Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

SUBMISSION TO THE HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON INFRASTRUCTURE AND COMMUNICATIONS INQUIRY INTO THE USE OF SUBSECTION 313(3) OF THE *TELECOMMUNICATIONS ACT 1997* BY GOVERNMENT AGENCIES TO DISRUPT THE OPERATION OF ILLEGAL ONLINE SERVICES

August 2014

Dr Mark Zirnsak
Director
Justice and International Mission Unit
Synod of Victoria and Tasmania
Uniting Church in Australia
Phone: +61-3-9251 5265
E-mail: mark.zirnsak@victas.uca.org.au

Executive Summary

The Synod of Victoria and Tasmania welcome this opportunity to make a submission to the inquiry by the House of Representatives Standing Committee on Infrastructure and Communications into the use of subsection 313(3) of the *Telecommunications Act 1997* by government agencies to disrupt the operation of illegal online services. This submission is focussed on urging the Committee recommend that the Australian Federal Police (AFP) be permitted to continue to use subsection 313(3) to require Australian Internet Service Providers (ISPs) to disrupt ready access to child sexual abuse material for sale online. The Synod strongly opposes a return to the situation where Australian ISPs were able to provide ready access to commercial child sexual abuse material online.

We completely agree with the Prime Minister that, "As a community we must have zero tolerance for the sexual abuse of children. Wherever abuse has occurred it must be tackled and it must be tackled vigorously, openly and transparently."[1] We strongly believe this also applies to children overseas who have been sexually abused and whose images have either been traded or purchased by Australians online. To that end, we welcome the statement by the Minister for Justice, the Hon Michael Keenan MP, on 30 July 2014 that "it is vital Australia's communication industry leaders assist law enforcement to detect and disrupt the darkest and most disturbing of criminal syndicates."[2]

The AFP having issued notices to ISPs under Section 313 of the *Telecommunications Act,* which requires Australian ISPs to disrupt access to child sexual abuse material using the INTERPOL domain list of the 'worst of' child sexual abuse material, means the vast majority (90%) of Australians using the internet are no longer able to readily access images of children being sexual abused on domains on the INTERPOL list. It is unlikely that this mechanism will ever achieve 100% coverage of Australian ISPs as there are an estimated 400 to 600 ISPs operating in Australia. However, only 97 of those have more than 1,000 clients. At the same time there are ISPs that made it publicly clear they will not disrupt their clients' ready access to child sexual abuse material unless forced to do so.

The Synod does not oppose subsection 313(3) being used by other parts of government to disrupt access to illegal online material, provided the nature of the material would justify such action, the disruption is well targeted to the illegal material and that it makes sense to use this tool for disruption. Disruption through subsection 313(3) would be best used to target online criminal activity that is severe and where there are a limited number of sites to be disrupted (in the hundreds, rather than in the tens of thousands). For example, the INTERPOL 'Worst of' list of child sexual abuse material ha around 400 domains on it at any one time. Too wide-scale use of this tool risks blocking sites and material not connected with the criminal activity.

Throughout this submission the terms 'child sexual abuse material' or 'child abuse material' will be used. This reflects the terminology used by those who work with survivors of online child sexual abuse and law enforcement. 'Child pornography' still appears in some international conventions and in early laws written to criminalise the material. Given the growing acceptance of pornography as a legitimate product in Western societies, the term 'child pornography' is now seen to offer some legitimacy to the material in question when it should be regarded as unacceptable and criminal. The term is also used by opponents of the full range of measures needed to remove this material.

[1] The Hon Tony Abbott MHR, Media Release, "The sexual abuse of children", 12 November 2012.
[2] The Hon Michael Keenan MP, Media Release, "Industry must play a role in fighting child online exploitation", 30 July 2014.

The commercial trade in images of child sexual abuse involves hundreds of commercial child sex abuse sites. An estimated 50,000 new child sexual abuse images are produced each year.[3] The industry is estimated to be worth about US$250 million globally.[4]

Organised criminals, mainly in Eastern Europe and increasingly in Asia, run 'businesses' selling images and videos of child sexual abuse online primarily to make money. The purchase and trade in commercial sexual abuse material generates a market and ongoing demand for abuse through the production of the material. Human trafficking particularly feeds the commercial child sexual abuse industry on the Internet.[5]

Children under the age of 18 who are used for commercial sexual purposes are deemed to be victims of human trafficking under the definition in the US *Victims of Trafficking and Violence Protection Act 2000*. The Act defines sex trafficking as "recruitment, harbouring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act."[6]

The commercial child sexual abuse industry is different to peer to peer networks of sex offenders who share images but do not seek to make a profit. The primary objective of the commercial industry is to sell images of child sexual abuse in order to make a profit. These commercial networks are more likely to involve younger children than peer to peer networks. In 2013, the UK Internet Watch Foundation found that 81% of the child victims on commercial child sexual abuse sites appear to be under 10 years old and 51% of the images and videos depicted sexual activity between adults and children including the rape and sexual torture of the child.[7]

The supply chain for child sexual abuse material entering Australia involves the following links:

- The producers of the child sexual abuse material, be it photos or video;
- The content host, that makes the material accessible online;
- The Internet Service Provider that allows the customer to access the material;
- The offender purchasing the material; and
- The body or bodies that provide the payment system that allows the producer to get paid for the material.

Actions can be taken against each link in this supply chain. In each case, counter strategies are available to offenders to try and circumvent actions to combat the commercial child sexual abuse trade.

In the same way that measures are being increasingly called for in relation to other goods that are imported and that involve human trafficking or forced labour in their production, a softer approach should not be adopted simply because the products of this abuse are sold online.

The actions that can be taken at each step in the chain are:

- **Producers**
    - Assist in the identification and location of those involved in the production so that law enforcement in the country they are located in can arrest and prosecute them.

[3] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[4] [i]bid.
[5] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[6] Catherine Marcum and George Higgins, *Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces,* Policing **5(4)**, p. 310.
[7] Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6.

  - Assist in the identification and location of their victims, so the victims can be rescued.
- **Content Hosts**
  - Enforce the offence of knowingly hosting child sexual abuse material.
  - Ensure that URLs and domains that have been used by commercial child sexual abuse operations are deregistered and cannot be used again.
  - Support the development of new technologies, such as Microsoft's Photo DNA, that are being used to remove known images of child sexual abuse material.
- **Internet Service Providers**
  - Enforce the offence of knowingly providing service to child sexual abuse material.
  - Require disruption of access to child sexual abuse sites through the mandatory requirement to block ready access based on a URL or domain list of child sexual abuse sites and domains, as is currently the case using subsection 313(3) of the *Telecommunications Act 1997*.
  - It may also be possible to disrupt access to child sexual abuse material through filters that use the filehash value of the images.
- **'Customers'**
  - Enforcement of existing offences for possession and trading in child abuse material.
  - Explore catered rehabilitation programs for non-contact offenders where there are sufficient numbers to justify such programs to reduce recidivism.
  - Provision of a help service for offenders who recognise they have a problem and wish to seek help in ending their offending behaviour. This can be advertised through the 'Stop' message tied to ISP level access disruption.
- **Payment Providers**
  - Deny the provision of credit card merchant facilities to any commercial child sexual abuse material provider.
  - Financial institutions to work with the Financial Coalition Against Child Pornography to identify known transaction patterns that would indicate a client is purchasing child sexual abuse material.

Scale of the problem

As of October 2011 five Australian ISPs were already working with the Australian Federal Police to block ready access to a limited list maintained by INTERPOL of child sexual abuse sites.[8] Telstra is one of those ISPs. Between 1 July 2011 and 15 October 2011 Telstra blocked 84,000 attempts by Australians to access the child sexual abuse domains on the list.

Impact of existing efforts

A combination of the above measures globally has already been yielding detectable results in removing commercial child sexual abuse material. According to the UK Internet Watch Foundation, the average length of time child sexual abuse images are hosted has been reduced from years to just days[9] as a result of the above measures. The webpage blocking list maintained by the Internet Watch Foundation now typically contains 600 URLs at any one time, down from 1,200 in 2008.[10] Further, in 2006 the common subscription price to commercial child sexual abuse sites was $30 a month. Today, due to the combination of efforts to shut down and disrupt these criminal enterprises, it is not unusual to find sites that cost up to $1,200 per month and it is rare to find sites charging less than $100 per month.[11]

[8] Senate Standing Committee on Legal and Constitutional Affairs. Australian Federal Police Question No 25.
[9] Internet Watch Foundation, '2010 Annual and Charity Report', p. 1.
[10] http://www.iwf.org.uk/resources/trends
[11] International Centre for Missing and Exploited Children and National Centre for Missing and Exploited Children, 'Financial Coalition Against Child Pornography Backgrounder', July 2011, p. 2.

Recommendations

1. Allow the AFP to continue to use subsection 313(3) of the *Telecommunications Act 1997* to require Australian ISPs to have to disrupt ready access to child sexual abuse material.
2. Extend the existing list of domains to be disruption from the INTEROPOL 'Worst of' list to include URLs disrupted by the UK Internet Watch Foundation. While the INTERPOL list only involves the sexual abuse of children under the age of 13, the Internet Watch List covers material involving the sexual abuse of older children which is more closely in keeping with 'child pornography' offences in Australian law.
3. Publicly report on an annual basis the number of times access to known child sexual abuse was blocked by each Australian ISP that has been subject to a section 313 requirement to do so.
4. If possible, use Section 313 of the *Telecommunications Act 1997* to require search engine providers to stop providing search results for terms that are clearly connected with child sexual abuse material for any search engine provider who refuses to do so voluntarily. Progress on this issue has been made by the UK Government threatening to legislate on the issue.
5. Actively promote where Australians should report inadvertent encounters with child sexual abuse material online to, to assist in the maintenance of an up-to-date list of sites and domains of child sexual abuse material to be subject to access disruption.

Table of Contents

1. Overview of the Online Child Sexual Abuse Industry

The commercial trade in child sexual abuse images involves hundreds of commercial child sex abuse sites. An estimated 50,000 new child sexual abuse images are produced each year and the industry is estimated to be worth about US$250 million globally.[12] Reportedly a single child sexual abuse site can attract up to one million hits monthly.[13] The purchase and trade in commercial sexual abuse material generates a market and ongoing demand for the human rights abuses that are involved in the production of the material.

The UN Office of Drugs and Crime (UNODC) have found the majority of commercial child sexual abuse operations are located in Eastern Europe. This is due to lower levels of law enforcement in Eastern Europe targeting this criminal activity and because the customers, who are largely from Western countries, have a preference for 'white' girls.

Commercial websites tend to cater to a specific group of offenders. They often have higher levels of extreme sexual abuse and sexual torture of children than images on non-commercial sites. Images are grouped in specific or narrow age ranges including categories for infants and toddlers, although this was a minority.[14] Just under a third of the images (29.7%) 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.

Trend data from the UK Internet Watch Foundation has found, disturbingly, the proportion of images of victims of child sexual abuse under the age of 10 increased from 74% in 2011 to 81% in 2012 and 2013.[15] In 2013 3% of the images detected by the Internet Watch Foundation involved the sexual abuse of children aged two or under.[16] At the same time the proportion of images of child sexual abuse showing sexual activity between adults and children including rape and sexual torture decreased from 64% of images in 2011 to 53% of images in 2012 and 51% of images in 2013.[17]

Children under the age of 18 who are used for commercial sexual purposes are deemed to be victims of human trafficking under the definition in the US *Victims of Trafficking and Violence Protection Act 2000*. *The Act* defines sex trafficking as "recruitment, harbouring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act."[18]

Offenders accessing child sexual abuse material use a variety of online methods. One study found, of a sample of offenders, 78% obtained images using Internet Relay Chat software, 42% used the World Wide Web, 39% used newsgroups, 30% e-mail and 21% ICQ.[19] This sample included offenders who both shared images and those that purchased images, so it

[12] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[13] R. Wortley, Child Pornography. In: Natarajan M, editor. *International crime and justice*. USA: Cambridge University Press, 2010, p.178-84, cited in J. Pritchard et.al, 'Internet subcultures and pathways to the use of child pornography', *Computer Law and Security Review* 27, 2011, p.589
[14] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 41.
[15] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6.
[16] Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6.
[17] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 11; and Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6.
[18] Catherine Marcum and George Higgins, *Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces,* Policing **5(4)**, p. 310.
[19] 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.

was not restricted only to offenders that purchase images from commercial child sexual abuse operations.

The UK Internet Watch Foundation report the make-up of the top 10 types of websites on which child sexual abuse material is hosted are:

- Image host (45%)
- Banner site (12%)
- Social networking site (12%)
- Generic websites (10%)
- File host (6%)
- Image Store (5%)
- Image Board (4%)
- Forum (3%)
- Web archive (2%)
- Blog (< 1%)

Commercial sites also rely on selling to a large number of customers, as this allows the sale price to be lower. It also means more revenue can be obtained for each image and the risk of detection and apprehension by law enforcement is reduced, as the production of each image involves greater risk of being caught by law enforcement. The Internet Watch Foundation report 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.[20]

Since 2009, the Internet Watch Foundation identified 998 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, 440 were active in 2011 and 513 were active in 2012. Of the 513 commercial child sexual abuse brands active in 2012 that were detected by the Internet Watch Foundation, 268 were new brands.[21] 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. Within the top 30 brands, no new 'top level' brand was identified in 2011.[22] They found of the top 30 most prolific 'brands' of commercial child sexual abuse material active in 2012, 16 of these appeared to be associated with a single 'top level' distributor.[23] Of the 9,550 child sexual abuse webpages detected by the Internet Watch Foundation in 2012, 2,587 (27%) were commercial sites.[24] In 2013 24% of child sexual abuse images detected by the Internet Watch Foundation that were being sold on a commercial basis.[25]

[20] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[21] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 16.
[22] Internet Watch Foundation, '2011 Annual and Charity Report', p. 15.
[23] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 16.
[24] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 16.
[25] Internet Watch Foundation, 'Internet Watch Foundation Annual & Charity Report 2013', p. 6.

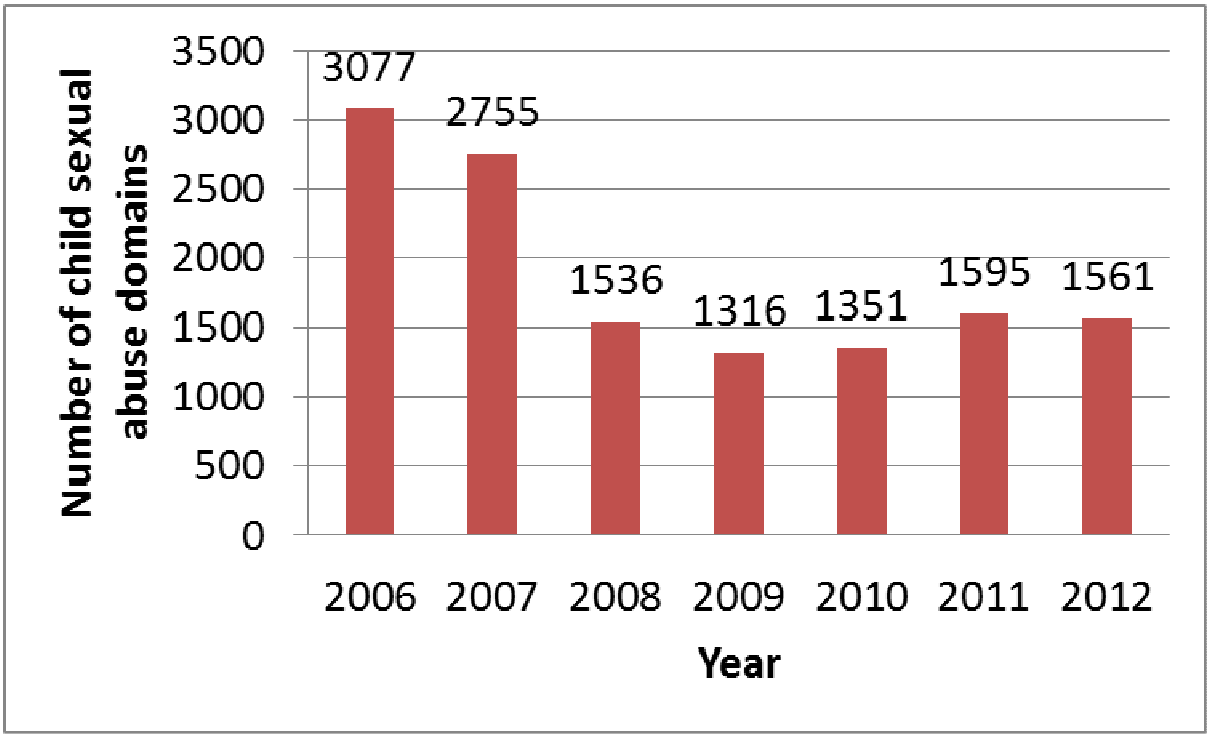

Figure 1. Number of child sexual abuse domains detected by the UK Internet Watch Foundation 2006 – 2012.[26]

The Internet Watch Foundation reports that in the last two years they have seen an increasing number of legitimate websites being criminally exploited to host child sexual abuse material.[27]

The UK Internet Watch Foundation reported in 2012 there were 26 URLs of child sexual abuse material hosted within hidden services. This is achieved through the use of proxy software that conceals the location of the web server hosting the content, making removal of the content at source impossible.[28]

The sites are also supported by a range of payment methods to help avoid detection.[29] 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. A report by Cybetip.ca identified 27 different payment types.[30] The majority (85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (an average of $53 a month). Membership could also be obtained for a one-time fee ranging from $30 to $1,990[31] with an average cost of $249.[32] DVDs were also sold for as much as $1,900. Other products include

[26] Internet Watch Foundation, '2011 Annual and Charity Report', p. 12; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012'.
[27] Internet Watch Foundation, '2011 Annual and Charity Report', p. 13.
[28] Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 17.
[29] Analysis by the Internet Watch Foundation (Annual and Charity report p.8) 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.
[30] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 10, 56.
[31] This type was used by 15.4% of the sites.
[32] Canadian Centre for Child Protection, *op.cit*. p. 65.

a variety of packages, image sets, videos and websites.[33] They concluded there is clearly a large consumer market for child sexual abuse images.

A UK commercial online child sexual abuse operation was estimated to have made £2.2 million through the distribution of millions of images. Their pages contained 121,654 images of child sexual abuse. Police were able to identify 1,511 suspected customers of the criminal operation.[34]

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 indirectly profit from the sale of child sexual abuse images.[35]

In addition, the Internet Watch Foundation reported in 2011 they had discovered a cluster of commercial (and some non-commercial) sites that can only be accessed via a predetermined 'digital path'. These 'disguised websites' present different content based on the route the user takes. When the URL is loaded directly into a browser, the page that loads usually contains legal adult content. However, if the same website is accessed via a particular gateway (referrer), the site displays child sexual abuse images. This technique means a commercial child sexual abuse operator may be able to acquire legitimate business services, such as banking services, if the website appears to host legal content when directly accessed. It also means that if the site is reported to law enforcement without the person reporting it also reporting the path to the illegal content, it will appear to be a false report to the law enforcement agency. The Internet Watch Foundation have developed a technique to circumvent the digital 'footpath' to gain access to the child sexual abuse content. The Internet Watch Foundation detected the use of this technique on 579 occasions during 2011.[36]

Whilst there is an emerging market it in Asia, it is predominantly in western countries where the market exists. According to the available data,[37] hundreds of thousands of people in western democratic societies access child sexual abuse material online either inadvertently or deliberately. In a 2008 survey of 1,000 adults in the UK, the Internet Watch Foundation found that 5% of all internet users had been exposed to child sexual abuse material online.[38] 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. [39] At the time, BT provided service to one third of UK internet users. Cybertip.ca also reported 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.[40] There is little reason to believe the situation

[33] DVDs accounted for 5.8% of the sites, packages 4.7%, image sets 3.1%, videos 1.1% and websites 0.2%.
[34] Child Exploitation and Online Protection Centre, "Operation Alpine: Four main suspects sentenced today", 13 June 2011; and "Three jailed over £2.2 million internet child porn business", The Daily Mirror, http://www.mirror.co.uk/news/uk-news/three-jailed-over-22million-internet-134758.
[35] Canadian Centre for Child Protection, *op.cit*, p. 56.
[36] Internet Watch Foundation, '2011 Annual and Charity Report', p. 15.
[37] Most ISPs that voluntarily block ready 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.
[38] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research
[39] http://news.bbc.co.uk/1/hi/uk/4687904.stm
[40] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 16.

in Australia is any different. Between 1 July 2011 and 15 October 2011 Telstra blocked 84,000 attempts by Australians to access the child sexual abuse domains on the list.[41]

The Asia-Pacific Financial Coalition Against Child Pornography report that Cybertip are receiving more complaints about online child sexual abuse material from within the Asia-Pacific region. In addition, Cybertip is reporting that the Electronic Service Provision (ESP) industry is becoming far more active in reporting matters related to online child sexual material (see Table 1)

Table 1. Public versus ESP reports to the Cybertip line 2006 to 30 September 2012.

Year	2006	2007	2008	2009	2010	2011	2012
Public	44,419	69,414	68,869	58,498	69,280	70,623	48,703
ESP	32,165	35,847	33,160	61,055	154,094	250,339	219,974
Total	76,584	105,261	102,029	119,547	223,374	320,962	268,677

Operation Centurion was triggered after a hacker infiltrated a respectable European website and inserted 99 degrading and explicit images of young girls from eastern Europe, the US and Paraguay. The site was then subject to 12 million hits in just 76 hours after word got around online networks that the images were available and the website's address was circulated. Almost 150,000 different computer users from 170 countries accessed the otherwise obscure website, including Australians using 2,883 computer IP addresses. Of those, 1,513 had downloaded one or more images in the 76-hour period.[42]

US CyberTipline refers attempts to access child sexual abuse images to law enforcement agencies. Between 2006 and 2010 the US CyberTipline made 3,113 child sexual abuse material referrals to Australian law enforcement agencies, compared to 289 to Hong Kong, 603 to New Zealand, 1,765 to Thailand and 5,658 to Japan.[43] Between 2006 and June 2012 7,015 referrals were made to Australian law enforcement agencies.

Table 2. CyberTipline referrals of attempts by Australians to access child sexual abuse material online 2006 – 2012.

Year	2006	2007	2008	2009	2010	2011	2012*	Total
Number of Referrals	198	228	306	517	1,676	2,760	1,330	7,015

* 1 January – 25 June 2012

The available data suggests Australians are also significant consumers of online child sexual abuse material. In the 2013-2014 financial year the Australian Communications and Media Authority conducted more than 7,600 individual investigations into child sexual abuse material based on complaints.[44]

As an example of Australians buying child sexual abuse material from commercial providers, in mid-November 2013 a joint police operation across borders busted a Canadian commercial child sexual abuse business making and selling 9,000 ‘movies’ and more than 350,000 images of abuse. The business had revenues in excess of $4 million. The Toronto owner of the business was arrested by Canadian police. Sixty-five Australian customers of the site were arrested by Australian police and 399 charges were laid against them. In addition 386 children globally were rescued from exploitation.

[41] Senate Standing Committee on Legal and Constitutional Affairs. Australian Federal Police Question No 25.
[42] Tom Allard, “Child sex abuse: Centurion's shocking fact file”, *The Sydney Morning Herald*, 5 June 2008, http://www.smh.com.au/articles/2008/06/05/1212258967845.html.
[43] International Centre for Missing and Exploited Children,’ Financial Coalition Against Child Pornography. Building a Global Network’, Visa Security Summit, Jakarta, Indonesia, 24 May 2011.
[44] ACMA Media Release, ‘Dramatic rise in child sexual abuse material investigations’, 18 July 2014.

The US administration has weighed into the Australian debate and stated that it opposes access disruption. However, the majority of child sexual abuse sites are hosted in the US. Cybertip.ca in Canada found the top five countries where URLs were registered for commercial child sexual abuse material were:[45]

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

Cybertip.ca found 80% of child sexual abuse sites hosted in Poland were commercial sites.[46]

The UK based Internet Watch Foundation also found 49% of URLs were hosted in North America, 43% in Russia and 8% in Asia. Only one site was found to be hosted in Australia.[47] There was a drop in the proportion of URLs hosted in Asia from 17% in 2010 to 8% in 2011.

The commercial child sexual abuse industry is very small compared to the vast amount of legal adult pornography on the Internet. A study in 2006 estimated the number of webpages containing the keyword 'porn' was 88.8 million, those containing the keyword 'XXX' numbered 181 million and those with the keyword 'playboy' numbered 43.2 million.[48] The UNODC estimates there are only several thousand commercial child sexual abuse websites at any one time. This makes maintaining a block list of such sites an achievable objective.

INTERPOL manages the International Child Sexual Exploitation Image Database (ICSE DB), which was launched in March 2009. The ICSE DB contains more than 500,000 images of child sexual abuse and is available to certified investigators in any member country in order for them to analyse and share data with colleagues in other countries. By the end of 2009, 1,453 child abuse victims had been identified and rescued worldwide based on the information contained in the ICSE DB.[49] Most victims remain unidentified.

[45] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 11.
[46] Ibid. p. 62.
[47] Internet Watch Foundation, '2011 Annual and Charity Report', p. 13.
[48] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p. 15.
[49] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, pp. 61-62.

2. Understanding the Consumers of Child Sexual Abuse Material

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.[50]

A UK study of internet sex offenders revealed a diverse group but one in which well-educated men in employment in non-manual jobs were over represented.[51] A further study described the typical adult engaged in online sexual abuse was a married male and professional in their early thirties.[52]

Offenders who access child sexual abuse material do not appear as sophisticated as is often assumed. The UNODC commented 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 more sophisticated consumers could have evaded detection. However, such statistics serve as a warning that simply because a counter-strategy is technologically available does not mean all offenders will avail themselves of the strategy.

2.1 The differences between contact and non-contact offenders

Research points to distinct typologies of offenders who access child sexual abuse material on the internet including 'contact' and 'non-contact' offenders. Non-contact offenders purchase and access child sexual abuse material online but do not engage in contact (actual physical sexual abuse) offences themselves. Many of these offenders first experience child sexual abuse material online accidentally. Further, many 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. Contact offenders commit physical sex offences against children and in addition may access, trade in or purchase child sexual abuse material online.

There are four basic psychological mechanisms. If any are dysfunctional, this may result in sex offences against children.[53] The pathways are as follows:

- Intimacy deficits (individuals offend during a time of social isolation or rejection).
- Distorted sexual scripts (individuals have cognitive distortions that guide sexual behaviour).
- Emotional dysregulation (individuals have difficulties regulating mood and emotions).
- Anti-social cognitions (individuals have general pro-criminal attitudes and beliefs and their offending reflects this).

There are further sub-typologies of offenders in both the contact and non-contact groupings, such as:[54]

- Periodically prurient offenders. Those who access images out of impulsivity or curiosity perhaps as part of a broader interest in pornography (not necessarily specifically related to children).

[50] 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.
[51] C. Atkinson & D. Newton, Online Behaviours of adolescents: Victims, Perpetrators and Web 2.0*, Journal of Sexual Aggression*, March 2010, Vol. 16, No. 1, p. 109
[52] Ibid. p. 110
[53] Kerry Sheldon, *What we know about men who download child abuse images,* British Journal of Forensic Practice **13(4)** 2011, p. 225.
[54] Kerry Sheldon, *What we know about men who download child abuse images,* British Journal of Forensic Practice **13(4)** 2011, pp. 224-225.

- Fantasy-only offenders. Those who access/ trade images to fuel a sexual interest in children who have no known history of contact sexual offending.
- Direct victimisation offenders. Those who use online technologies for offending both in a contact and non-contact way, such as downloading pornography and grooming children online with the intention of committing a later contact sex offence.
- Commercial exploitation offenders. Those who produce or trade images for financial gain rather than a sexual interest in children per se.

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).[55] This study highlighted many of the differences in behaviour of contact and non-contact offenders. She found the contact offenders were more likely than non-contact offenders to masturbate to child sexual abuse material.[56] She found that 36% of non-contact and 53% of contact offenders traded in child sexual abuse material.[57] 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 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.[58]

Nielssen *et al.* (2011) studied a sample of 52 Australian offenders detected by police online.[59] They found only 25% of the offenders had associated with other offenders.[60]

McCarthy noted 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.[61] Professor David Middleton of De Mountford University found only around 10% of offenders who download child sexual abuse material online went on to commit actual child sexual abuse themselves.[62]

Non-contact offenders tend to justify their offending behaviour by distancing themselves from the very act they are viewing. The internet facilitates this distancing as well as justifying a view that they are not sex offenders themselves. They are then able to justify continued access to child sexual abuse material believing they are not directly responsible for the harm and are simply a passive viewer.[63] For example in the view of one offender, “Having sexual

[55] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 186.
[56] Ibid. p. 186
[57] Ibid. p. 186
[58] Ibid. pp. 189-190.
[59] O. Nielssen, J. O’Dea, D. Sullivan, M. Rodriguez, D. Bourget and M. Large, *Child pornography offenders detected by surveillance of the Internet and by other methods,* Criminal Behaviour and Mental Health **21** (2011), p. 215.
[60] Ibid., p. 219
[61] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 193.
[62] 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.
[63] 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.

thoughts and fantasies about a child isn't all that bad because at least it is not really hurting the child".[64] Another offender stated:[65]

> *"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:[66]

> *"…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:[67]

> *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.[68] 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".[69]

Non-contact offenders morally disengage with their behaviour by dehumanisation (viewing the image as a sexual commodity), displacement or diffusion of responsibility (placing the responsibility onto the producers), and disregarding the consequences (perceiving the likelihood of detection on the internet to be minimal).[70]

A number of studies that have found that offenders who access child sexual abuse material, but do not themselves commit contact offences against children, are a significant proportion of those offenders accessing material online. McCarthy also found that contact offenders were more likely to purchase child sexual abuse material (36%) compared to non-contact offenders (29%).[71]

Briggs *et al* (2011) argued the internet has enabled unique forms of deviant sexual behaviour. They distinguished two sub groups of offenders – contact-driven offenders who use the internet for grooming victims with the intention to meet and fantasy driven offenders who use the internet as a sexual medium for the purpose of cybersex and masturbation. Contact driven offenders they argued were younger and most had never been married. In

---

[64] Ibid. 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.
[65] 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.
[66] Ibid. p. 132.
[67] Ibid. p. 132.
[68] Ibid. p. 129.
[69] Ibid. p. 130.
[70] Kerry Sheldon, *What we know about men who download child abuse images,* British Journal of Forensic Practice **13(4)** 2011, p. 228.
[71] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.

contrast fantasy driven offenders were older, more likely to be employed and were either married or divorced prior to arrest.[72]

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.[73]

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.[74] 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.[75]

Research has even found different sexual responses between contact and non-contact offenders. 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.[76]

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.[77] 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.

Those offenders with emotional dysregulation problems were described as lacking control during periods of strong negative mood states, which then coupled with deviant sexual desire

[72] Briggs et. Al, An exploratory study of Internet-initiated Sexual offences and the chat room sex offender: Has the internet enable a new typology of sex offender?, *Sexual Abuse, A journal of research and treatment*, Vol 23, no. 3, 2011, p. 22
[73] 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.
[74] 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.
[75] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 183.
[76] 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.
[77] 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.

could lead to the use of pornography (in this case child sexual abuse material) as a mood alleviating strategy.[78] For some offenders, but not all, accessing images on the Internet may function as a way of avoiding or dealing with difficult emotional states.

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.[79] 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.[80]

Offenders 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.[81]

2.2 How the Online Environment Makes Accessing Child Sexual Abuse Material Easier

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.[82]

The anonymity of the online environment has a powerful disinhibiting effect on users purchasing child sexual abuse images. Without face-to-face communication, offenders are able to normalise their activities and legitimate their orientations and behaviours.[83] 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.[84]

Winder and Gough (2010) detail the behaviour of an offender who justified his behaviour through the inconsistency of laws globally to combat child sexual abuse, arguing what he did would have (erroneously) been legal in Japan.[85] Another offender argued that children in poverty overseas being photographed naked for money was better than them starving.[86]

---

[78] 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.
[79] 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),** July 2010, p.16.
[80] 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),** July 2010, p. 20.
[81] 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),** July 2010, p. 20.
[82] 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.
[83] Ibid. p. 78.
[84] 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.
[85] Ibid. p. 131.
[86] ibid, pp. 131-132.

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."[87]

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.[88] Access disruption may provide a check on these cybersex addicts by reminding them the material they are accessing and collecting is illegal.

2.3 Non-Contact Offenders are easier to rehabilitate

The effectiveness of interventions with non-contact offenders is borne out by the lower reconviction rates of these offenders compared to contact offenders.[89] Seto and Eke (2005) conducted a study of a sample of 201 Canadian adult male offenders for child sexual abuse material offences. They found that in a three year period (April 2001 to April 2004) the recidivism rate for non-contact offenders was lower than for those who also had contact offences (3.9% compared to 5.3%). Those with only offences related to viewing child sexual abuse material were far less likely to reoffend with a contact offence than those with a past history of sexual contact offences (1.3% compared to 9.2%).[90] A Swiss study of 231 offenders, for an average of 7.5 years, found only 11 went on to commit another offence, of which only two involved physical contact with a child.[91] Webb *et al.* (2007) examined 73 offenders related to child sexual abuse material and found only 4% failed to adhere to the

[87] 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.
[88] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 184 and O. Nielssen, J. O'Dea, D. Sullivan, M. Rodriguez, D. Bourget and M. Large, *Child pornography offenders detected by surveillance of the Internet and by other methods,* Criminal Behaviour and Mental Health **21** (2011), 221.
[89] 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.
[90] 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.
[91] J. Endrass, F. Urbaiok, L.C. Hammermeister, C. Benz, T. Elbert, A. Lauerbacher and A Rossegger, *The Consumption of Internet child pornography and violent sex offending,* BMC Psychiatry **9** (2009), p. 43.

conditions of community supervision and none were charged with new offences during 18 months of supervision.[92]

This lower rate of recidivism amongst non-contact offenders and their ability to be persuaded to empathise with the victims of the abuse they are viewing, points to the value of access disruption by ISPs. Use of a block message provides an educative moment to challenge the cognitive distortions of the non-contact offender. Informal discussions with law enforcement officials who work to combat child sexual abuse online indicate that education of offenders and potential offenders is a vital tool. However, to our knowledge there are no wide scale education campaigns targeting this group. While the Australian Federal Police are engaging with academia and non-government organisations on the issue of offender education, they are not currently engaged in any education program specifically targeted at online offenders.[93]

With the right message on a 'stop' page that pops up when an attempt is made to access child sexual abuse material 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 International Telecommunications Union highlighted the educative value of block pages when a list is used by ISPs to disrupt the commercial child sexual abuse industry online:[94]

> *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.*

If ISP level access disruption is implemented a message would pop up letting the viewer know that they were trying to access illegal content. This serves as an educational moment for offenders. Research has shown that many offenders who buy child sexual abuse material (but who do not physically abuse children themselves) believe they are doing nothing wrong because access to such material is not challenged. Because there is ready availability of such material on the Internet, this view is reinforced. Access disruption challenges this view.

The 'stop' page may also refer to them to services where they can seek help. There are certainly examples of offenders who have sought assistance to address their accessing of child sexual abuse material, without having been detected by law enforcement officials.[95]

---

[92] L. Webb, J. Craissati and S. Keen, *Characteristics of Internet child pornography offenders: A comparison with child molesters*, Sexual Abuse **19** (2007), pp. 449-465.
[93] Senate Estimates Hansard, Assistant Commissioner Neil Gaughan, Australian Federal Police, 18 October 2011.
[94] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 29.
[95] Olav Nielssen, Jeremy O'Dea, Danny H Sullivan, Marcelo Rodriguez, Dominique Bourget and Matthew M Large, *Child pornography offenders detected by surveillance of the Internet and by other methods*, Criminal behaviour and mental health 21(3) 2011, pp. 215-224

3. The Impact on Victims of On-line Child Sexual Abuse

Research has consistently identified the serious and long-lasting effects of sexual assault on children. However, when the abuse is on-line these effects are significantly exacerbated.[96] For victims, knowing the image of their abuse is being viewed over and over again means that they are being re-victimised time and time again. They feel shame and intense feelings of powerlessness knowing there is nothing they can do about others viewing indecent pictures of themselves indefinitely.[97]

Victims of sexual abuse can also suffer psychiatric disorders relating to anxiety, post-traumatic stress disorder, mood and substance abuse. These may lead to other issues such as post-traumatic stress disorders, cognitive disorders, emotional pain, avoidance behaviours, low-self-esteem, guilt, self-blame, delinquency, substance abuse, vulnerability to repeated victimisation, interpersonal difficulties, dissociation and disbelief about the abuse, functional amnesia and effects on relationship with others.[98]

A study of 100 victims whose sexual abuse was recorded by the perpetrator found victims reported that initial feelings of shame and anxiety did not fade but intensified to feelings of deep despair, worthlessness and hopelessness. Their experience provided them with a distorted model of sexuality, and many had particular difficulties in establishing and maintaining healthy emotional and sexual relationships.[99]

A German study looking at the impact on victims who presented for counselling concluded working with victims of online sexual abuse is much more complex as they display different symptoms than other traumatized children. The number of unreported cases of online child sexual abuse is also higher than unreported cases of child sexual abuse that take place offline.[100] Cases went unreported for a number of reasons including:

- Children being confronted with the permanence of the abusive images which led to feelings of helplessness;
- Their fear of organised crime; and
- Worrying about the consequences such as their computer being confiscated

In most cases the existence of the abusive images made it much easier for the parents to believe their children. It was also felt that parents were more likely to prosecute in order to have the images destroyed than in cases of 'mere' child sexual abuse due to feelings of anger, being horrified and public humiliation. In some cases victims were still being blamed by professionals within the criminal justice system. An account was given of a judge who when looking at a picture of a 15 year old boy said it seemed he had participated willingly.[101]

Many perpetrators insist on the children smiling and appearing to enjoy themselves because it relieves the guilt of the people who purchase the images and allows them to rationalise that

[96] Child Sexual Abuse Prevention Program (CSAPP Inc) Submission to the Joint Select Committee on Cyber Safety Inquiry into Cyber safety, No 107, p. 3
[97] C. Atkinson & D. Newton, Online Behaviours of adolescents: Victims, Perpetrators and Web 2.0, *Journal of Sexual Agression*, March 2010, Vol. 16, No. 1, p. 109
[98] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p.34.
[99] R. Wortley and S. Smallbone, 'Child Pornography on the Internet', Problem-Oriented Guides for Police – Problem-Specific Guides Series, no. 41, US Department of Justice, Office of Community Oriented Policing Services, Washington, USA, 2006.
[100] J. von Weiler, A. Haardt-Becker, S. Schulte, Care and Treatment of child victims of child pornographic exploitation, Journal of Sexual Aggression, June 2010, 16, 2, p.214
[101] Ibid., p.216

they really did not harm the child. This causes a great deal of confusion for counsellors, caretakers and law enforcement. [102]

It also often ensures the child's silence. One therapist recounted a case of a child who was tickled just as the photos were taken. Thus she always looked like she was having fun. She was then told that she obviously liked it, so she had better never tell.[103]

The Australian Institute of Family Studies released a report on 5 February 2013 on *The long-term effects of child sexual abuse*. The report found child sexual abuse has significant lifelong negative impacts for survivors, affecting their behaviour, relationships, mental health and physical health, and increasing their likelihood of addiction. A piece in *The New York Times* related the story of a girl who had been sexually abused by her father who then distributed the images on the internet. She was harassed by a man who had viewed the material and suffered from paranoia, nightmares, had trouble concentrating at school and found it difficult to make friends.[104]

In 2009 the International Telecommunications Union (ITU) issued their *Guidelines for Policy Makers on Child Online Protection.* They pointed out:[105]

> *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.[106] 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]."[107]

The online environment is catering for markets who view images of very young children. Professionals agree that children cannot yet fully grasp the implications of the permanency of their abuse.[108] The damage will therefore be ongoing.

---

[102] Ibid. p.216
[103] Ibid. p.217
[104] Emily Bazelon, 'The Price of a Stolen Childhood', *The New York Times*, 24 January 2013.
[105] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 19.
[106] Ibid., p. 27.
[107] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 28.
[108] J. von Weiler, A. Haardt-Becker, S. Schulte, Care and Treatment of child victims of child pornographic exploitation, Journal of Sexual Aggression, June 2010, 16, 2.

4. Australia's Human Rights Obligations to Combat Commercial Child Sexual Abuse Material

The role of the Internet and other new technologies in facilitating more readily human rights abuses and transnational criminal activity has been receiving growing recognition globally. For example, the resolution of the UN Human Rights Council A/HRC/8/L.17 of 12 June 2008 called 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.*

Australia has obligations to combat transnational criminal activity under the *United Nations Convention against Transnational Organized Crime (UNTOC)*. Under this Convention Australia has obligations to ensure that Australian businesses do not profit from transnational criminal activity. Article 2 of UNTOC defines "Proceeds of Crime" as "any property derived from or obtained, directly or indirectly, through the commission of an offence". By this definition, videos and images produced through the use of human trafficking and forced sexual exploitation should be considered proceeds of crime, along with any revenue derived from such videos and images. Article 12 of UNTOC requires that States Parties take legal steps to confiscate the proceeds of crime and to identify and trace the proceeds of crime.

Australia has obligations to combat human trafficking as a States Party to, amongst a number of treaties:

- the *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children of the United Nations Convention against Transnational Organized Crime* (known as the Palermo Protocol);
- The *UN Convention on the Rights of the Child* (Article 35); and
- The *UN Convention on the Elimination of All Forms of Discrimination Against Women* (Article 6).

Child sexual abuse materials are also prohibited by a number of human rights treaties Australia has signed up to. These include Article 34 of the *UN Convention on the Rights of the Child,* the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* and ILO Convention No 182 on the Elimination of the Worst Forms of Child Labour.

The submitting bodies note that the UN Committee on the Rights of the Child noted the limited manner in which corporations can be held liable for acts or omissions related to child sexual abuse material under Australian law and recommended that legislation be amended to remedy this deficiency.[109]

[109] UN Committee on the Rights of the Child, "Consideration of reports submitted by States parties under article 12, paragraph 1, of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Concluding observations: Australia", CRC/C/OPSC/AUS/CO/1 19 June 2012, p. 5.

5. Take Down Notices

Global efforts are being made to have child sexual abuse material removed when it is detected. Law enforcement and regulatory authorities in different countries collaborate to issue 'take down' notices to content hosts to remove child sexual abuse material. The Australian Communication and Media Authority (ACMA) already issues such notices to content hosts for content hosted in Australia. The content must generally be taken down by 6 pm the next business day. Failure to comply may result in the commission of an offence. The ACMA has reported that it has had complete industry compliance with its actions to remove such content.[110]

The Canadian Cybertip.ca has received close to 25,000 reports resulting in 2,800 websites being shut down, at least 30 arrests and the removal of a number of children from abusive environments.[111]

The UK Internet Watch Foundation has reported 50% of all non-UK hosted child sexual abuse URLs occurs within 10 days of detection. When the content of hosted by an Internet Watch Foundation member, 85% is removed within 10 days and 95% within 13 days.[112]

An assessment commissioned by the UK Internet Watch Foundation concluded:[113]

> *There is compelling evidence that domestic notice and takedown systems adopted in some countries are beneficial in effectively removing child sexual abuse content at source without compromising the simultaneous capture of evidence necessary to investigate and prosecute offenders.*

However, the Financial Coalition Against Child Pornography reports "Bulletproof Hosting" is being used to defeat the system of take down notices. These hosts promise customers their websites will not be taken down, regardless of complaints or content. Bulletproof hosts use a combination of distributed services to maintain uptime for their customers. Specific tactics they use include:[114]

- Registering the domain name with a registrar with relaxed enforcement. Depending on the location and enforcement policies, some registrars are used more heavily than others for illicit activities.
- Sharing and shuffling IP addresses to minimise downtime if particular IPs are shut down. This ensures content remains up while being indifferent to the status of particular domains. Instead of relying on one IP, bulletproof hosting relies on multiple IPs that can keep the content up independent of specific IP shut downs.
- Using a standardised yet specific naming methodology for name servers to minimise service interruption.
- Soliciting business and communicating with customers using unmonitored, private media. Bulletproof hosts frequently advertise their services on message boards frequented by their target customer base. From there, e-mail, instant messaging and other non-public options are used to further business dealings. This allows bulletproof

[110] Australian Law Reform Commission, 'Classification – Content Regulation and Convergent Media', ALRC report 118, February 2012, p. 291.
[111] Kim-Kwang Raymond Choo, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' Australian Institute of Criminology Research and Public Policy Series 103, 2009, p. 70.
[112] Internet Watch Foundation, "2011 Annual and Charity Report", pp. 5, 16.
[113] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, p. 2.
[114] Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011, pp. 12-13.

hosting services to remain largely underground and reduces exposure to enforcement entities.

- Collecting payment using unregulated payment services to limit scrutiny and preserve anonymity. The use of small payment processors originating from outside the US is popular due to lax regulatory environments and lessened cooperation with law enforcement agencies.

Cybertip.ca has made recommendations for content hosts 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 sexual abuse website, and potentially rescuing children from ongoing sexual abuse.[115]
- 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-known to consumers of child sexual abuse images, steps need to be taken to remove them permanently from circulation.[116]

Research from other jurisdictions suggests a minority of people report even the worst types of material. As noted earlier, 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.[117] 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.

In 2012, UK Internet Watch Foundation found 40% of people said they would not know where to report child sexual abuse material online if they encountered it, while 12% said they would simply ignore it.[118] The survey of 2,058 adults in the UK found 4% of men and 2% of women had inadvertently accessed child sexual abuse material online.[119]

[115] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 48.
[116] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 49.
[117] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research
[118] Internet Watch Foundation, 'New study reveals child sexual abuse content as top online concern and potentially 1.5m adults have stumbled upon it', http://www.iwf.org.uk, 18 March 2013.
[119] Internet Watch Foundation, 'New study reveals child sexual abuse content as top online concern and potentially 1.5m adults have stumbled upon it', http://www.iwf.org.uk, 18 March 2013.

6. ISP Access Disruption

The use of access disruption by ISPs is a key tool in the global effort needed to effectively stem the production of child sexual abuse images and prevent victims being re-victimised.

ISP access disruption is supported by the international police organisation INTERPOL. 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.*

ISP level access disruption limits the commercial child sexual abuse industry's ability to build their customer base, thus reducing demand for the production of such material.

ISP access disruption of child sexual abuse material is technically feasible, as demonstrated by a number of European countries in which ISPs already do so and through the Australian ISPs that are working with the Australian Federal Police to already do so.

The Synod of Victoria and Tasmania would support ISP level access disruption being extended to all forms of sexual abuse, not just sexual abuse involving children. For example, it would be desirable to disrupt access to online games that allow players to earn points and upgrade to higher-levels by attacking and raping sexy female cartoon characters. In one game the victim of the brutal rape game is a young Japanese girl drawn in the anime style, who is blindfolded and tied to a chair.[120] The Australian Institute of Criminology cited psychiatrist Dr Ang Yong Guan who argues allowing children to play such rape games will cause them to grow up with warped values and will negatively impact on their value system. He also argued it may affect their emotional growth.

Permitting access to sexual abuse material further violates the rights of victims. Victims who have pictures of their abuse online suffer extreme feelings of powerlessness and are 're-victimised' each time the image is viewed. While it is desirable to locate and remove such images whenever possible, often it is very difficult. Blocking ready access to sexual abuse material blocks inadvertent access and disrupts deliberate attempts to access such images and protects the rights of victims not to have their images viewed.

ISPs should not be allowed to profit from clients engaged in criminal activity, such as accessing and downloading child sexual abuse material. ISPs need to take reasonable steps to disrupt the ability of their customers to freely use their service for criminal activity. There are other products imported into Australia where slavery of human trafficking may have been involved in their production, such as cocoa, cotton and seafood. For these products it is difficult to detect if they have been produced with human rights abuses. By contrast, there is no dispute about the human rights abuses involved in the production of child sexual abuse material.

ISP level access disruption to sexual abuse material does not replace the role of education of both parents and minors and the need for parents to assist their children in safe use of the online environment. It does provide some level of a safety net to inadvertent access to sexual abuse material where these other measures are not adequately in place.

---

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

ISP level access disruption to child sexual abuse material in other democracies is done on a targeted list of URLs (such as the UK Internet Watch Foundation, who currently have a list of around 600 URLs at any one time updated twice a day) or domains (as per the INTERPOL list, with around 400 at any one time, updated weekly). This method provides very targeted disruption. Most user side filters Australians would be familiar with work on analysis-based filtering, which employ key words, image analysis, file type, link analysis, reputation and deep packet inspection criteria to analyse content.[121] Analysis-based filtering often results in over-blocking (restricting access to more content than is intended).

Access disruption of commercial child sexual abuse sites cannot be done on IP address. Cybertip.ca noted that some of the child sexual abuse sites use the counter-strategy of 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 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.[122] This renders any system that would attempt to block access to child sexual abuse sites on the basis of IP addresses ineffective.

There is also an ability to disrupt on the filehash values of child sexual abuse images of which the Microsoft Photo DNA technology outlined the previous section is an example. Each image has a unique filehash value and it is possible to block the transmission of images where the filehash value is known. This can be used to disrupt peer-to-peer transmission of images. Currently this technology is used by law enforcement to reduce the number of images they need to view when they catch an offender. The offenders collection of images is run against a database of filehash values of known child sexual abuse images. This means only images not currently in the database must be viewed by police officers. The use of this technology may assist in combating commercial operations that have moved to more individualised sale of images than from a website. It is unlikely to have much impact in deterring networks of contact offenders who will seek counter strategies to defeat it, given their committed sexual interest in children. However, the technology could be adapted to be used as a detection technology to identify offenders trading in known child sexual abuse images for investigation, arrest and prosecution.

In the Australian Government's response to the UN Committee on the Rights of the Child in their review of Australia's compliance with the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* the Government stated:

> *As part of a national strategy under the auspices of the Australian and New Zealand Police Advisory Agency (ANZPAA) Child Protection Committee, work is progressing on the trial of internet technology that aims to reduce the flow of child exploitation material across the internet within Australia. This technology utilises the known hash values of offending images as a means of identifying inappropriate content being exchanged on peer to peer networks. Work is also progressing on the introduction of the national Child Exploitation Tracking System (CETS), which will enable seizures of child exploitation material to be analysed and compared against known holdings.*

[121] Australian Law Reform Commission, 'Classification – Content Regulation and Convergent Media', ALRC report 118, February 2012, pp. 248-249.
[122] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 62-63.

Google has also developed a way of 'tagging' child sexual abuse videos so that they can be identified and removed.

6.1 The International Criminal Police Organisation (INTERPOL)

The INTERPOL 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 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".[123] As of 25 October 2011 the INTERPOL 'worst of' list contained 409 domains.[124]

INTERPOL requires that all the domains on the list be 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 the domain administrator 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 who 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 blocking access to child sexual abuse material also has additional benefits:

> *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*

[123] http://www.interpol.int/Public/THBINternetAccessBlocking/
[124] Senate Standing Committee on Legal and Constitutional Affairs. Australian Federal Police Question No 25.

> *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.*

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.*

6.2. Other Support for Access Disruption

In their extensive review of classification of media content in Australia, the Australian Law Reform Commission (ALRC) has recommended ISPs be required to disrupt access to 'Prohibited Content' which includes child sexual abuse material.[125] The ALRC suggested that particular subcategories of Prohibited content could be prioritised in ISP access disruption, particularly actual child sexual abuse and non-consensual sexual violence.[126]

The International Telecommunications Union recognises the place of ISP blocking of ready access to child abuse material as one important tool in the fight against such material: [127]

> *Blocking access to web sites and Usenet Newsgroups containing CAM [Child Abuse Material] 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.*

On 15 October 2010 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*

[125] Australian Law Reform Commission, 'Classification – Content Regulation and Convergent Media', ALRC report 118, February 2012, Recommendation 5-7 pp. 12, 286, 379.
[126] Ibid. p. 297.
[127] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009.

> *other appropriate proactive measures – to identify and remove illegal content (involving the sexual exploitation of children) from the Internet.*

On 4 November 2011 the European Parliament issued a directive on combating the sexual abuse and sexual exploitation of children and child pornography.[128] Article 25(2) states:

> *Member States may take measures to block access to webpages containing or disseminating child pornography towards the internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.*

While expressing concern about the inappropriate use of blocking on the internet by Governments seeking to stifle legitimate freedom of expression, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, stated:[129]

> *"child pornography is one clear exception where blocking measures can be justified, provided that the national law is sufficiently precise and there are effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body."*

Further, he later went on to state:[130]

> *"The Special Rapporteur considers that child pornography constitutes an act of violence against children and an offence to their human dignity, which provokes more violence against children. Moreover, the victim's privacy must be protected and appropriate protection measures and care adapted to the needs and characteristics of children must be available."*

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:[131]

> *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.[132] 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*

---

[128] European Parliament, 'Directive of the European Parliament and of the Council on combating sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA', PE-CONS 51/11, 4 November 2011.
[129] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", UN Human Rights Council, 16 May 2011, p. 10.
[130] "Promotion and protection of the right to freedom of opinion and expression", UN General Assembly, 10 August 2011, p. 8.
[131] 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.
[132] Ibid. p. 232.

documented evidence of the sexual exploitation of a child, and once the material is available on the internet it constitutes permanent revictimisation.

The COSPOL Internet Related Child Abusive Material Project (CIRCAMP) is a European Commission-funded network of law enforcement agencies across Europe including Europol and Interpol. It has formulated the following primary aims of ISPs' domain-based filtering of pre-identified websites containing child-abusive material to:

1. prevent the re-victimisation 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.[133]

The European NGO Alliance for Child Safety Online (eNACSO) campaigns for governments to introduce mandatory requirements on ISPs to disrupt client access to 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

In Australia, the following non-government organisations have indicated support for requiring ISPs to disrupt ready access to child sexual abuse material:

1. Adults Surviving Child Abuse
2. Anglican Archdiocese of Adelaide
3. Anglican Diocese of Gippsland
4. Anglican Diocese of Wangaratta
5. Australian Childhood Foundation
6. Australian Christian Churches Victoria
7. Australian Christian Churches WA
8. Australian Christian Lobby
9. Australian Youth Affairs Coalition
10. Baptist Churches in SA
11. Baptist Churches Western Australia
12. Baptist Union of Victoria
13. Bravehearts Inc
14. Catholic Diocese of Ballarat
15. Catholic Diocese of Broken Bay
16. Child Abuse Consultancy Education and Training Global
17. Childwise
18. Churches of Christ in Australia

[133] 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.

19. Collective Shout
20. Communications Law Centre
21. Crime Victims Support Association
22. Human Rights Law Centre
23. International Social Service Australia
24. Justice and Peace Office, Catholic Archdiocese of Sydney
25. NAPCAN
26. National Child Protection Alliance
27. National Children's and Youth Law Centre
28. National Council of Churches in Australia
29. National Council of Jewish Women Australia (Vic)
30. NSW & ACT Baptist Churches
31. Office for Justice and Peace, Catholic Archdiocese of Melbourne
32. Plan International
33. Project Futures
34. Salvation Army, Southern Territory
35. Sisters of St Joseph
36. Starfish Ministries
37. STOP THE TRAFFIK Australia
38. The Freedom Project
39. Trades Hall Victoria
40. UNICEF Australia
41. Uniting Church in Australia, Synod of NSW and ACT
42. Uniting Church in Australia, Synod of SA
43. Uniting Church in Australia, Synod of Victoria and Tasmania
44. World Vision Australia

6.3 ISP Level Access Disruption Growing Globally

Access disruption to online child sexual abuse material is gaining momentum in democratic countries, as its value as a tool in the fight against such material gains recognition.

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 to "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 material. The Italian police from the 'Centre against Child Pornography 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. Germany has passed a similar law but is yet to implement it.

In the UK, the Internet Watch Foundation reports that its 76 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.[134]

During 2010 there were a total of 14,602 webpages that featured on the UK Internet Watch Foundation blocking list of live child sexual abuse content. In 2011 this number decreased to 12,966 URLs, hosted in 39 countries.[135] An average of 59 webpages were added to the list each day in 2010, 45 new URLs were added each day in 2011 and 37 new URLs were added each day in 2012, reflecting the speed at which child sexual abuse content moves

[134] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4; and Internet Watch Foundation, '2011 Annual and Charity Report', p. 17.
[135] Internet Watch Foundation, '2011 Annual and Charity Report', pp. 12-13.

online location.[136] The webpage blocking list now typically contains 580 URLs at any one time, down from 1,200 in 2008.[137] They update their list twice a day.[138] The Internet Watch Foundation report their entire operation ran on a budget of just £1 million ($1.5 million) per annum between 2009 and 2011.[139]

The Internet Watch Foundation reported that in 2011 and 2012 it did not receive a single complaint from content owners concerned that they had included in their URL list legitimate content.[140] This demonstrates that it possible to maintain a highly dynamic block list without legitimate content being mistakenly placed on the list.

The Internet Watch Foundation has also publicly announced they are examining the feasibility of extending their operations globally to become Internet Watch Foundation International. This would include offering their URL block list to ISPs internationally.[141]

The Unit urges that the Australian Government seek to extend ISP level access disruption to all the online child sexual abuse sites contained on the UK Internet Watch Foundation, using the UK Internet Watch Foundation list as well as the INTERPOL domain list.

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.[142]

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.[143]

---

[136] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4; Internet Watch Foundation, '2011 Annual and Charity Report', p. 17; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 21.
[137] Internet Watch Foundation, '2011 Annual and Charity Report', p. 17; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 21.
[138] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[139] Internet Watch Foundation, '2010 Annual and Charity Report', p. 16; and Internet Watch Foundation, '2011 Annual and Charity Report', p. 22.
[140] Internet Watch Foundation, '2011 Annual and Charity Report', p. 20; and Internet Watch Foundation, 'Internet Watch Foundation Annual and Charity Report 2012', p. 21.
[141] Internet Watch Foundation Strategic Plan 2012-2015.
[142] 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.
[143] 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.

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.[144] The US also requires public schools and libraries to take measures against child sexual abuse material on the Internet.[145]

Both South Africa and Japan require ISPs to disrupt customer access to child sexual abuse material.[146] In 2008, French ISPs reached an agreement with the French Government to disrupt access to child sexual abuse material.[147]

6.4 Problems with leaving it to ISPs to voluntarily disrupt access

Implementing access disruption to child sexual abuse material online should not be a voluntary decision by ISPs. There will always be ISPs who will not agree to participate. This then provides 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.

The Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church in Australia 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. All the conversations indicated access disruption by ISPs was technical feasible.

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 through a proxy site.[148] 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. However, building a cultural norm that criminal activity has no place in business activities must start with some companies or some countries being willing to take a stand and not participate in the criminal activity. Over time work must be done to bring more countries and more companies into the fold of those that refuse to be part of criminal activity.

---

[144] '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.
[145] W. Ph. Stol, et al. *op.cit*, p. 5.
[146] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, p. 73.
[147] Weixiao Wei, 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation, p. 73.
[148] 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.

Some online businesses have demonstrated they cannot be relied upon to deal with child sexual abuse material even when they become aware of it. Amazon initially defended their online sales of the how-to manual for sex with children '*The Pedophile's Guide to Love and Pleasure*' under the banner of being opposed to censorship.[149]

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.[150]

[149] See for example Helen Popkin, "Amazon defends 'Pedophile's Guide'', 11 October 2010, http://www.msnbc.msn.com/id/40112145/ns/technology_and_science-tech_and_gadgets/t/amazon-defends-pedophiles-guide/
[150] The Age 18/10/2010 and AFP media release 27 August 2010.

7. Disrupting Searches for Child Sexual Abuse Material

UK Prime Minister David Cameron has put pressure on Google, Bing (owned by Microsoft) and Yahoo to stop assisting people trying to access images of child sexual abuse, “There are some searches which are so abhorrent and where there can be no doubt whatsoever about the sick and malevolent intent of the searcher that there should be no search results returned at all…. I simply don’t accept the argument that some of these companies have used to say that these searches should be allowed because of freedom of speech.”

Google and Microsoft have given in to the pressure and will introduce software to block 100,000 search terms that are clearly used only to find child sexual abuse material online. They will also stop the auto-complete feature from prompting users with child sexual abuse search terms even if the person was not looking for them. A further 13,000 search terms linked with child sexual abuse will flash up with warnings to users that the content could be illegal, and pointing them towards help. Google and Microsoft cover 95% of users.

These measures will also cover Australian users. We urge the Australian Government to actively support the requirement that searches for child sexual abuse material be disrupted and that Section 313 of the *Telecommunications Act 1997* might be used for this purpose if search engine providers refuse to implement these measures voluntarily.

Prime Minister David Cameron stated the UK National Crime Agency will monitor the effectiveness of the new technology introduced by Google and Microsoft and “If the search engines are unable to deliver on their commitment to prevent child abuse material being returned from search terms used by paedophiles. I will bring forward legislation that will ensure it happens.”

8. Arrest and Prosecution

Arrest and prosecution of those producing and consuming child sexual abuse material is believed to deter others seeking to access such material. It is a vital tool in the struggle against online child sexual abuse material, but it alone cannot be relied upon as the only response. As the Virtual Global Taskforce of law enforcement agencies has stated many times "law enforcement cannot prosecute itself out of the online sexual exploitation of children alone."[151]

In short, arrest and prosecution activities by the AFP do not remove the need for the use of subsection 313(3) to require Australian ISPs to disrupt ready access to known child sexual abuse material.

There are no Australian studies publicly available about the number of Australians accessing child sexual abuse material, nor the trend in these numbers. Therefore, it is impossible to provide any comment on how effective arrest and prosecution is in deterring consumption of child sexual abuse material. The UNODC report suggests that law enforcement efforts may be catching as little as 1% of all consumers of child sexual abuse materials worldwide.[152] It is expected that the AFP would be doing much better than that.

Arrest and prosecution data are likely to be more indicative of the resources made available to law enforcement to combat this criminal activity, rather than an indication of the number of consumers of child sexual abuse material. In the 2010 – 2011 financial year, law enforcement in Australia charged 112 offenders with offences related to the possession, production or supply of child sexual abuse material.[153] Table 2 outlines prosecution for use of a carriage service for child pornography material or child abuse material, with the data for prosecutions from the Commonwealth Director of Public Prosecution.[154] This does not include additional prosecutions at State and Territory level. The submitting bodies note the current difficulty of trying to collect arrest and prosecution data across States and Territories, as demonstrated by the Commonwealth's own difficulty in trying to provide the data this year to the UN Committee on the Rights of the Child for their review of Australia's implementation of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.*

Table 3. Prosecutions in Australia for use of a carriage service for child pornography material or child abuse material.

Financial Year	2005/2006	2006/2007	2007/2008	2008/2009	2009/2010
Number of Convictions	2	31	48	126	136
Number of Convictions per million people	0.1	1.5	2.3	6.0	6.2

In the data provided in 2012 to the UN Committee on the Rights of the Child:

- Victoria reported 393 offences in the 2009 – 2010 financial year related to possessing or making child sexual abuse material, but no data was provided on the number of offenders involved;

[151] Virtual Global Taskforce Media Release, 'VGT Board of Management Meeting Communique: September 2011', 26 September 2011, http://www.virtualglobaltaskforce.com/
[152] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[153] http://www.afp.gov.au/media-centre/fact-stats/online-child-sex-offences.aspx
[154] Commonwealth Director of Public Prosecutions submission to the Joint Select Committee on Cyber-Safety inquiry into Cyber Safety, 2010, p. 5.

- Western Australia reported 173 files were received in 2011 that related to child sexual abuse material and 28 offenders were arrested. 107 of the files are still under investigation.
- South Australia reported 339 offences related to child sexual abuse material and 205 cases being finalised in SA criminal courts, with a conviction rate of 49.3% for the 2009-2010 financial year.
- NSW reported 81 convictions in 2010 for offences related to production, dissemination or possession of child sexual abuse material.

Table 3 provides a comparison with the UK, for the years the Unit has been able to find data for.[155] However, the UK data includes convictions for taking, making, distributing, showing, possessing, or publishing any advertisement conveying the distribution of indecent photographs, both online and by other means. The vast majority of these offences are for online activities.

Table 4. Number of convictions related to child sexual abuse material in the UK.

Year	2001	2002	2003	2004	2005
Number of Convictions	364	531	1287	1162	1296
Number of Convictions per million people	7.0	10.2	24.8	22.4	24.9

The 1,296 convictions in the UK in 2005 for the publication, possession or distribution of obscene matter and indecent photographs of children, were 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.[156]

In the US, the number of suspects referred to US attorneys for offences related to child sexual abuse material increased from 169 (0.65 per million people) in 1994 to 2,539 (8.5 per million people) in 2006.[157] Convictions increased from 156 (0.6 per million people) in 1994 to 1,150 (3.8 per million people) in 2006.[158] By 2006, of the offenders sentenced for offences involving child sexual abuse material, 97% were for online offences. Further 95% of the offences involved depictions of children under the age of 12.[159]

In 1998, the US established the Internet Crimes against Children Task Force Program, which has led to the arrest of approximately 17,000 individuals and has had the largest increase in arrests (988%) compared to all law enforcement agencies across the US.[160] An evaluation of the Program found that its effectiveness increased with more trained personnel dedicated to computer forensic examinations.[161]

[155] Yaman Akdeniz, 'Internet Child Pornography and the Law', Ashgate Publishing Limited, Surrey, UK, 2008, p. 25.
[156] 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.
[157] Mark Motivans and Tracey Kyckelhahn, *Federal Prosecution of Child Sex Exploitation Offenders, 2006,* US Bureau of Justice Statistics Bulletin, December 2007, p.1.
[158] Ibid. p. 6.
[159] Ibid. p.6.
[160] Catherine Marcum and George Higgins, *Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces,* Policing **5(4)**, p. 312.
[161] Ibid., p. 314.

There is a need for the preservation of evidence in the investigation of cases involving online child sexual abuse. As noted by the Australian Institute of Criminology:[162]

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

Arrest and prosecution alone is not an adequate response to online sexual abuse material, given the low estimates of the proportions of offenders accessing such material that actually get caught and in the absence of any data demonstrating the level of deterrent effect current arrest and prosecution efforts are having. Further, arrest and prosecution is highly resource intensive. Thus, any educative or disruption measure that deters even a small proportion of offenders from continuing their offending behaviour is likely to be cost effective by comparison to traditional law enforcement.

The Federal Government has increased resources to law enforcement to combat online child sexual abuse. As part of the cybersafety plan, $49 million of $125.8 million announced in the 2008-2009 budget was allocated for 91 additional Australian Federal Police officers in the Child Protection Operations Team.

Due to the size of the problem and limited resources by comparison, police usually catch offenders who download child sexual abuse material after they have built substantial collections. UK research found that 56% of a sample of 72 offenders who had been caught collected more than 50 images, while 24% of the sample had collections of over 1,000. Two offenders had collections of over 30,000 images and one had a collection of over 80,000 images of child sexual abuse.[163] McCarthy's (2010) study of US offenders who had been caught found the average size of collections 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 offender with the largest collection had 50,150 child sexual abuse images and videos. This again points to the need for interventions that address offending or potential offending behaviour earlier.

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.[164]

---

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

[163] 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.

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

9. References

Abbott, Tony, Media Release, "The sexual abuse of children", 12 November 2012.

ACMA Media Release, 'Dramatic rise in child sexual abuse material investigations', 18 July 2014.

Akdeniz, Y., *Internet Child Pornography and the Law*, Ashgate Publishing Limited, Surrey, UK, 2008.

Allard, T., "Child sex abuse: Centurion's shocking fact file", *The Sydney Morning Herald*, 5 June 2008, http://www.smh.com.au/articles/2008/06/05/1212258967845.html.

Atkinson C. & D. Newton, 'Online Behaviours of adolescents: Victims, Perpetrators and Web 2.0'*, Journal of Sexual Aggression*, March 2010, Vol. 16, No. 1.

Australian Federal Police, http://www.afp.gov.au/media-centre/fact-stats/online-child-sex-offences.aspx

Australian Law Reform Commission, 'Classification – Content Regulation and Convergent Media', ALRC report 118, February 2012.

Avina, J., 'Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility', *Journal of Financial Crime* Vol 18, No.3, 2011, pp. 282-291.

Bazelon, Emily, 'The Price of a Stolen Childhood', *The New York Times*, 24 January 2013.

BBC, 'US firms to block child sex sites', 10 June 2008, accessed at http://news.bbc.co.uk/2/hi/americas/7446637.stm on 14 June 2008.

Beech, A.R., I.A. Elliott, A. Birgden, and D. Findlater, 'The internet and child sexual offending: A criminological review'*, Aggression and Violent Behaviour,* 2008, Vol 13, No 226.

Briggs et. al, 'An exploratory study of Internet-initiated Sexual offences and the chat room sex offender: Has the internet enable a new typology of sex offender?', *Sexual Abuse, A journal of research and treatment*, Vol 23, No. 3, 2011.

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

Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Commonwealth Director of Public Prosecutions', submission to the *Joint Select Committee on Cyber-Safety inquiry into Cyber Safety*, 2010.

Child Exploitation and Online Protection Centre, "Operation Alpine: Four main suspects sentenced today", 13 June 2011.

Child Sexual Abuse Prevention Program (CSAPP Inc) Submission to the *Joint Select Committee on Cyber Safety Inquiry into Cyber safety*, No 107.

Choo, Kim-Kwang Raymond, 'Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences' *Australian Institute of Criminology Research and Public Policy Series*, 2009, No. 103.

Elliott, I.A., 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, 2009, No.* 21

Endrass, J., F. Urbaiok, L.C. Hammermeister, C. Benz, T. Elbert, A. Lauerbacher and A Rossegger, *The Consumption of Internet child pornography and violent sex offending,* BMC Psychiatry **9** (2009).

Eneman, M., 'Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness'*, Journal of Sexual Aggression*, 2010, Vol 16, No.2

Financial Coalition Against Child Pornography, 'Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography', 1 February 2011.

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

International Centre for Missing and Exploited Children,' Financial Coalition Against Child Pornography. Building a Global Network', Visa Security Summit, Jakarta, Indonesia, 24 May 2011.

International Centre for Missing and Exploited Children and National Centre for Missing and Exploited Children, 'Financial Coalition Against Child Pornography Backgrounder', July 2011.

International Telecommunications Union, *Guidelines for Policy Makers on Child Online Protection*, 2009.

Internet Watch Foundation, http://www.iwf.org.uk/resources/trends

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

Internet Watch Foundation, *2010 Annual and Charity Report*.

Internet Watch Foundation, *2011 Annual and Charity Report*.

Internet Watch Foundation, *Internet Watch Foundation Annual and Charity Report 2012*.

Internet Watch Foundation, *Internet Watch Foundation Annual & Charity Report 2013.*

Internet Watch Foundation, 'New study reveals child sexual abuse content as top online concern and potentially 1.5m adults have stumbled upon it', http://www.iwf.org.uk, 18 March 2013.

Internet Watch Foundation Strategic Plan 2012-2015.

INTERPOL, http://www.interpol.int/Public/THBINternetAccessBlocking/

Keenan, Michael, Media Release, "Industry must play a role in fighting child online exploitation", 30 July 2014.

Marcum, C., and G. Higgins, 'Combating Child Exploitation Online: Predictors of Successful ICAC Task Forces*', Policing* **5(4)**, pp. 310-316.

McCarthy, J., 'Internet sexual activity: A comparison between contact and non-contact child pornography offenders', *Journal of Sexual Aggression*, 2010, No. 16, Vol 2.

Middleton, D., 'From Research to Practice: The Development of the Internet Sex Offender Treatment Programme (i-SOTP)', *Irish Probation Journal*, Sept 2008, No. 5.

Middleton, D., 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, 2009 Vol 15, No. 1.*

Motivans, M., and T. Kyckelhahn, 'Federal Prosecution of Child Sex Exploitation Offenders, 2006', *US Bureau of Justice Statistics Bulletin*, December 2007.

Nielssen, O., J. O'Dea, D. Sullivan, M. Rodriguez, D. Bourget and M. Large, 'Child pornography offenders detected by surveillance of the Internet and by other methods', *Criminal Behaviour and Mental Health* **21(3),** 2011, pp. 215-224.

Osborn, J., I.A. Elliott, D. Middleton and A.R. Beech, 'The use of actuarial risk assessment measures with UK internet child pornography offenders', *Journal of Aggression, Conflict and Peace Research,* 2010, Vol 2, No. 3.

Popkin, H., "Amazon defends 'Pedophile's Guide'', 11 October 2010, http://www.msnbc.msn.com/id/40112145/ns/technology_and_science-tech_and_gadgets/t/amazon-defends-pedophiles-guide/

"Promotion and protection of the right to freedom of opinion and expression", UN General Assembly, 10 August 2011.

"Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", UN Human Rights Council, 16 May 2011.

Senate Standing Committee on Legal and Constitutional Affairs. Australian Federal Police Question No 25.

Seto, M.C., and A.W. Eke, 'The Criminal Histories and Later Offending of Child Pornography Offenders', *Sexual Abuse: A Journal of Research and Treatment, 2005, Vol 17, No. 2.*

Sheldon, K., 'What we know about men who download child abuse images', *British Journal of Forensic Practice* **13(4)** 2011, pp. 221-234.

Stol, W. Ph., 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.

UN Committee on the Rights of the Child, "Consideration of reports submitted by States parties under article 12, paragraph 1, of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Concluding observations: Australia", CRC/C/OPSC/AUS/CO/1, 19 June 2012.

UN Office on Drugs and Crime, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*, 17 June 2010.

Virtual Global Taskforce Media Release, 'VGT Board of Management Meeting Communique: September 2011', 26 September 2011, http://www.virtualglobaltaskforce.com/

Webb, L., J. Craissati and S. Keen, 'Characteristics of Internet child pornography offenders: A comparison with child molesters', *Sexual Abuse* **19** (2007), pp. 449-465.

Wei, W., 'Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System', UK Internet Watch Foundation.

von Weiler, J., A. Haardt-Becker, S. Schulte, 'Care and Treatment of child victims of child pornographic exploitation', *Journal of Sexual Aggression*, June 2010, Vol.16, No. 2.

Wortley, R., Child Pornography. In: Natarajan M, editor. *International crime and justice*. USA: Cambridge University Press, 2010, p.178-84, cited in J. Pritchard et.al, 'Internet subcultures and pathways to the use of child pornography', *Computer Law and Security Review* 27, 2011.

Wortley, R., and S. Smallbone, 'Child Pornography on the Internet', *Problem-Oriented Guides for Police – Problem-Specific Guides Series*, US Department of Justice, Office of Community Oriented Policing Services, Washington, USA, 2006, no. 41.