Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA

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

July 2011

THE CASE FOR ACCESS DISRUPTION TO ONLINE CHILD SEXUAL ABUSE MATERIAL

The commercial trade in child sexual abuse images is a reality. It involves thousands of commercial child sex abuse sites and an estimated 50,000 new child sexual abuse images are produced each year.[1] The industry is estimated to be worth about US$250 million globally.[2] The purchase and trade in commercial sexual abuse material generates a market and ongoing demand for human rights abuses, involved in the production of the material. Human trafficking particularly feeds the commercial child sexual abuse industry on the Internet.[3]

Blocking ready access to child sexual abuse material is an important tool in the struggle against the commercial child sexual abuse industry. Organised criminals, mainly in Eastern Europe and growingly in Asia, run 'businesses' selling images and videos of child sexual abuse online primarily to make money. It is this activity that ISP level access disruption has the greatest benefit in combating.

There are two types of child sexual abuse networks online. Non-commercial peer-to-peer networks and commercial child sexual abuse operations, often involving the World Wide Web. Non-commercial networks are generally used by dedicated offenders who share images with other sex offenders. Commercial networks are primarily criminal operations whose primary aim is to produce profit. These commercial networks are more likely to involve younger children than non-commercial material. The Internet Watch Foundation found that 73% of the child victims on commercial child sexual abuse sites appear to be under 10 years old and 66% of the images and videos depicted sexual activity between adults and children including the rape and sexual torture of the child.[4] It is this industry that ISP level access disruption based on urls is particularly useful in disrupting.

The Federal Government has moved to require Internet Service Providers (ISPs) to block ready access to material that would be classified as Refused Classification (RC) under the Australian classification system. Material that is classified RC is already banned in Australia in media such as books, magazines, films and computer games. It is also banned on Australian hosted websites.

The RC classification category encompasses materials that:

> *(a) describe, depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards or morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified;*

[1] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[2] ibid.
[3] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[4] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.

(b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or
(c) promote, incite or instruct in matters of crime or violence.

The refused classification category includes child sexual abuse material and this would make up the majority of what would be subject to access disruption by ISPs.

There has been considerable debate over what material would be impacted by access disruption and how this would impact upon free speech. Under the Government's proposal, only access to material in the RC category would be required to be disrupted by the ISP. The RC category also covers other harmful material that would be missed if access disruption was simply limited to child sexual abuse material. This would include 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.[5] 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 RC 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 RC material blocks inadvertent access and disrupts deliberate attempts to access such images and protects the rights of victims not to have their images viewed.

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

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 would challenge this view.

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.

The Australian Government has also voluntarily signed up to international treaties promising to combat human rights abuses, human trafficking and transnational crime. Access disruption by ISPs helps fulfil these promises made by the Australian Government.

[5] 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 filtering 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.*

It is important to note that ISP access disruption is only one tool in ending the abuse of children to produce images. It can be by-passed by those with the technical knowledge to do so or by finding an ISP willing to provide unrestricted service to child sexual abuse material.

Other tools the Australian Government could provide include:

- Arrest and prosecution for material such as child sexual abuse material, as a means to deter both producers and consumers of such material.
- The use of 'take-down' notices where possible, to require content hosts to remove material and highly desirable for child sexual abuse material online.
- Education of offenders and potential offenders accessing criminal material such as child sexual abuse material, to disrupt cognitive distortions of many offenders that they are doing nothing wrong if they are only accessing or purchasing such material.
- ISPs and content hosts being required to report clients using their services for criminal activity when they detect such criminal activity taking place, such as accessing or posting online child sexual abuse material.

A combination of ISP level access disruption and the above measures has already been yielding detectable results in the fight against 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[6] as a result of the above measures. The webpage blocking list maintained by the Internet Watch Foundation now typically contains 500 urls at any one time, down from 1,200 in 2008.[7]

ISP level access disruption to RC classified 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 where these other measures are not adequately in place.

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 trials the Australian Government has carried out.

ISP level access disruption 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. There is no justification for the need to access illegal material in the RC category. Access disruption is also a technically feasible and cost effective measure that prevents people profiting from criminal behaviour. It would also free up police resources to focus on other aspects of the commercial child sexual abuse industry.

[6] Internet Watch Foundation, '2010 Annual and Charity Report', p. 1.
[7] http://www.iwf.org.uk/resources/trends

Table of Contents

1. INTERPOL's support for ISP level access disruption for child sexual abuse material

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".[8]

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

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

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

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.

2. Other Support for Access Disruption

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: [9]

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.

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:[10]

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.

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

[10] 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.

Further, Eneman (2010) argued blocking by ISPs reduces the display of child sexual abuse material and consequently reduces revictimisation of the abused child.[11] She summarised this issue as follows:

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

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

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

The following countries are members of the CIRCAMP network: Norway, UK, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Malta, the Netherlands, Poland, Spain and Sweden.[12]

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

3. Re-victimisation of Victims of Child Sexual Abuse

Victims of sexual abuse have a right to not have images of their abuse viewed by others, either inadvertently or deliberately.

Research has documented that victims of sexual abuse 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,

[11] 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.
[12] 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.

vulnerability to repeated victimisation, interpersonal difficulties, dissociation and disbelief about the abuse, functional amnesia and effects on relationship with others.[13] 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.[14]

According to the Child Sexual Abuse Prevention Program, "Research has consistently identified the serious and long-lasting effects of sexual assault on children. However, for child victims of child pornography these effects are significantly exacerbated."[15] 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. It is also very difficult to completely remove images once they have been uploaded making it even more important for some form of regulation to exist in the online environment.

In 2009 the International Telecommunications Union (ITU) issued their *Guidelines for Policy Makers on Child Online Protection.* They pointed out:[16]

> *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.[17] 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]."[18]

[13] 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.
[14] 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.
[15] Child Sexual Abuse Prevention Program (CSAPP Inc) Submission to the Joint Select Committee on Cyber Safety Inquiry into Cyber safety, No 107, p. 3
[16] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 19.
[17] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 27.
[18] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 28.

4. Volume of Access to Child Sexual Abuse Material

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. However, what data is available suggests western democratic societies have thousands of people who inadvertently access child sexual abuse material or deliberately seek to access child sexual abuse material. There is little reason to believe the situation in Australia would be any different.

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.[19]

A BBC report from 2006 indicated that UK ISP BT were blocking 35,000 attempts to access child sexual abuse material each day by their clients, 18 months after they started using the Internet Watch Foundation list of known child sexual abuse sites.[20] BT provided service to one third of UK internet users.

Cybertip.ca reported in their 2009 report that in the UK, a single ISP blocked more than 20,000 daily attempts to access child sexual abuse material and in Norway the estimate was 15,000 – 18,000 daily attempts.[21]

5. Consumption of Commercial Child Sexual Abuse Material

Purchasing child sexual abuse material makes up a significant proportion of the material offenders are able to access. McCarthy found that 29% of non-contact and 36% of contact offenders purchased child sexual abuse material.[22]

Research suggests that a reasonable proportion of offenders access child sexual abuse material use the World Wide Web, with one study finding of a sample of such offenders, 78% obtained images using Internet Relay Chat software, 42% used the World Wide Web, 39% used newsgroups, 30% e-mail and 21% ICQ.[23] This sample included offenders who both shared images and those that purchased images.

6. The Commercial Child Sexual Abuse Industry

The UN Office of Drugs and Crime has noted that human trafficking feeds particularly the commercial child sexual abuse industry on the Internet.[24] The UNODC report estimates the commercial child sexual abuse industry on-line, as opposed to non-commercial peer-to-peer networks, generates an estimated 50,000 new child sexual abuse images each year and is worth about US$250 million globally. It involves thousands of commercial child sex abuse sites. Commercial child sexual abuse sites are more likely to involve younger children than

[19] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research
[20] http://news.bbc.co.uk/1/hi/uk/4687904.stm
[21] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 16.
[22] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[23] 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.
[24] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010

non-commercial material. The Internet Watch Foundation found that 73% of the child victims on commercial child sexual abuse sites appear to be under 10 years old and 66% of the images and videos depicted sexual activity between adults and children including the rape and sexual torture of the child.[25]

Cybertip.ca found that commercial websites tend to cater to a specific group of offenders, with images grouped in specific or narrow age ranges. A minority of commercial sites cater to individuals with a sexual interest in very young children, showing mainly infants and toddlers.[26] They found that 29.7% of images on commercial child sexual abuse sites depict children being sexually assaulted, with 3.3% of images on commercial sites being of extreme sexual assaults (compared to 2.7% of images on all child sexual abuse websites).

The UNODC report that the majority of commercial child sexual abuse operations are in located Eastern Europe. This is apparently due to lower levels of law enforcement in Eastern Europe against this transnational criminal activity and that their customers, who appear to be largely from Western countries, have a preference for 'white' girls.

The Internet Watch Foundation has identified 715 unique sources of commercial child sexual abuse websites, each with a distinct website name and brand. They found 321 of these were active in 2010. Of these, the ten most prolific 'brands' account for at least 47.7% of the commercial webpages seen by the Internet Watch Foundation, with the most prolific using 862 urls. Each of the webpages or websites is a gateway to hundreds or even thousands of individual images or videos of children being sexually abused, supported by layers of payment mechanisms, content stores, membership systems and advertising frames. Payment systems may involve pre-pay cards, credit cards, 'virtual money' or e-payment systems and may be carried out across secure webpages, text or e-mail. Analysis by the Internet Watch Foundation has identified that the criminals running these operations do so in a cluster of commercial child sexual abuse 'brands' from the manner in which they share hosting patterns, payment arrangements, advertising systems and registration details as well as from the overall appearance of the websites.[27]

The Internet Watch Foundation reports that there has been a change in the way child sexual abuse material is hosted on the internet with a growing amount of content being posted to separate locations rather than large collections of images stored within a folder on a single website.[28]

The 2009 analysis of child sexual abuse images online by Cybertip.ca reported they had examined 800 commercial child sexual abuse sites (representing 12.6% of all child sexual abuse sites they had dealt with) which used 27 different payment types, most of which would be considered online payment systems.[29] In 55% of cases the sites claimed to be able to accept traditional credit cards for payment. For 61 of the sites payment could be made from a traditional bank or financial institution.[30] Nearly a quarter (23.8%) of the commercial child sexual abuse sites offered multiple payment methods, with the average number of payment types being offered being 2.4 for those that offered multiple payment types.[31] The majority

[25] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.
[26] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 41.
[27] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[28] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[29] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 10, 56.
[30] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 64.
[31] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 64.

(85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (average of $53 a month). Membership obtained for a one-time fee (15.4% of the sites) ranged from $30 to $1,990 with an average cost of $249.[32] DVDs were also sold (5.8%) for as much as $1,900, as were a variety of packages (4.7%), image sets (3.1%), videos (1.1%) and websites (0.2%). They concluded there is clearly a large consumer market for child sexual abuse images.

They noted that in addition to the commercial child sexual abuse sites there are many sites that do not have their own commercial component but exist for the purpose of promoting commercial sites. In providing links, re-directs or advertisements for distinct commercial websites, these sites may receive payment or reciprocal linking for making child sexual abuse material available. These websites are indirectly profiting from the sale of child sexual abuse images.[33]

Their analysis found the top five countries where urls were registered for commercial child sexual abuse material were:[34]

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

They found that 80% of child sexual abuse sites hosted in Poland were commercial sites.[35]

Of the sites on the Internet Watch Foundation list containing child sexual abuse material, 42% of urls were hosted in North America, 41% in Russia and 17% in Asia. Only one site was found to be hosted in Australia.[36]

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

The UNODC estimates there are several thousand commercial child sexual abuse websites at any one time. This makes maintaining a block list of such sites an achievable objective.

The commercial child sexual abuse industry is very small compared to the vast empire of legal adult pornography on the Internet. For example a study in 2006 estimated that the number of webpages containing the keyword ‘porn’ was 88.8 million, those containing the

[32] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 65.
[33] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 56.
[34] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 11.
[35] Canadian Centre for Child Protection, ‘Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca’, November 2009, p. 62.
[36] Internet Watch Foundation, ‘2010 Annual and Charity Report’, p. 9.

keyword 'XXX' numbered 181 million and those with the keyword 'playboy' numbered 43.2 million.[37]

7. 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.[38] Access disruption by ISPs blocking ready access to such material may assist in arresting the curiosity of some potential offenders towards such material.

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

7.1 Differences between 'Contact' and 'Non-Contact' Offenders

According to Professor David Middleton of De Mountford University, only around 10% of offenders who download child sexual abuse material online go on to commit actual child sexual abuse themselves (become contact offenders).[39] His research suggests that such offenders use self-distancing to justify their offending behaviour, with the Internet providing a vehicle to distance themselves from the act they are viewing as well as justifying a view that they are not sex offenders themselves. They are able to justify continued access to child sexual abuse material in a context that they are not directly responsible for the harm and are simply a passive viewer.[40]

There are 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 such material. These offenders are commonly referred to in the literature as 'non-contact offenders'. 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.[41] A study of print and news reports of 205 Internet offenders found 19% of offenders traded

[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.

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.[42] 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.[43]

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).[44] 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.[45] She found that 36% of non-contact and 53% of contact offenders traded in child sexual abuse material.[46] 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.[47] It should be noted that McCarthy found that her research led to the conclusion that possessing child sexual abuse material was not causal of going on to commit contact offences, as 84% of contact offenders in the sample reported sexually abusing a child prior to possessing child sexual abuse material.[48]

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.[49]

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.[50] Those with intimacy deficits were described as having low expectations of the

[42] 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.
[43] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 183.
[44] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 186.
[45] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[46] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[47] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), pp. 189-190.
[48] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 193.
[49] 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.
[50] 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.

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 hen coupled with deviant sexual desire could lead to the use of pornography (in this case child sexual abuse material) as a mood alleviating strategy.[51] For some offenders, but not all, accessing images on the Internet may function as a way of avoiding or dealing with difficult emotional states.

Research has found that the cognitive distortions of those who purchase commercial child sexual abuse images are different from those who are contact offenders. Internet offenders appeared to hold cognitive distortions related to the notion that sexual fantasies and images of child sexual abuse are not directly harmful (for example, "Having sexual thoughts and fantasies about a child isn't all that bad because at least it is not really hurting the child").[52] Another offender stated:[53]

> *"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:[54]

> *"…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:[55]

> *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.[56] 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".[57]

---

[51] 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.

[52] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), p. 79 and D. Middleton, R. Mandeville-Norden and E. Hayes, *Does treatment work with internet sex offenders? Emerging findings from the Internet Sex offender Treatment Programme (i-SOTP),* Journal of Sexual Aggression **15(1)** (2009), p. 8.

[53] 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.

[54] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 132.

[55] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 132.

[56] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 129.

[57] 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.

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.[58] 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.[59]

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.[60]

7.2 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.[61]

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.[62] 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.[63]

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.[64] Another offender argued that children in poverty overseas being photographed naked for money was better than them starving.[65]

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

---

[58] 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.
[59] 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.
[60] 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.
[61] 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.
[62] 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.
[63] 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.
[64] B. Winder and B. Gough, *"I never touched anybody – that's my defence": A qualitative analysis of internet sex offender accounts,* Journal of Sexual Aggression **16(2)** (2010), p. 131.
[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), pp. 131-132.

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."[66]

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

7.3 Non-Contact Offenders easier to rehabilitate

The lower frequency of pro-offending attitudes and beliefs that serve to legitimise and maintain sexually abusive behaviours displayed by non-contact Internet offenders suggests that they may be unlikely to represent persistent offenders or potentially progress to commit future contact sexual offences. Similarly, a greater ability to empathise with victims may also contribute positively to Internet offenders' achievements in therapeutic interventions.[68]

The effectiveness of interventions with those who purchase child sexual abuse material is borne out by the lower reconviction rates of such offenders compared to contact offenders.[69] Seto and Eke (2005) found that in a three year period (April 2001 to April 2004) in a sample of 201 Canadian adult male offenders for child sexual abuse material offences the recidivism rate for non-contact offenders of a further offence related to child sexual abuse material was lower than for those who also had contact offences (3.9% compared to 5.3%). Those with only offences related to child sexual abuse material were far less likely to reoffend with a sexual contact offence than those with a past history of sexual contact offences (1.3% compared to 9.2%).[70]

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 block messages delivered through access disruption by ISPs and the non-contact offender

---

[66] 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.

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

[68] I.A. Elliott, A.R. Beech, R. Mandeville-Norden and E.Hayes, *Physchological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders,* Sexual Abuse: A Journal of Research and Treatment **21,** (2009), pp. 87-88.

[69] 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.

[70] 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.

attempts to access a child sexual abuse site. The 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 they believe that education of offenders and potential offenders is a vital tool in this fight. However, the Unit is unaware of there being in Australia any wide scale education campaign targeting this group. 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 ITU highlighted the educative value of block pages when a list is used by ISPs to disrupt the commercial child sexual abuse industry online:[71]

> *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.*

8. Australia's Human Rights Obligations to Combat 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*. It also has obligations to ensure that Australian businesses do not profit from transnational criminal activity. Australia is a State Party to the UN *Convention Against Corruption* (UNCAC). Article 2 of UNCAC 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 31 of UNCAC 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).

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

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.

9. Arrest and Prosecution not enough to deal with Online Child Sexual Abuse

Arrest and prosecution of those producing and consuming child sexual abuse material is believed to have a deterrent impact on 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 to such 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.[72]

The Unit believes 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.[73] Table 1 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.[74]

Table1. 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

Table 2 provides a comparison with the UK, for the years the Unit has been able to find data for.[75] 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.

[72] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[73] http://www.afp.gov.au/media-centre/fact-stats/online-child-sex-offences.aspx
[74] Commonwealth Director of Public Prosecutions submission to the Joint Select Committee on Cyber-Safety inquiry into Cyber Safety, 2010, p. 5.
[75] Yaman Akdeniz, 'Internet Child Pornography and the Law', Ashgate Publishing Limited, Surrey, UK, 2008, p. 25.

Table 2. 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 comparison suggests that Australia is significantly behind the UK in adequately resourcing police to deal with this criminal activity. It is possible there is a greater number of offenders in the UK, but this seems less likely than the difference being due to policing resources directed to the problem.

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.[76]

The Unit notes that the priority for Australian police in dealing with child sexual abuse online is to protect Australian children.

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.

Due to limited resources, police usually only catch offenders who download child sexual abuse material after they have built up substantial collections of child sexual abuse material. 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.[77] McCarthy's (2010) study of US offenders 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 points to the need for interventions that address offending or potential offending behaviour earlier.

10. ISP Level Access Disruption growing globally

Access disruption to online child sexual abuse material is gaining momentum in democratic countries, as its value as 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 shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered." Italy also has a legislative requirement on all ISPs to not provide access to their clients seeking to access

[76] 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.
[77] 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.

child sexual abuse materials. 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 70 ISP, search and content providers, mobile operators and filtering companies who block client access to child sexual abuse material now cover 98.6% of residential broadband connections.[78]

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. An average of 59 webpages were added to the list each day reflecting the speed at which child sexual abuse content moves online location.[79] The webpage blocking list now typically contains 500 urls at any one time, down from 1,200 in 2008.[80] They update their list twice a day.[81] The Internet Watch Foundation report their entire operation ran on a budget of just £1 million ($1.5 million) in 2009 and in 2010.[82]

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.[83]

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

[78] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[79] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[80] http://www.iwf.org.uk/resources/trends
[81] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[82] Internet Watch Foundation, '2010 Annual and Charity Report', p. 16.
[83] 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.

discourage such activity.[84] The US also requires public schools and libraries to take measures against child sexual abuse material on the Internet.[85]

11. Problems with leaving it to ISPs to voluntarily disrupt access

Implementing access disruption to RC classified material online should not be left to 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 Unit 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, as through a proxy site.[86] However, this is a common argument for not restricting Australian companies from engaging in transnational crime. The argument is that if Australian companies are restricted from participating in the transnational criminal activity (be it paying bribes or money laundering for example) foreign companies will continue to engage in these activities and it will have no net impact in reducing the criminal activity and only increase the costs on Australian businesses and their Australian customers.

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

Both the Australian Crime Commission and the Australian Federal Police have complained that the IT industry do not adequately assist them through their failure to report online criminal activity (The Age 18/10/2010). In the case of the AFP, they publicly complained about the case where Facebook detected the activities of a child exploitation network and failed to report this network to law enforcement (AFP media release 27 August 2010).

---

[84] '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.

[85] 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.

[86] 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.