited form of domain blocking by ISPs, at the same time noting that existing efforts by some countries to block access to child sexual abuse materials has had “very good results”.[4]

The INTERPOL promoted domain name blocking requires that all the domains on the list have been verified as containing child sexual abuse material by at least two different governments/ agencies under the CIRCAMP umbrella. The domain to be blocked must fit the following criteria:

- The children are real. Sites containing only computer generated, morphed, drawn or pseudo images are not included.
- The ages of the children depicted in sexually exploitative situations are (or appear to be) younger than 13 years.
- The abuses are considered severe by depicting sexual contact or focus on the genital or anal region of the child.
- The domains have been online within the last three months.

The method results in over-blocking as the whole domain is deemed illegal if any part of it is found to contain sexual abuse material with children. However, the fact the material has to have been on the domain for three months suggests a domain administrator that is not serious about monitoring the content of the domain, and this is a method to force them to act. However, the tight criteria of this form of access blocking reduces its effectiveness as a dynamic disruption strategy against the commercial child sexual abuse industry (compared to the Internet Watch Foundation that update their list of urls to be blocked twice a day).

INTERPOL argue the “primary goal of blocking access to child sexual abuse material is to protect the rights of the children being depicted, while the secondary goal is to prevent illegal viewing, possession and distribution of the said material.” They argue on blocking access to child sexual abuse material more generally:

> *Utilising access blocking will free up resources within the police to work on identifying the victims of child sexual abuse rather than handling recurring reports from the public or NGOs about content being redistributed again and again on commercial web pages. In addition, an overview of the material distributed on the Web pages may provide important evidence and clues in identification cases and can complement ongoing investigations.*

INTERPOL also point out that access blocking assists law enforcement in prosecuting offenders accessing child sexual abuse material as those offenders who circumvent the blocking will then be barred from “using the ‘accidental and unwilling access’ argument if detected by the police.”

They summarise the advantages of access blocking as:

> *The system prevents crimes from being committed, limits the number of criminals having to be investigated in cases related to commercial child sexual abuse material web pages and protects victims. By preventing crime and thereby reducing the amount of work for the police, more resources can be put into investigations and subsequent court proceedings.*

[4] http://www.interpol.int/Public/THBINternetAccessBlocking/

INTERPOL acknowledges that access blocking:

> *…. must be used in combination with traditional police methods, such as investigations into and the removal of child abuse material hosted on the Internet, undercover operations, arrests, searches etc. Blocking child sexual abuse material should never be used instead of the above methods, it should be used in addition to these – in a holistic approach to combat sexual exploitation.*

Policy Recommendations of the International Telecommunications Union

In 2009 the International Telecommunications Union (ITU) issued their *Guidelines for Policy Makers on Child Online Protection.* They pointed out:[5]

> *Every time an image of a child being abused appears on the Internet or is downloaded in an important sense that child is being re-abused. Victims must live with the longevity and circulation of these images for the rest of their lives. The best proof of this is the reaction of the victims and their families when they learn the images have been put into circulation or uploaded to the Internet.*

The ITU recommended that ISPs and ESPs should be encouraged to proactively scan their networks for child abuse material and report it to the relevant law enforcement authorities. They recommend that legislation should provide protection for ISPs, ESPs and other private entities that report child abuse material and should include guidance for the safe handling and transmission of images.[6] The ITU concluded that "It is clear that law enforcement cannot arrest their way out of this problem and more needs to be done to disrupt and reduce the traffic in CAM [Child Abuse Material]."[7] They also highlight the educative value of block pages when a list is used by ISPs to disrupt the commercial child sexual abuse industry online:[8]

> *When a site is blocked, a STOP page should be displayed to the user. This STOP page has the dual function of giving information as to the reason the site was blocked (illegality of content) plus acting as a prevention vehicle that reminds the user/ consumer of the illegal nature of the material, as well as the presence of law enforcement agencies online.*

In summary the ITU recognises the place of ISP blocking of access to child abuse material as one important tool in the fight against such material:

> *Blocking access to web sites and Usenet Newsgroups containing CAM can make an important contribution to disrupting and reducing the volume of content being circulated or distributed over the Internet. However, this is recognised as only part of the solution. This approach is not meant to be the only solution. The goal is to complement the efforts of law enforcement and to reduce the availability of CAM online. Individuals who have a sexual interest in children and enough technical knowledge and determination, may still be able to locate it. However, the web in particular, has such as easy user interface and has become one of the most widely used and most popular Internet applications, that it is essential to develop specific approaches for tackling it while continuing to evaluate new methods to thwart distribution on the other platforms of the Internet.*

[5] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 19.

[6] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 27.

[7] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 28.

[8] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 29.

Volume of Blocking

Most ISPs that voluntarily block access by their clients to child sexual abuse material either do not collect data on the number of attempts made by clients or do not report this statistic. However, what data is available suggests western democratic societies have thousands of people who seek to access child sexual abuse material. There is little reason to believe that Australians would be any different.

A BBC report from 2006 indicated that UK ISP BT were blocking 35,000 attempts to access child sexual abuse material each day by their clients, 18 months after they started using the Internet Watch Foundation list of known child sexual abuse sites.[9] BT provided service to one third of UK internet users.

Cybertip.ca reported in their 2009 report that in the UK, a single ISP blocked more than 20,000 daily attempts to access child sexual abuse material and in Norway the estimate was 15,000 – 18,000 daily attempts.[10]

Cybertip.ca reported that the Internet Filtering Learning Centre reported in 2007 that "teen porn" was in the top 20 of adult search requests.[11]

Internet Watch Foundation Experience

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.[12] This indicates high disruption for any commercial operator seeking to making profit from selling images. In every instance where an image is removed quickly the risk of a child being revictimised by someone viewing their abuse has been substantially reduced.

Discussions with law enforcement officials working in the area suggest that commercial child sexual abuse businesses rely on selling to a large number of customers, as this allows the sale price to be lower, means more revenue can be obtained for each image and reduces risk of detection and apprehension by law enforcement. The production of each abusive image involves a criminal offence that carries risk of detection and apprehension in the carrying out of the offence. These businesses do not primarily rely on a small number of customers that purchase large volumes of images. Thus, disrupting the ability of commercial child sexual abuse businesses to be accessed by large volumes of customers reduces those that will seek to profit from this particular form of organised transnational crime.

The Internet Watch Foundation reports that there has been a change in the way child sexual abuse material is hosted on the internet with a growing amount of content being posted to separate locations rather than large collections of images stored within a folder on a single website.[13]

The 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 the commercial webpages seen 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

[9] http://news.bbc.co.uk/1/hi/uk/4687904.stm

[10] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 16.

[11] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 16.

[12] Internet Watch Foundation, '2010 Annual and Charity Report', p. 1.

[13] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.

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.[14]

The Internet Watch Foundation reports that its 70 ISP, search and content providers, mobile operators and filtering companies who block client access to child sexual abuse material now cover 98.6% of residential broadband connections.[15]

During 2010 there were a total of 14,602 webpages that featured on their 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.[16] The webpage blocking list now typically contains 500 urls at any one time, down from 1,200 in 2008.[17]

Of the sites blocked containing child sexual abuse material, 42% were hosted in North America, 41% in Russia and 17% in Asia. Only one site was found to be hosted in Australia.[18]

They 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.[19]

In a 2008 survey of 1,000 adults in the UK, the Internet Watch Foundation found that 5% of internet users had been exposed to child sexual abuse material online.[20] Of those exposed to this material 6% reported it to the police, 4% to their ISP, 4% to a charity, 11% to a hotline that deals with such material, 47% ignored it and 30% said they would have reported it, but did not know how to do so.

Those who argue that requiring ISPs to not provide unrestricted access to child sexual abuse material will be expensive should note that the Internet Watch Foundation report their entire operation ran on a budget of just £1 million ($1.5 million) in 2009 and in 2010.[21]

Cybertip.ca analysis of commercial child sexual abuse sites

The 2009 analysis of child sexual abuse images online 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) which used 27 different payment types, most of which would be considered online payment systems.[22] 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

[14] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.

[15] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.

[16] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.

[17] http://www.iwf.org.uk/resources/trends

[18] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.

[19] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.

[20] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research

[21] Internet Watch Foundation, '2010 Annual and Charity Report', p. 16.

[22] 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.[23] Nearly a quarter (23.8%) of the commercial child sexual abuse sites offered multiple payment methods, with the average number of payment types being offered being 2.4 for those that offered multiple payment types.[24] The majority (85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (average of $53 a month). Membership obtained for a one-time fee (15.4% of the sites) ranged from $30 to $1,990 with an average cost of $249.[25] 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%). They concluded there is clearly a large consumer market for child sexual abuse images.

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.[26]

Their analysis found the top five countries hosting commercial child sexual abuse material were:[27]

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

They found that 80% of child sexual abuse sites hosted in Poland were commercial sites.[28]

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.[29]

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).

Cybertip.ca noted that some of the child sexual abuse sites operate on fast flux networks. Fast flux domains use nameservers that supply IP addresses that change quickly and constantly. Typically these are IP addresses of compromised residential computers that are serving the content of the webpage or acting as a proxy to the content hosted at another location. This means that a geographic lookup conducted on a website may provide a different result depending on when it is conducted – even if the lookups occur 10 minutes

[23] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 64.
[24] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 64.
[25] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 65.
[26] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 56.
[27] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 11.
[28] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 62.
[29] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 41.

apart. Cybertip.ca found that over a 48 hour period one child sexual abuse website cycled through 212 unique IP addresses, located in 16 different countries (including Australia) and would change approximately every three minutes.[30] This renders any system that would attempt to block access to child sexual abuse sites on the basis of IP addresses ineffective.

Update on legislation globally against child sexual abuse material

The International Centre for Missing & Exploited Children has conducted updated research into legislation against child sexual abuse material globally.[31] They specifically examined if 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 continue to have no legislation at all that specifically addresses child pornography.[32]

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

The International Telecommunications Union has also stressed the need for international harmonisation of laws against child abuse material online as a key step towards the success of any strategy for child online protection.[33]

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

[30] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 62-63.

[31] International Centre for Missing & Exploited Children, http://www.icmec.org

[32] International Centre for Missing & Exploited Children, 'Child Pornography: Model Legislation & Global Review', 6th Edition, 2010, p.iii.

[33] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 21.