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

15 March 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

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 supplementary 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 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.

The Unit believes that Australia should be doing more to deter and prevent its citizens from being consumers of commercial child sexual abuse materials, than the existing law enforcement approach that catches only a small minority of offenders.

The Unit is disappointed with the submissions to this inquiry that oppose ISPs being required not to provide an unrestricted access to Refused Classification material on the Internet. These submissions show no attempt to understand the nature of sexual abuse material on the Internet or the diversity of the typologies of those who seek to access it. Further, almost none of them show any concern for the victims of child sexual abuse overseas, whose images are sold to consumers of such material all over the world, including Australia. The focus only seems to be on protecting Australian children from such harm.

The Unit notes the on-going evidence of the commercial child sexual abuse industry online. 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.[1]

This submission outlines research on the distinct differences between those who purchase online child sexual abuse images and are not involved in contact offences and contact

[1] The Hon Brendan O'Connor, Launch of the Virtual Global Taskforce Conference, Opening Address, 2 December 2010.

offenders who often work in networks trading child sexual abuse images. The research largely supports the utility of blocking access to commercial child sexual abuse sites as a prevention mechanism to prevent some people becoming non-contact offenders online.

1. Summary

1.1 The Problem

- Chapter 10 of the UN Office of Drugs and Crime (UNODC) report on *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* that was released on 17 June 2010 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. Each one of these images involves the abuse of a child, many of these child victims fit the definition of being victims of human trafficking.
- 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 appearing 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.
- Our partner church in India, the Church of North India, who work with victims of human trafficking, report that an increasing number of children are being used to produce child sexual abuse images for sale on the Internet.
- UNICEF in the Philippines has reported that Australians have been involved in setting up commercial child sexual abuse Internet businesses in that country, selling web camera access to clients in places like Europe, the US and Australia.
- Those convicted of offences related to child sexual abuse material in the developed world is growing. In 2005 in the UK, there were 1,296 convictions for the publication, possession or distribution of obscene matter and indecent photographs of children, an increase of almost 500% since 1999. Also this meant these offences were over a quarter of the 4,800 convictions for all sexual offences in the UK in that year.[2]
- The UNODC report suggests that law enforcement efforts may be catching as little as 1% of all consumers of child sexual abuse materials.
- Most consumers of online child sexual abuse material claim they were looking for adult pornography initially and their first encounter with child sexual material online was accidental.
- Conventional law enforcement is very resource intensive in terms of both investigation and prosecution, meaning that law enforcement agencies must be selective about which cases they investigate.
- Further, conventional law enforcement has an impact on all those in the judicial system required to view the child sexual abuse material in such cases, including police, lawyers and judges.
- Thus, it would appear Australians are consumers of commercial child sexual abuse materials out of those globally purchasing such material and the vast majority will not face prosecution through conventional law enforcement means. However, there is a severe lack of research on Australians who access child sexual abuse material online.
- Child sexual abuse material online represents a revictimisation of the abused children.
- There are a significant group of offenders who purchase child sexual abuse material online and do not engage in physical child sexual abuse themselves (contact offenders). These are two largely separate groups of offenders. Contact offenders are those that

[2] D. Middleton, R. Mandeville-Norden and E. Hayes, *Does treatment work with internet sex offenders? Emerging findings from the Internet Sex offender Treatment Programme (i-SOTP),* Journal of Sexual Aggression **15(1)** (2009), p. 7.

dominate peer-to-peer networks, while non-contact offenders often operate by themselves reinforcing their own self view that they are not sex offenders.

- Those who only purchase child sexual abuse material are far more likely to access more abusive images than those involved in peer-to-peer networks.
- There is evidence that interventions with those who purchase commercial child sexual abuse materials are more effective at reducing recidivism compared to contact offenders.
- Research has indicated that the ready access to child sexual abuse material online has created an impression for offenders that this is a common practice and so reduces inhibitions to abuse.

1.2 Requiring ISPs not to provide an unrestricted service to customers

- Requiring Australian ISPs not to provide unrestricted access to child sexual abuse sites on the internet through blocking of a list of such websites is a disruption strategy.
- It will not block the determined consumer of child sexual abuse material.
- It is largely ineffective against peer-to-peer networks.
- It will block inadvertent access.
- It will assist in deterring those who are curious and do not have high internet skills. The available literature on those who purchase commercial child sexual abuse material on the Internet suggests this is a behaviour that escalates. It is therefore reasonable to postulate that a shock early in offending behaviour may deter some offenders from further access to child sexual abuse material. In other words, this measure is of benefit to those that are deterred from offending behaviour and those around them that would be impacted by this behaviour.
- It will disrupt the ability of commercial child sexual abuse providers to market themselves and provide a smooth service to their customers, in the same way it would disrupt any legitimate business if their websites were to be place on a list of sites that Australian ISPs were required not to provide a service to.
- The more countries that use blocking systems the less successful and active the US$250 million online commercial child sexual abuse market will become.
- Due to the different characteristics of offenders that purchase commercial child sexual abuse material, it appears interventions that challenge their beliefs that what they doing is acceptable, will be more effective than offenders involved in peer-to-peer networks of contact offenders.
- It will send a message to potential offenders that the material they are seeking to access is not acceptable to assist in maintaining inhibitions to abuse.
- It reduces revictimisation of the children depicted in the sexual abuse material.
- This action does not replace the need for law enforcement, but is complementary to disrupt the activities of the majority of offenders that law enforcement will not end up investigating or prosecuting.
- It does not replace the need for the education of Australian children and parents about cyber-safety, but is a measure that Australia can take for the tens of thousands of victims of child sexual abuse overseas every year whose images are sold to consumers in Australia online.

1.3 Alternatives or additional measures to placing requirements on ISPs to block unrestricted access to child sexual abuse material

- Australia should be providing greater assistance to other governments to introduce laws criminalising the production, dissemination and distribution of child pornography and the effective enforcement of these laws. 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.
- The Parliament should enhance Section 313 of the *Telecommunications Act 1997* and Part 10.6 Subdivision E Section 474.25 of the *Criminal Code* so that if members of the IT industry are aware of any of their clients accessing child sexual abuse materials they are left in no doubt they have an obligation to report such activity to the appropriate authorities. There are cases of parts of the IT industry failing to report clients accessing and sharing child sexual abuse material, even when they have detected it.
- In addition to blocking, legislation could be introduced an provide an obligation on ISPs to implement software which monitors if any of their clients access known child sexual abuse sites. The data would then be provided to the appropriate authority for investigation. This would not monitor the activity of clients unless they attempted to access the child sexual abuse site. In other words, it is site monitoring, not user monitoring. No data would be captured of activity involving visits to sites not on the child sexual abuse list.
- The Australian Government should conduct further research on the Australian consumers of child sexual abuse materials to build up a picture of their typology and their behaviour (the point above could be used to conduct this task, even if it was not used for the purposes of prosecution).
- The Australian Government should work with other governments and appropriate UN bodies to conduct research on those that produce commercial child sexual abuse material to gain a greater understanding of their business model and additional measures to disrupt their businesses.

2. Offenders who purchase child sexual abuse material online are different from other child sexual abuse offenders

The following section outlines some of a available peer reviewed research into offenders who access child sexual abuse material online. The research points to distinct typologies of offenders. One category are offenders who purchase and access child sexual abuse material online and do not engage in contact offences themselves. Many of these offenders first experience child sexual abuse material online accidentally. Further, they do not regard themselves as sex offenders. However, on average they end up purchasing images of younger children and of more abusive acts than contact offenders do.

According to Professor David Middleton of De Mountford University, only around 10% of offenders who download child sexual abuse material online go on to commit actual child sexual abuse themselves (become contact offenders).[3] His research suggests that such offenders use self-distancing to justify their offending behaviour, with the Internet providing a vehicle to distance themselves from the act they are viewing as well as justifying a view that they are not sex offenders themselves. They are able to justify continued access to child

[3] D. Middleton, *From Research to Practice: The Development of the Internet Sex Offender Treatment Programme (i-SOTP),* Irish Probation Journal **5,** Sept 2008, p. 52.

sexual abuse material in a context that they are not directly responsible for the harm and are simply a passive viewer.[4]

A US based National Juvenile Online Victimisation Study found of a sample of 429 possessors of child sexual abuse material, only 11% had known previous sexual offences. In the same study the authors looked at 241 legal cases involving possessors of abusive images of children and found that 55% could be deemed 'dual offenders', engaging in both the obtaining of images of child sexual abuse and in contact offences. Of the 55%, 40% had committed a contact sexual offence against a child and a further 15% had attempted to commit a contact sexual offence against a child. Seto and Eke (2005) studied 201 Canadian male adult offenders convicted of offences related to child sexual abuse material. They found that 24% had prior convictions for sexual contact offences with children and 15% had prior convictions related to child sexual abuse material.[5] A study of print and news reports of 205 Internet offenders found 19% of offenders traded and collected child sexual abuse images while simultaneously manipulating children online for offline offences. This compared to 59% of offenders who solely trafficked and collected abusive images and 22% who were using the Internet solely to manipulate children for contact offences.[6] A study of 90 offenders possessing child sexual abuse material and 118 child contact offenders found that while there is a subgroup of those who possess child sexual abuse material who may recidivate via the Internet, there is no evidence to suggest that these offenders would escalate to a contact sex offence.[7]

Research tends to indicate that those accessing child sexual abuse material online under-report their involvement in contact offences.[8] However, most of these studies have failed to examine if there are differences between offenders who source such material through peer-to-peer networks and those who purchase material commercially and have no contact with networks of other offenders.

McCarthy (2010) considered a sample of 107 male adult Internet offenders in the US, 56 of whom were non-contact offenders and 51 were contact offenders (based on offender history or conviction of sexually abusing a child).[9] She found the contact offenders were more likely than non-contact offenders to masturbate to child sexual abuse material.[10] She found that 29% of non-contact and 36% of contact offenders purchased child sexual abuse material, while 36% of non-contact and 53% of contact offenders traded in child sexual abuse material.[11] Contact offenders attempted significantly more involvement with children than non-contact offenders. Non-contact offenders were found to be far more likely to operate on their own, while contact offenders are more likely to operate in networks. Only 11% of non-contact offenders communicated with others that shared their interest in child sexual abuse

[4] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 88.
[5] M.C. Seto and A.W. Eke, *The Criminal Histories and Later Offending of Child Pornography Offenders,* Sexual Abuse: A Journal of Research and Treatment **17(2)** (2005), p. 201.
[6] A.R. Beech, I.A. Elliott, A. Birgden, and D. Findlater, *The internet and child sexual offending: A criminological review,* Aggression and Violent Behaviour **13** (2008), p. 223.
[7] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 183.
[8] J. Buschman, D. Wilcox, D. Krapohl, M. Oelrich, and S. Hackett, *Cybersex offender risk assessment. An explorative study,* Journal of Sexual Aggression **16(2)** (2010), p. 2006.
[9] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 186.
[10] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[11] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.

material online, compared to 50% of contact offenders. Only 3% of non-contact offenders communicated in person with others who shared their interest in child sexual abuse material compared to 28% of contact offenders.[12] It should be noted that McCarthy found that her research led to the conclusion that possessing child sexual abuse material was not causal of going on to commit contact offences, as 84% of contact offenders in the sample reported sexually abusing a child prior to possessing child sexual abuse material.[13]

In a sample of 72 Internet offenders in the UK it was found that 60% could be assigned to the intimacy deficits or emotional dysregulation pathways as the causes of their offending behaviour.[14] Those with intimacy deficits were described as having low expectations of the efficacy of initiating and maintaining age-appropriate relationships and accessed child sexual abuse images at times of loneliness and dissatisfaction. This creates a form of pseudo-intimacy, whereby the images represent a less fearful and accepting "partner" and circumvent problems initiating appropriate sexual relationships.

Research also shows that the anonymity of purchasing child sexual abuse images online with its lack of face-to-face communication may function to lessen social risk and has a powerful disinhibiting effect on users. Also within these social contexts, offenders are able to normalise their activities and legitimate their orientations and behaviours.[15] The act of downloading images allows the perpetrator to block the idea that there is a victim – no one is struggling with them or screaming.[16]

Those offenders with emotional dysregulation problems were described as lacking control during periods of strong negative mood states, which hen coupled with deviant sexual desire could lead to the use of pornography (in this case child sexual abuse material) as a mood alleviating strategy.[17] For some offenders, but not all, accessing images on the Internet may function as a way of avoiding or dealing with difficult emotional states.

Research has found that the cognitive distortions of those who purchase commercial child sexual abuse images are different from those who are contact offenders. Internet offenders appeared to hold cognitive distortions related to the notion that sexual fantasies and images of child sexual abuse are not directly harmful (for example, "Having sexual thoughts and fantasies about a child isn't all that bad because at least it is not really hurting the child").[18] Another offender stated:[19]

---

[12] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), pp. 189-190.
[13] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 193.
[14] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 78.
[15] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 78.
[16] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 137.
[17] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 78.
[18] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 79 and D. Middleton, R. Mandeville-Norden and E. Hayes, *Does treatment work with internet sex offenders? Emerging findings from the Internet Sex offender Treatment Programme (i-SOTP),* Journal of Sexual Aggression **15(1)** (2009), p. 8.
[19] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 130.

> *"Yet, you know if you come up, come up, with those images on your computer then everybody assumes, then you know, you are creating victims and to me that's a, that's a, nonsense. You can't create a victim by masturbating over someone cos that victim never knows that's happening to them".*

Or another:[20]

> *"…cos internet is like it fuels your fantasies. You can look at pictures and you can imagine all sorts of things, without anybody getting hurt."*

As the researchers noted in this case:[21]

> *The phrase "fuels your fantasies" re-locates the abuse from the real world into a private domain in one's head, where the children become almost fictional images, thereby breaking the link with the acts of abuse required to produce such images.*

Winder and Gough (2010), in interviews with seven Internet offenders, found they distanced themselves from the charge of creating child victims, rejected the offender label for themselves and presented their activities as relatively inoffensive when compared to other, mainly contact crimes. The researchers found the offenders repeatedly invoked the non-contact nature of the online offence to mitigate their responsibility.[22] Such self-distancing was also easier where the offender accessed images in which the child victims appeared happy. For example, one offender stated "They're enjoying it, they're having fun, nobody's getting harmed – they're only pictures".[23]

Winder and Gough (2010) had an offender justify his behaviour through the inconsistency of laws globally to combat child sexual abuse, arguing what he did would have (erroneously) been legal in Japan.[24] Another offender argued that children in poverty overseas being photographed naked for money was better than them starving.[25] Should this attitude be held more widely by offenders, it would add weight for the need to have a uniform global effort to combat child sexual abuse, including online child sexual abuse.

They also found that the Internet offenders regarded contact sex offenders as separate from themselves and regarded them largely as the general public does, as obscene, insatiable predators.[26]

Most online consumers of child sexual abuse material claim they were looking for adult pornography initially and their first encounter with child sexual abuse material was accidental.[27]

Henry *et al* (2010) studied 422 Internet sexual offenders from the UK and found three recognisable populations of offenders akin to contact offenders: the apparently normal, the inadequate and the deviant. Victim empathy deficits were concentrated in one group, and

---

[20] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 132.
[21] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 132.
[22] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 129.
[23] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 130.
[24] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 131.
[25] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), pp. 131-132.
[26] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 132.
[27] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 135.

self-esteem and emotional loneliness difficulties in another. The sample did not separate offenders who purchased child sexual abuse images from those that shared such images in peer-to-peer networks.[28]

Child sexual abuse material is deliberate and stylised to meet both implicit and explicit audience demands, where coercive instructions, such as to "smile" and "look at the camera" are often heard in child sexual abuse videos available on the Internet.[29]

Research has found that the readily available wealth of child sexual abuse material on the Internet may create a false impression amongst offenders that this is a common practice, and so reduces inhibitions to abuse. Child sexual abuse material is also hypothesised to serve as a reinforcer for both sexual attraction to children and the self-justification process. This reinforcement is particularly potent due to the immediate and interactive nature of the feedback received. It is also argued that the research so consistently produces correlations between pornography and harm that pornography should be re-conceptualised as "instrumentally casual [though not solely casual] in the etiology of sex offending."[30]

Contact offenders who download child sexual abuse material online are more likely to have images of sexual abuse they would engage in, as opposed to those who purchase images online who tend to view more abusive images.

A higher number of offenders who are at low risk of reoffending or going on to commit contact offences appear to be accessing images of child abuse of younger children and depicting more serious victimisation than those offenders at high risk of reoffending or going on to commit contact offences.[31] In a sample of 72 Internet offenders from the UK, 85% viewed images up to severity levels 4 and 5, with 31% of offenders viewing level 5 images. These categories refer to images depicting 'penetrative sexual activity between child(ren) and adult(s)' (level 4) and images of 'sadism and bestiality' (level 5). None of those offenders assessed as being high risk were found to be in possession of level 5 images. In contrast, a quarter of those assessed as medium risk and 35% of those assessed as low risk had been found to have level 5 images.[32]

In terms of the images possessed by the offenders, the average age of the youngest child depicted in an image was 6.3 years (with a median of six years). The reported age of the youngest victim in the collection was four years for the high-risk group (with a mean of seven years and a median of eight years of age), two years for the medium-risk group (with a mean of 7.3 years and a median of eight years of age) and under one year for the lowest risk group (with a mean of six years and a median of five years of age). None of the low-risk offenders were viewing images of adolescent teenagers only.[33] In other words, non-contact offenders

---

[28] O. Henry, R. Manderville-Norden, E. Hayes, V. Egan, *Do internet-based sexual offenders reduce to normal, inadequate and deviant groups?,* Journal of Sexual Aggression **16(1)**, (2010), p. 44.
[29] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 88.
[30] A.R. Beech, I.A. Elliott, A. Birgden, and D. Findlater, *The internet and child sexual offending: A criminological review,* Aggression and Violent Behaviour **13** (2008), 222.
[31] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p.16.
[32] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p. 20.
[33] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p. 20.

who purchase images of child sexual abuse on the Internet, on average, seek images of younger children than those likely to be involved in contact offences.

Some offenders download thousands of images, but only view a small number of their favourites. The research found that 44% of the offender group collected fewer than 50 images, while 24% of the sample had collections of over 1,000 images and almost all of these were offenders at low risk of re-offending or of going on to commit contact offences. Two offenders had collections of over 30,000 images and one had a collection of over 80,000 images of child sexual abuse.[34] This contrasted with the study by McCarthy (2010) of US offenders, which found that contact offenders tended to have larger collections of child sexual abuse material compared with non-contact offenders. The average size of child sexual abuse images and videos for contact offenders was 3,400 compared to 860 for non-contact offenders. In the sample of offenders in McCarthy's study, the contact offender with the largest collection had 50,150 child sexual abuse images and videos, compared to the largest collection of a non-contact offender being 5,500. Non-contact offenders had vastly larger collections of adult pornography compared to contact offenders. However, both groups spent an average of 10 hours a week viewing child sexual abuse material.[35]

One researcher has postulated that there are offenders who are "cybersex addicts" who, owing to the habituation process of their addictive cycle, become bored with routine sexual themes. To this end, they seek to satiate their sexual desires by escalating their internet access gradually to sexually inappropriate material, including child sexual abuse material. The "cybersex addict" accesses child sexual abuse material because of poor impulse control and an insatiable sexual appetite. Combined, these factors can impel the addicted individual to spend a great number of hours downloading child sexual abuse material, which results in the possession of a significant number of images and video clips. Moreover, owing to the obsessive quality of their collecting, some addicts go on to divide their cache of child sexual abuse material into folders according to category (such as physical attributes or sexual content). Other researchers see this as "the collector syndrome", which involves the compulsive acquisition of child sexual abuse material for its own sake, rather then the careful selection of images based on inappropriate sexual arousal.[36]

Based on a sample of 100 offenders convicted of offences related to child sexual abuse material, Seto *et al.* (2006) found much greater levels of sexual arousal to sexualised images of children amongst contact offenders that accessed child sexual abuse material compared to non-contact offenders. Non-contact offenders were found to have a similar level of sexual arousal to sexualised images of children as general sexology patients, but higher than offenders who had committed sexual offences against adults.[37]

Those who purchase commercial child sexual abuse images have, on average, a higher level of education than contact offenders.

Treatment of those who purchase child sexual abuse images aims to stop further offending and prevent progression to contact offending.

---

[34] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p. 21.

[35] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 191.

[36] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 184.

[37] M. C. Seto, J. M. Cantor and R. Blanchard, *Child Pornography Offences Are a Valid Diagnostic Indicator of Pedophilia,* Journal of Abnormal Psychology **115(3)** (2006), p. 613.

The lower frequency of pro-offending attitudes and beliefs that serve to legitimise and maintain sexually abusive behaviours displayed by non-contact Internet offenders suggests that they may be unlikely to represent persistent offenders or potentially progress to commit future contact sexual offences. Similarly, a greater ability to empathise with victims may also contribute positively to Internet offenders' achievements in therapeutic interventions.[38]

The effectiveness of interventions with those who purchase child sexual abuse material is borne out by the lower reconviction rates of such offenders compared to contact offenders.[39] Seto and Eke (2005) found that in a three year period (April 2001 to April 2004) in a sample of 201 Canadian adult male offenders for child sexual abuse material offences the recidivism rate for non-contact offenders of a further offence related to child sexual abuse material was lower than for those who also had contact offences (3.9% compared to 5.3%). Those with only offences related to child sexual abuse material were far less likely to reoffend with a sexual contact offence than those with a past history of sexual contact offences (1.3% compared to 9.2%).[40]

By contrast, those who advocate for tougher penalties on Internet offenders as a means of deterring such offending behaviour, Beech *et al* (2008) argue social science evidence indicates that deterrence through increased penalties will not improve community protection.[41] Not one single review of controlled outcome research in criminal justice or corrections has found a large or consistent effect on reducing re-offending through variations in the type or severity of the criminal penalty.

3. Impact of Child Sexual Abuse on Law Enforcement Officials and the Judiciary

Practitioners counselling law enforcement officials and judiciary involved in the prosecution of offenders who access child sexual abuse material online report that the requirement to view such material in the investigation and prosecution of the case can have harmful impacts on those involved. The STOP Program in Christchurch has powerful footage of an interview with a police officer in Ireland who talked about not being able to get the screams of the child in the on-line material out of his head, they continued to haunt him.

The Australian Government needs to ensure that there are adequate support services for those required to view child sexual abuse material as a result of being involved in cases related to this offence.

4. Why is it reasonable to mandate ISPs to block unrestricted access to child sexual abuse material online?

Up until recently 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

[38] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Physchological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), pp. 87-88.
[39] J. Osborn, I.A. Elliott, D. Middleton and A.R. Beech, *The use of actuarial risk assessment measures with UK internet child pornography offenders*, J. of Aggression, Conflict and Peace Research **2(3)** (2010), p.16.
[40] M.C. Seto and A.W. Eke, *The Criminal Histories and Later Offending of Child Pornography Offenders,* Sexual Abuse: A Journal of Research and Treatment **17(2)** (2005), p. 207.
[41] A.R. Beech, I.A. Elliott, A. Birgden, and D. Findlater, *The internet and child sexual offending: A criminological review,* Aggression and Violent Behaviour **13** (2008), 226.

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. In the UK, British Telecom provides a filtered service at a wholesale level as well as on a retail basis. Filtering is undertaken using the Internet Watch Foundation list of URLs. Media reports suggest that the UK Government is considering extending the requirements on ISPs, requiring them to filter out all pornography, unless the consumer requests to have access to such material.[42]

The following information about the voluntary measures taken by ISPs in Canada and a number of Scandinavian countries has been provided publicly by the Australian Department of Broadband, Communications and the Digital Economy.[43]

In Canada, Cybertip.ca maintains and distributes to ISPs a list of URLs hosted outside of the country containing child sexual abuse material. Eight major ISPs in Canada voluntarily block the Cybertip.ca list, providing coverage to almost 90% of Canadian Internet subscribers.

In Denmark, 19 ISPs voluntarily participate in a scheme covering around 99% of Internet subscribers.

In Finland a majority of ISPs block client access to child sexual abuse material, with a 2007 law allowing them to do so. This covers around 80% of Internet users.

In Norway, approximately 15 ISPs (including all major ISPs) filter a list of child sexual abuse sites maintained by the National Criminal Investigation Service, covering around 95% of Norwegian Internet subscribers. Norway also requires all employers and management to take measures to prevent employees from downloading child sexual abuse material.[44]

In Sweden, approximately 15 ISPs voluntarily filter a Swedish list of child sexual abuse material, covering around 85% of Swedish internet subscribers.

In the US, Verizon, Sprint and Time Warner Cable decided to block access to child sexual abuse material on websites and bulletin boards. They also agreed to provide US$1 million to remove such sites. They agreed to do this after they were threatened with being charged with fraud and deceptive business practices by the New York Attorney General. The New York Attorney General had conducted an eight month investigation into the lack of action by ISPs to combat child sexual abuse material despite customer service agreements pledging to discourage such activity.[45] The US also requires public schools and libraries to take measures against child sexual abuse material on the Internet.[46]

The COSPOL Internet Related Child Abusive Material Project (CIRCAMP) is a European Commission-funded network of law enforcement agencies across Europe including Europol

---

[42] NewsCore, 'All internet porn will be blocked to protect children, under UK government plan', *Herald Sun,* 19 December 2010 (accessed online).
[43] Australian Government Department of Broadband, Communications and the Digital Economy, 'ISP Filtering – Frequently Asked Questions', http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/ accessed on 28 May 2010.
[44] W. Ph. Stol, H. W. K. Kaspersen, J. Keretens, E.R. Leukfeldt and A.R. Looder, *Filtering and blocking of child pornographic material on the internet. Technical and legal possibilities in the Netherlands and other countries,* Boom Juridische uitgevers, WODC, 2008, p. 5.
[45] 'US firms to block child sex sites', BBC, 10 June 2008 accessed at http://news.bbc.co.uk/2/hi/americas/7446637.stm on 14 June 2008.
[46] W. Ph. Stol, H. W. K. Kaspersen, J. Keretens, E.R. Leukfeldt and A.R. Looder, *Filtering and blocking of child pornographic material on the internet. Technical and legal possibilities in the Netherlands and other countries,* Boom Juridische uitgevers, WODC, 2008, p. 5.

and Interpol, has formulated the following primary aims of ISPs' domain-based filtering of pre-identified websites containing child-abusive material to:

1. prevent the revictimisation of children;
2. prevent the illegal distribution of material and the files;
3. prevent the illegal display of abuse material and reduce the harm to the general population while informing the public of the extent of the problem; and
4. prevent access to child abuse material and thus limiting the market, reducing the demand for new production.

The following countries are members of the CIRCAMP network: Norway, UK, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Malta, the Netherlands, Poland, Spain and Sweden.[47]

The European Union has launched a proposal (Article 18 in Proposal for an EU Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography) that suggests that:[48]

> *each member state shall take the necessary measures to enable competent judicial or police authorities to order or similarly obtain the blocking of access by internet users to internet pages containing or disseminating child pornography.*

In 2008 it was estimated that some 40 countries provide some level of filtering or blocking of the Internet.[49]

Recently Telstra, Optus and iPrimus have all agreed to voluntarily block their customers from accessing child sexual abuse material. They cover around 70% of internet users in Australia. The Unit notes that Yahoo! in their submission to this inquiry has stated that they use a combination of filters, algorithms, human review and customer complaints to identify child sexual abuse material. They have also removed known child sexual abuse URLs from the Yahoo! search index results.

The problem with such a voluntary approach means there will always be ISPs who will not agree to participate that provide an easy channel for those seeking to access and purchase child sexual abuse material online. It also sends a message that allowing clients to access child sexual abuse material is a voluntary business decision and creates a niche market for such clients.

We wrote to 30 Australian ISPs to ask what steps they took to prevent their clients from accessing child sexual abuse material and what assistance they gave to law enforcement to combat online child sexual abuse. Six replied by verbal conversations and Vividwireless replied in writing. Three indicated they supported Australian ISPs being required to block access to child sexual abuse materials. One said his company had been subjected to strong abuse and threats for supporting such requirements on ISPs. One had been part of the Government's trials and indicated that technically the blocking worked well and had no noticeable impact on internet access speed. One ISP stated they already block both RC and X rated material for all their clients and if clients want access to such material they need to go to other ISPs. Others indicated they provided a blocking service to the level requested by their clients (often companies). Vividwireless replied in writing to say that they were attempting to join Telstra, Optus and Primus in blocking client access to child sexual abuse

---

[47] M. Eneman, *Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness,* Journal of Sexual Aggression **16(2)**, (2010), pp. 223-224.

[48] M. Eneman, *Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness,* Journal of Sexual Aggression **16(2)**, (2010), p. 224.

[49] W. Ph. Stol, H. W. K. Kaspersen, J. Keretens, E.R. Leukfeldt and A.R. Looder, *Filtering and blocking of child pornographic material on the internet. Technical and legal possibilities in the Netherlands and other countries,* Boom Juridische uitgevers, WODC, 2008, p. 4.

material. All the conversations indicated that blocking was technical feasible, but the question was what the impact of doing so would be.

Naturally, the easiest way around Australian ISPs being required to block access to child sexual abuse material will be for a foreign ISP to provide access to such sites, as through a proxy site.[50] However, this is a common argument for not restricting Australian companies from engaging in transnational crime. The argument is that if Australian companies are restricted from participating in the transnational criminal activity (be it paying bribes or money laundering for example) foreign companies will continue to engage in these activities and it will have no net impact in reducing the criminal activity and only increase the costs on Australian businesses and their Australian customers.

Research suggests that a reasonable proportion of offenders access child sexual abuse material use the World Wide Web, with one study finding of a sample of such offenders, 78% obtained images using Internet Relay Chat software, 42% used the World Wide Web, 39% used newsgroups, 30% e-mail and 21% ICQ.[51] This sample included offenders who both shared images and those that purchased images.

In her consideration of ISP filtering through interviews with 15 convicted Internet offenders and the head of the Child Protection Team at the IT crime section within the Swedish National Criminal Police, Eneman (2010) concluded that:[52]

> *Although the filter mechanisms do not seem to hinder child pornographers who are intent upon accessing child abusive material, one could argue that the systems may have the effect of preventing potential offenders from starting to access such material. Regulation models that require extra steps for the users to gain access to child-abusive material may prevent people who may try to access this type of content based on curiosity. Such regulation could have a positive effect by limiting the market of child-abusive material.*

Further, Eneman (2010) argued blocking by ISPs reduces the display of child sexual abuse material and consequently reduces revictimisation of the abused child.[53] She summarised this issue as follows:

> *In the debate of internet filtering a significant amount of attention has been placed upon the issue of freedom of expression and privacy. Filtering is considered a serious threat to these civil liberties. Although they are important rights that should be protected, they need to be better balanced with other important liberties, such as the right of the child not to be sexually exploited or abused. Child-abusive material is documented evidence of the sexual exploitation of a child, and once the material is available on the internet it constitutes permanent revictimisation.*

The Philippines Republic Act No. 9775 *An Act Defining and Penalising the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes* contains an obligation for "All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered." Italy also has a legislative requirement on all ISPs to not provide access to their clients seeking to access child sexual abuse materials. The Italian police from the 'Centre against Child Pornography

---

[50] M. Eneman, *Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness,* Journal of Sexual Aggression **16(2)**, (2010), p. 231 found that in a sample of 15 offenders (11 of whom were also contact offenders) the majority used proxy servers to circumvent filtering in Sweden.

[51] A.R. Beech, I.A. Elliott, A. Birgden, and D. Findlater, *The internet and child sexual offending: A criminological review,* Aggression and Violent Behaviour **13** (2008), 226.

[52] M. Eneman, *Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness,* Journal of Sexual Aggression **16(2)**, (2010), p. 232.

[53] M. Eneman, *Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness,* Journal of Sexual Aggression **16(2)**, (2010), p. 232.

on the Internet' maintain a list of sites to be blocked, which is shared with ISPs who have six hours to block a site newly added to the list.

ISPs being required to take some responsibility in relation to what their clients access to help combat transnational criminal activity, such as child sexual abuse, is no different to the positive obligations that the Howard Government introduced on banks and other financial institutions to know their clients and report suspicious activity by clients who may be involved in transnational crime. In fact if a person known to be involved in the commercial child sexual abuse industry attempted to open an account with an Australian financial institution, the financial institution would be required to submit a suspicious activity report to AUSTRAC. This stands in stark contrast to ISPs being effectively required to do nothing to disrupt this criminal activity[54], even when they detect it, and being able to leave it entirely to law enforcement.

5. Requiring ISPs and other IT providers to report when they detect clients accessing child sexual abuse material

Currently Section 313 of the *Telecommunications Act 1997* requires carriers or carriage service providers to do their best to prevent telecommunication networks and facilities from being used in, or in relation to, the commission of offences of which the downloading or dissemination of child sexual abuse material would present such offences. Part 10.6, Subdivision E, Section 474.25 of the *Criminal Code Act* requires ISPs and internet content hosts to refer any detected child abuse material to the Australian Federal Police within a reasonable period of time. However, the current provision has not been enforced and there are those in the IT industry who do not believe that this provision requires them to report clients who they know are accessing child sexual abuse material. One ISP we spoke to said that he would not report any clients accessing child sexual abuse material as he feared prosecution for breach of privacy. Others expressed uncertainty about their conflicting obligations to protect the privacy of their clients against reporting any detected criminal activity by their clients in accessing child sexual abuse material to the appropriate authority. Both the Australian Crime Commission and the Australian Federal Police have complained that the IT industry do not adequately assist them through their failure to report online criminal activity (The Age 18/10/2010). In the case of the AFP, they publicly complained about the case where Facebook detected the activities of a child exploitation network and failed to report this network to law enforcement (AFP media release 27 August 2010).

These requirements have already been incorporated in Filipino law. Given the anecdotal evidence of Australians both assisting in the running of child sexual abuse businesses in the Philippines and of being customers of such businesses, it would be good if Australia could assist the Philippines in combating this transnational criminal activity by matching their laws. Section 9 of the Republic Act No. 9775 *An Act Defining and Penalising the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes* has the following requirements:

- "All internet service providers (ISPs) shall notify the Philippines National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person."

[54] While it might be argued Australian law requires the reporting of such activity when it is detected, the reality is that no ISP has ever been subjected to prosecution for failing to do so.

- “An ISP shall preserve such evidence for purposes of investigation and prosecution by relevant authorities.”
- “An ISP shall upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography.”

Section 11 of the Filipino law requires internet content hosts to “Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such internet address, to the proper authorities.”

Under US criminal law §2258A of USC Title 18 provides that any ISP that becomes aware of its servers being used to provide child pornography material must report that to national authority (the Cyber Tipline). ISPs must furnish as soon as possible a report that includes various information in relation to the identifying material of individuals who it is aware of that are registered as controlling the material. It also requires that ISPs provide the details of any other customers of theirs who access the material in the period prior to the material being taken down.

However, §2258A does expressly prohibit the ISPs from monitoring their customers, making it illegal to track customers for any length of time. This is largely a product of American concerns about the right to freedom of speech being impinged by ISPs being granted a broad-ranging right to monitor their customers.

Liability for breaching any of the rules of §2258A is set at a company level (in the form of fines), but individual directors or officers of companies cannot be criminally prosecuted unless it can be shown that they acted intentionally or recklessly.

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