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 Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001
classification@alrc.gov.au

Submission on the National Classification Scheme Review

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

The Synod of Victoria and Tasmania seeks to end the abuse of children which occurs in the production of child pornography, and the trafficking of children for the purpose of producing child sexual abuse material.

The Unit's primary interest in the review is in ensuring Australians are not able to purchase and possess material which creates a demand for images that involve human rights abuses or transnational criminal activity in their production. The Unit is concerned by a small, but vocal, minority who believe Australians should be able to view whatever they like with no restrictions imposed by Government or the wider community, with a reckless disregard for the abuse such a position may facilitate.

The Unit believes that material that facilitates gross human rights abuses or transnational criminal activity should be Refused Classification. The Unit notes that most, if not all such material, would be Refused Classification (RC) under the current definition:

(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;

(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 Unit notes that newer technologies, such as the internet and mobile phones, have created new avenues to profit from human rights abuses and transnational criminal activity. The UN Office of Drugs and Crime has noted that human trafficking particularly feeds the commercial child sexual abuse industry on the Internet.[1] 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

[1] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010

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 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.[2]

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.[3] 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).

A higher number of internet 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.[4] 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.[5]

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.[6]

The Unit notes that adults are also trafficked and forced to produce sexual abuse material for sale on the internet. Thus a classification system that allowed for violent rape materials to be available for viewing by Australian adults may facilitate human trafficking by allowing Australia to contribute to a market for such materials.

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.*

---

[2] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.
[3] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 41.
[4] 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.
[5] 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.
[6] 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.

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 23 of UNCAC addresses the proceeds of crime:

> *1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally*
> *(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;*
> *(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;*
> *(b) Subject to the basic concepts of its legal system:*
> *(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;*
> *(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.*
> *2. For purposes of implementing or applying paragraph 1 of this article:*
> *(a) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences;*
> *(b) Each State Party shall include as predicate offences at a minimum a comprehensive range of criminal offences established in accordance with this Convention;*
> *(c) For the purposes of subparagraph (b) above, predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;*

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, stating:

> *1. Each State Party shall take, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:*
> *(a) Proceeds of crime derived from offences established in accordance with this Convention or property the value of which corresponds to that of such proceeds;*
> *(b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Convention.*
> *2. Each State Party shall take such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation….*

Australia has obligations to combat human trafficking as a States Party to the following 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).

It is important that the Australian National Classification Scheme uphold Australia's commitment to human rights and to combat transnational criminal activity.

Question 1. Should the ALRC focus on developing a new framework for classification, or improving key elements of the existing framework?
The Unit believes that the ALRC should seek to improve on key elements of the existing framework. The Unit believes that the National Classification Code should contain a principle that material that facilitates gross human rights abuses or transnational criminal activity should be prohibited.

The purchase and trade in commercial sexual abuse material generates a market for such material, stimulating demand for the human rights abuses involved in its production.

The Unit supports Recommendation 2 of the Senate Legal and Constitutional Affairs References Committee in their *Review of the National Classification Scheme: achieving the right balance*, that the National Classification Code should be expanded to take into account community concerns about the sexualisation of society, and the objectification of women.

Question 2. What should be the primary objectives of a national classification scheme?
The Unit considers the primary objectives of the National Classification Code to be:

a) Adults should be able to read, hear and see what they want, provided such material does not facilitate gross human rights abuses or transnational criminal activity;
b) Minors should be protected from material likely to harm or disturb them;
c) Everyone should be protected from exposure to unsolicited material that they find offensive;
d) The need to take account of community concerns about:
    (i) Depictions that condone or incite violence, particularly sexual violence;
    (ii) The portrayal of persons in a demeaning manner; and
    (iii) Sexualisation of children in society and the objectification of women.

The Unit believes that 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, vulnerability to repeated victimisation, interpersonal difficulties, dissociation and disbelief about the abuse, functional amnesia and effects on relationship with others.[7] 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

[7] 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.

sexuality, and many had particular difficulties in establishing and maintaining healthy emotional and sexual relationships.[8]

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."[9] 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.

Question 3. Should the technology or platform used to access content affect whether content should be classified, and, if so, why?

There are two issues here. One is whether different classification categories should apply across different forms of technology or platform and the other is how material on different technologies and platforms is subjected to the classification categories.

Classification categories across different technologies and platforms should reflect the objectives of the National Classification Scheme. They should seek to prohibit viewing or access to material that is Refused Classification due to the harm such material causes in its production, to the viewer or to the wider community (for example a person incited to commit racially motivated violence as a result of accessing material inciting such criminal activity). Where it is not possible to prohibit access to RC classified material, the category should be used as a deterrent to access. For other categories, classification categories should seek to provide a warning to adults about the nature of the material so they can decide if they wish to access the material or if it will offend or disturb them. The community, through government, may also use the categories to decide that certain material should not be produced and sold for commercial purposes, as is the case across States in Australia in relation to X rated films.[10]

The categories should seek to assist in regulating the access of minors to material that may harm or disturb them. They should also assist parents and guardians in protecting minors from such material where it is not reasonably possible to stop minors from being exposed to the material through regulation.

The Unit recognises that different technologies and platforms may require very different regulatory responses in applying the classification categories to the material.

For example, it is relatively easy to require and enforce classification of commercial video sold through retail outlets. While some retail outlets (such as service stations and stalls at weekend markets) might escape effective enforcement, larger commercial retail outlets comply with the need for the material they sell to be classified with limited enforcement effort.

However, even in the existing regime, there is no attempt to force classification on small scale amateur material such as 'home movies' that might be traded and sold between small groups of individuals in the community. The problem with regulation of the online environment is the vast amount of material and that much of it is non-commercial, produced by individuals or small groups.

---

[8] 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.

[9] Child Sexual Abuse Prevention Program (CSAPP Inc) Submission to the Joint Select Committee on Cyber Safety Inquiry into Cyber safety, No 107, p. 3

[10] Although X rated films can be sold in the ACT and Northern Territory.

Further, consideration needs to be given to the risk of harmful material being undetected if regulatory resources are not applied. For example, for films shown in cinemas, a film advertised as PG but which in reality was an R18+ film, would undoubtedly attract a large number of complaints to the relevant regulatory authority from the cinema audience. Thus, the level of inspection needed to enforce classification for such a platform is low by comparison to many other platforms.

Within the limits of regulatory resources, priorities need to be established. For example, it is far more important to warn members of the community of material that is Refused Classification online than to worry about ensuring those online know if a site would meet the classification of G or PG.

The Unit would put priority on regulatory resources being applied to deal with material likely to cause the greatest levels of harm if left unaddressed. Without such prioritisation, material that causes serious harm may be left unaddressed due to regulatory resources being deployed to address issues of minor significance. Thus, the Unit believes regulatory resources would best be applied to deal with material considered RC, X or R18+ when considering the online environment and in relation to new technology.

The need to identify and deter or block access to material depicting sexual abuse and other material produced through human rights abuses is necessary across technologies. However, the on-line environment has particular characteristics which make it even more necessary to restrict or remove such material.

For example, 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.[11] 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.[12]

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.[13] Another offender argued that children in poverty overseas being photographed naked for money was better than them starving.[14] 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.[15] 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

[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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.

and harm that pornography should be re-conceptualised as "instrumentally casual [though not solely casual] in the etiology of sex offending."[16]

These particular behaviours occurring in the online environment reinforce the need for a classification code that makes it clear some material is unacceptable and the need for restriction of that material so people can't "accidentally" come across it. This is particularly important due to the amount of child sexual abuse material online. Restriction is also crucial In order to stem the demand for this sort of material.

Another problem with new technology platforms is that even large providers appear to have a greater disrespect for compliance with Australian law in relation to classification. The willingness of providers to comply with and abide by the National Classification Code should be an important factor in the deployment of regulatory resources. Amazon recently 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.

In opposition to the Government's plans that ISPs not provide unrestricted access to RC classified material the Google Australian managing director Karim Temsamani stated that such a measure "goes way beyond child sexual abuse material and would block access to important online information for all Australians".[17] Mr Temsamani did not elaborate on what RC classified material Google Australia thought it was important for all Australians to have access to. With such public disregard of the Australian classification system, it is difficult to believe that the ICT industry can be collectively relied upon not to freely allow clients access to material that promotes human rights abuses or transnational criminal activities in violation of the RC category. It highlights the need for government regulation to force co-operation with law enforcement where it will not be freely given.

The Unit also recognises that the online environment poses a much greater challenge to achieving the objective of protecting minors from material that may harm or disturb them. It requires much greater levels of vigilance by parents and guardians compared to media like free-to-air television, radio or billboards. The Unit believes that the burden of achieving this objective of the National Classification Code should not be left entirely to parents and guardians. They should be assisted by being provided with readily available and easy to use tools, such as PC based filtering tools.

Question 4. Should some content only be required to be classified if the content has been the subject of a complaint?

The Unit recognises a complaints based mechanism only is limited, as many people will not report material that disturbs them or involves serious human rights abuses or criminal activity. ACMA deals with reasonable levels of complaint about material, having investigated over 10,500 complaints about online content since 1 January 2000 and having taken action on over 8,000 items of prohibited content as a result.[18] However, given the vast amount of media available to Australians this is probably only a very small fraction of material that would be Refused Classification or that has been displayed in breach of Australian legislation.

By comparison, from 1 July 2009 to 30 April 2010, ACMA received 2,554 complaints[19], while the UK Internet Watch Foundation hotline dealt with 48,702 reports in 2010.[20] Both bodies report substantial increases in the number of complaints made over the previous year.

---

[16] 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.
[17] Asher Moses, 'Conroy backs down on net filters', *The Age,* 9 July 2010.
[18] ACMA submission to the Joint Select Committee on Cyber-Safety, July 2010, p. 8.
[19] ACMA submission to the Joint Select Committee on Cyber-Safety, July 2010, p. 8.

Research from other jurisdictions suggests a minority of people report even the worst types of material. 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.[21] 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.

Thus for a complaints mechanism to be effective in identifying material requiring classification, substantial effort needs to be made to ensure the general public easily know where to go to make a complaint and that lodging a complaint is quick and simple. Complex and lengthy online forms that need to be completed or hot lines that require a caller to have to wait more then five minutes will deter many from lodging complaints.

The Unit supports the recommendation of the Senate Legal and Constitutional Affairs Reference Committee in their *Review of the National Classification Scheme: achieving the right balance* for the need for a 'Classification Complaints' clearinghouse where complaints in relation to matters of classification can go (Recommendation 29).

Despite their limitations, complaints based mechanisms do have value. 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.[22]

In addition to simple and easy to use complaints mechanisms, Australian regulatory authorities should avail themselves of identification of child sexual abuse sites and material online by working with respected bodies located overseas such as INTERPOL and the UK Internet Watch Foundation. Such collaboration assists in combating commercial child sexual abuse operations located overseas.

Further, complaints alone cannot be relied upon and regulatory resources need to be applied for the detection of harmful content, especially in the RC category. However, such resources are not necessarily expensive.

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.[23] The webpage blocking list now typically contains 500 URLs at any one time, down from 1,200 in 2008.[24] They update their list twice a day.[25] The Internet Watch Foundation report their entire operation ran on an annual budget of just £1 million ($1.5 million) in 2009 and in 2010.[26]

In addition to listing child sexual abuse sites, the UK Internet Watch Foundation also detects and responds to:[27]

---

[20] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[21] Internet Watch Foundation, 'UK adult internet users: 2008 research report', http://www.iwf.org.uk/resources/research
[22] 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.
[23] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[24] http://www.iwf.org.uk/resources/trends
[25] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[26] Internet Watch Foundation, '2010 Annual and Charity Report', p. 16.
[27] Internet Watch Foundation, '2010 Annual and Charity Report', p. 2.

- Criminally obscene adult content hosted in the UK;
- Incitement to racial hatred content hosted in the UK; and
- Non-photographic child sexual abuse images hosted in the UK.

Question 5. Should the potential impact of content affect whether it should be classified? Should content designed for children be classified across all media?
Most discussion around the National Classification Code focuses only on the harm to those who view the material. The Unit believes consideration of harm must extend to its production and to whether the purchase, viewing or consumption of the material will stimulate further demand, thus increasing the harm caused in its production. Such consideration obviously points to the need to prohibit access to sexual abuse material.

The Unit strongly supports the view that the potential harm material may do to a viewer or consumer of the content or the harm done in the production of the material should be of highest priority in determining the need for material to be classified.

Ideally, where the regulatory resources can be made available, it is highly desirable to classify all content designed for children. However, such a goal should not be at the expense of the need to regulate material that is causing harm in either its consumption or production.

Question 6. Should the size or market position of particular content producers and distributors, or the potential mass market reach of the material, affect whether content should be classified?
The Unit supports the view that it may be appropriate in some circumstances to allow companies to self-regulate. This will help to reduce the regulatory burden on the State, but ultimately shifts the costs directly to consumers as companies engaged in self-regulation are likely to pass the costs onto consumers. It has the advantage of freeing up the resources of government regulatory bodies to be directed at material that is harder to police and that involves serious harm in its production or consumption.

For self-regulation to work, there needs to be confidence the bodies that are self-regulating are competent and committed to doing so. For example, based on the public comments by the managing director of Google Australia towards RC material above, there would be questions about the commitment of Google Australia to be trusted to self-regulate content classification.

However, the Unit supports the recommendations of the Senate Legal and Constitutional Affairs Reference Committee in their *Review of the National Classification Scheme: achieving the right balance* to provide greater safeguards over the existing provider self-regulation:

- Recommendation 23 that industry codes of practice under current self-regulatory and co-regulatory schemes, including those under the *Broadcasting Services Act 1992*, the ARIA/AMRA Labelling Code and the advertising industry, should be required to incorporate the classification principles, categories, content, labelling, markings and warnings of the National Classification Scheme. The adoption of these measures by industry should be legally enforceable and subject to sanctions.
- Recommendation 24 that industry bodies wishing to exercise classification decision-making functions should be required to be accredited by the Australian Government.
- Recommendation 25 that the Classification Board should be responsible for the development of a content assessor's accreditation, including formalised training courses for all industries covered under the National Classification Scheme.
- Recommendation 26 that the accreditation of content assessors should be subject to disqualification as a result of poor performance.

- Recommendation 27 that transgressions of classification requirements within codes of practice by industry participants should, if verified by the Classification Board, be punishable by substantial monetary fines.

Question 12. What are the most effective methods of controlling access to online content, access to which would be restricted under the National Classification Scheme?

A range of methods are required to control access to online content and meet the various objectives of the National Classification Scheme, access to which would be restricted under the National Classification Scheme.

Q12.1 Protecting everyone from exposure to content they find offensive

From the point of view of protecting everyone from exposure to unsolicited material they find offensive, user side filtering of online content would appear to be an appropriate response to material outside the RC category. Individuals who do not wish to see certain content use a filter to block the classifications of material they do not wish to see. However, filters to deal with legal pornography provide a substantial challenge, due to the sheer volume of online pornography. For example a study in 2006 estimated that 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.[28] Many of these sites will change URL from time to time.

In response some user filters work on the basis of keywords on the site or the level of skin tone colours. Such filters will undoubtedly result in some level of over-blocking, blocking access to content that the user would not find offensive. However, given the use of such filters is up to the user, this is not a significant problem.

However, to achieve this objective of the National Classification Scheme, it would be helpful to increase knowledge of the availability of such filters to users. Ideally, ISPs may be required to make their clients aware of the availability of such filters.

The Unit also notes that often the ability to access user side filtering can come at a cost to the user. It is reasonable to question if users should be required to pay for filtering when it is an objective of the National Classification Scheme to protect everyone from unsolicited material they find offensive. There is a strong argument to say that individuals that choose to make use of user specified filtering not be required to bare the full cost of doing so. This might mean the government provides free filters, or a rebate or that where an ISP provides a filtering service they spread the cost across all users and not just those making use of the filter.

Q12.2 Protecting minors from material likely to harm or disturb them

Again parents and guardians may be expected to make use of user side filtering of online content to protect minors in their care from access to material likely to harm or disturb them. However, in this case, the government has a much greater role in making access to such filters readily available, easy to use and effective.

The problems with user side filters to protect minors from material likely to harm or disturb them are that the usage of such filters by parents is very low and often the filters can be by-passed by a determined minor.

[28] 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.

Education for both parents and minors plays an important role in assisting minors to avoid material likely to harm or disturb them.

In addition, the Unit supports the view that ISPs should be required to disrupt ready access to RC classified material to reduce inadvertent access of minors and adults to such material that may harm or disturb them. This provides a limited back up to provide some protection to minors in cases where their parents have failed to take steps to protect their children from exposure to such material, or the steps they have taken are inadequate. As noted earlier, an Internet Watch Foundation survey found that 5% of adults stated they had accessed child sexual abuse material alone, and it can be reasonably assumed such self-reporting is likely to be for inadvertent access.

The Unit rejects the reported assertion by academics such as Professor Karen Vered from Flinders University and Dr Barbara Spears from the Australian University Cyberbullying Research Alliance that allowing minors to be exposed to RC material will assist them in learning from their mistakes.[29] Given the RC category includes such extreme online material as images and videos of the rape of infants, sexual torture of children, rape of children by animals, and general graphic torture material the Unit is unaware of studies that demonstrate the benefit of allowing minors access to such material to learn from the experience. Even exposure to less extreme RC classified material is unlikely to be of benefit to minors. The Australian Institute of Criminology (AIC) noted the reports of publicly available games online 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.[30] The AIC noted that psychiatrist Dr Ang Yong Guan argued that 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.

Such 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.

Q12.3 Measures to deal with RC classified material

Much of the detected RC material online is child sexual abuse material. For such material it should not be left to individual users to decide if they wish to access such material. There are more significant issues to be considered than merely if the material in question will disturb the viewer. When dealing with such material stronger measures are needed to deter and limit access to the material for the following reasons:

- Access to such material violates the rights of the victims of the sexual abuse to not have the images of their abuse readily accessible. This applies to images of other victims of human rights abuse posted online. While it is desirable to locate and remove such images whenever possible, where this is not possible additional measures should be taken to disrupt ready and inadvertent access to such images. Access to such images is generally described as ‘re-victimisation’ and is seen to add to the sense of helplessness and violation many victims experience. Victims should not have to rely on every user voluntarily implementing user side filtering to protect them from having images of their abuse accessed either deliberately or inadvertently.

[29] ‘Judgment call for online safety’, About the House, May 2011, p. 13.

[30] 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.

- Much of the material that would be classified RC has either abused or harmed people in its production or causes harm to those accessing the material or to those around them through the possible influence of the material on the person accessing it.
- Those deliberately seeking to access RC classified material can not be relied upon to implement user side filters to prohibit such access.
- Content providers of RC classified material online are rarely likely to voluntarily comply with 'take-down' notices even where it is possible to issue such notices. Those seeking to profit from the sale of child sexual abuse material or to incite racially motivated violence through online content are deliberately engaged in criminal activity.
- Failure to disrupt access to commercial child sexual abuse material allows for unrestricted growth in demand for such material, and may lead to providers producing more material or encourage new entrants into the market.
- The Australian Government should not be allowing Australian ISPs to be profiting from clients engaged in criminal activity, such as accessing and downloading child sexual abuse material. ISPs should be expected to take reasonable steps to disrupt the ability of their customers to freely use their service for criminal activity.

The Australian Government needs to provide a range of measures to combat RC classified material online, which includes:

- 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.
- ISP access disruption of URLs of RC classified content. The Unit notes that ISPs blocking access to URLs serves only as a disruption measure, as such blocking can be by-passed by those with the technical knowledge to do so or by finding an ISP willing to provide unrestricted service to RC classified content.

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

In 2009 the International Telecommunications Union (ITU) issued their *Guidelines for Policy Makers on Child Online Protection.* They pointed out:[31]

> *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.

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

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.[32] 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]."[33]

A combination of the above measures has already been yielding detectable results in the fight against commercial child sexual abuse material. In their 2010 annual report the UK Internet Watch Foundation report through the range of activities to combat child sexual abuse material online, including blocking by ISPs, the length of time child sexual abuse images are hosted has been reduced from years to just days.[34] This indicates high disruption for any commercial operator seeking to make a profit from selling images. In every instance where an image is removed quickly the risk of a child being re-victimised by someone viewing their abuse has been substantially reduced. A further indication of progress being made against child sexual abuse material on the Internet is the webpage blocking list maintained by the Internet Watch Foundation. It now typically contains 500 URLs at any one time, down from 1,200 in 2008.[35]

The Unit notes that most efforts to deal with online child sexual abuse in Australia are directed at protecting Australian children. Very little concern and effort is expressed towards protecting children overseas who are victims of sexual abuse and whose images are purchased or traded by Australians. In the recent inquiry into cyber-safety by the Joint Select Committee on Cyber-Safety, very few submissions even considered this group. The Committee itself did not make a single recommendation to provide greater protection to such children through efforts to combat Australians accessing and purchasing images of children overseas who are subjected to sexual abuse.

Q12.3.1 Arrest and Prosecution

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 vitally important part of the efforts to combat child sexual abuse material online, but it has limitations. Given there are no Australian studies publicly available about the number of Australians accessing child sexual abuse material, nor the trend in these numbers, 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 globally of child sexual abuse material.[36] The Australian Federal Police are probably doing better than that, but the Unit is unable to make that assessment in the absence of any publicly available data.

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 relating to the possession, production or supply of child sexual abuse material.[37] Table 1 outlines the number of convictions for use of a carriage service for child pornography material or child

[32] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 27.
[33] International Telecommunications Union, 'Guidelines for Policy Makers on Child Online Protection', 2009, p. 28.
[34] Internet Watch Foundation, '2010 Annual and Charity Report', p. 1.
[35] http://www.iwf.org.uk/resources/trends
[36] UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* on 17 June 2010
[37] http://www.afp.gov.au/media-centre/fact-stats/online-child-sex-offences.aspx

abuse material, with the data for convictions from the Commonwealth Director of Public Prosecution.[38]

Table1. Convictions 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.[39] However, the UK data includes convictions for taking, making, distributing, showing, possessing, or publishing any advertisement conveying the distribution of indecent photographs of children, both online and by other means. The vast majority of these offences are for online activities.

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 are a greater number of offenders in the UK, but this seems less likely than the difference being due to policing resources directed at 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.[40]

Arrest and prosecution alone is not an adequate response to online sexual abuse material, given the low estimates of offenders who actually get caught (compared to the estimates of the size of the problem) 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, meaning measures to prevent crimes may be more cost effective.

Due to limited resources, often police 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.[41] 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

[38] Commonwealth Director of Public Prosecutions submission to the Joint Select Committee on Cyber-Safety inquiry into Cyber Safety, 2010, p. 5.
[39] Yaman Akdeniz, 'Internet Child Pornography and the Law', Ashgate Publishing Limited, Surrey, UK, 2008, p. 25.
[40] 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.
[41] 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.

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.

Q12.3.2 Access Disruption by ISPs

Requiring ISPs to disrupt access to RC classified material is an important additional tool in combating child sexual material online.

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

> *Encourages member countries to promote the use of all the technical tools available, including access-blocking of websites containing child sexual abuse images, in order to intensify the fight of their national specialised units against the dissemination of child sexual abuse images on the internet;*
>
> *Encourages member countries to systematically provide the INTERPOL General Secretariat with updated lists of websites containing child sexual abuse images for 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".[42]

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

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

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

They summarise the advantages of access blocking as:

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

INTERPOL acknowledges that access blocking:

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

…. 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.

ITU recognises the place of ISP blocking of ready access to child abuse material as one important tool in the fight against such material: [43]

> *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:[44]

> *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 re-victimisation of the abused child.[45] 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 re-victimisation.*

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;

---

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

[44] 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.

[45] 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.

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.[46]

Inadvertent access to sexual abuse material online is a significant issue. 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.

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.[47] 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.[48]

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.

As noted earlier 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, compared to attempting to have a block list of the hundreds of millions of websites that contain material that would be classified as X18+ or R18+.

The UNODC report that the majority of commercial child sexual abuse operations are located in 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

[46] 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.
[47] http://news.bbc.co.uk/1/hi/uk/4687904.stm
[48] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 16.

commercial web pages seen by the Internet Watch Foundation, with the most prolific using 862 URLs. Each of the web pages 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 web pages, 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.[49]

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.[50]

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.[51] 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.[52] 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.[53] The majority (85%) sold memberships, with recurring monthly payments ranging from $4 to $490 (average of $53 a month). Membership obtained for a one-time fee (15.4% of the sites) ranged from $30 to $1,990 with an average cost of $249.[54] 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.[55]

Their analysis found the top five countries hosting commercial child sexual abuse material were:[56]

- US (65.6%)

[49] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[50] Internet Watch Foundation, '2010 Annual and Charity Report', p. 8.
[51] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, pp. 10, 56.
[52] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 64.
[53] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 64.
[54] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 65.
[55] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 56.
[56] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 11.

- 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.[57]

Of the sites on the Internet Watch Foundation list containing child sexual abuse material, 42% were hosted in North America, 41% in Russia and 17% in Asia. Only one site was found to be hosted in Australia.[58]

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.[59]

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.[60] This sample included offenders who both shared images and those that purchased images.

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.[61] 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 do not regard themselves as sex offenders. However, on average they end up purchasing images of younger children and of more abusive acts than contact offenders do.

According to Professor David Middleton of De Mountford University, only around 10% of offenders who download child sexual abuse material online go on to commit actual child sexual abuse themselves (become contact offenders).[62] His research suggests non-contact 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.[63]

---

[57] Canadian Centre for Child Protection, 'Child Sexual Abuse Images. An Analysis of Websites by Cybertip!ca', November 2009, p. 62.
[58] Internet Watch Foundation, '2010 Annual and Charity Report', p. 9.
[59] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[60] 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.
[61] 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.
[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.

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.[64] 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.[65] 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 these offenders would escalate to a contact sex offence.[66]

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).[67] 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.[68] She found that 36% of non-contact and 53% of contact offenders traded in child sexual abuse material.[69] 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.[70] 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.[71]

---

[64] 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.
[65] 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.
[66] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 183.
[67] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 186.
[68] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[69] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 189.
[70] 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.
[71] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 193.

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.[72]

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.[73] 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 could lead to the use of pornography (in this case child sexual abuse material) as a mood alleviating strategy.[74] 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").[75] Another offender stated:[76]

> *"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:[77]

> *"…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:[78]

---

[72] 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.
[73] 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.
[74] 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.
[75] 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.
[76] 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.
[77] 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.

> *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.[79] 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".[80]

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.[81]

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

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.[83]

---

[78] 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.
[79] 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.
[80] 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.
[81] 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.
[82] J. McCarthy, *Internet sexual activity: A comparison between contact and non-contact child pornography offenders,* Journal of Sexual Aggression **16(2)** (2010), p. 184.
[83] 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.

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.[84] 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%).[85]

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 when the non-contact offender 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:[86]

> *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.*

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 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.[87]

---

[84] 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.

[85] 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.

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

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.[88]

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.[89] The US also requires public schools and libraries to take measures against child sexual abuse material on the Internet.[90]

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 through a proxy site.[91] However, this is a common argument for not restricting Australian companies

---

[87] Internet Watch Foundation, '2010 Annual and Charity Report', p. 4.
[88] 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.
[89] '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.
[90] 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.
[91] 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

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.

Q12.3.3 Requirements of ISPs to report clients accessing child sexual abuse material

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

These requirements have already been incorporated in Filipino law. Section 9 of the Republic Act No. 9775 *An Act Defining and Penalising the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes* has the following requirements:

- "All internet service providers (ISPs) shall notify the Philippines National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person."
- "An ISP shall preserve such evidence for purposes of investigation and prosecution by relevant authorities."
- "An ISP shall upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography."

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

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

---

offenders (11 of whom were also contact offenders) the majority used proxy servers to circumvent filtering in Sweden.

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

This results in a situation where US ISPs are required to report clients accessing child sexual abuse material to the authorities, but are then free to provide unrestricted and ready access to clients wishing to access such material.

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

Q12.4 Summary of Unit position regarding online content

Table 3 summarises what the Unit believes the regulatory response should be to different classifications of material online.

Table 3. Summary of Justice and International Mission Unit's preferred regulatory response to online material

Classification category of the online material	**Regulatory Response**
Illegal abusive material, such as child sexual abuse material	• Criminal sanctions for production, distribution and possession • Requirement on ISPs and content hosts to report such material to authorities • Requirement of content host to remove material • Requirement on ISPs to disrupt ready access to material where content removal is not possible, by blocking access to a listed that is updated at least daily • Measures to educate offenders and potential offenders to deter access and possession related offences • Working with financial institutions to disrupt payment to online commercial sites
Refused Classification material outside of that attracting criminal sanctions	• Requirement on ISPs and content hosts to report such material to authorities • Requirement of content host to remove material • Requirement on ISPs to disrupt ready access to material where content removal is not possible, using a list updated at least daily • Parent and minor education to minimise exposure to such material
X18+, R18+ and MA material that may offend some adults and may harm or disturb minors	• User side filtering or user requested filtering from ISP or filtering provider • Parent and minor education to manage responding to the presence of such online material

Question 16. What should be the respective roles of government agencies, industry bodies and users in the regulation of content?
The Unit believes government should be responsible for ensuring the implementation of the National Classification Scheme across all technology and platforms. However, the Unit does not oppose industry classifying some content, provided industry decisions are subject to review and audit by government agencies. Self-regulation by industry should be permitted where decisions are likely to be simple and where the risk of harm to consumers and those involved in the production of the material is low. Government regulatory resources are best concentrated towards material that may be complex to classify or where the content is likely to harm or disturb viewers, especially minors, or the material may promote serious human rights abuses or transnational criminal activity.

The Unit supports the recommendation of the Senate Legal and Constitutional Affairs Reference Committee in their *Review of the National Classification Scheme: achieving the right balance* that the Classification Review Board should become the final arbiter of classification decisions for all media in Australia in order to ensure uniformity and consistency (p. ix).

As noted earlier, the Unit supports the recommendations of the Senate Legal and Constitutional Affairs Reference Committee in their *Review of the National Classification Scheme: achieving the right balance* to provide greater safeguards over the existing provider self-regulation:

- Recommendation 23 that industry codes of practice under current self-regulatory and co-regulatory schemes, including those under the *Broadcasting Services Act 1992*, the ARIA/AMRA Labelling Code and the advertising industry, should be required to incorporate the classification principles, categories, content, labelling, markings and warnings of the National Classification Scheme. The adoption of these measures by industry should be legally enforceable and subject to sanctions.
- Recommendation 24 that industry bodies wishing to exercise classification decision-making functions should be required to be accredited by the Australian Government.
- Recommendation 25 that the Classification Board should be responsible for the development of a content assessor's accreditation, including formalised training courses for all industries covered under the National Classification Scheme.
- Recommendation 26 that the accreditation of content assessors should be subject to disqualification as a result of poor performance.
- Recommendation 27 that transgressions of classification requirements within codes of practice by industry participants should, if verified by the Classification Board, be punishable by substantial monetary fines.

Question 17. Would co-regulatory models under which industry itself is responsible for classifying content, and government works with industry on a suitable code, be more effective and practical than current arrangements?
The Unit does not support a model in which industry alone would be left to carry out classification. Given the serious harm that can be inflicted in the production of material such as child sexual abuse material and the harm that can result to those accessing material that would be classified RC, Government has a responsibility to protect the community and uphold basic human rights standards. Government needs to play a role in directly regulating content that is likely to involve harm and in ensuring that any industry co-regulation is carried out effectively and in compliance with the National Classification Scheme.

Industry cannot be solely relied upon to classify all content. Auditing is required with any industry classification. The Unit notes the earlier example it provided of Amazon selling online a guide to sex between adults and children and initially defending its decision to do so. The Unit further notes the evidence provided to the Senate Legal and Constitutional Affairs References Committee of failings in industry self-compliance with serial classification

declarations and display of restricted publications.[92] The Classification Board revoked the classification of seven adult publication titles in the 2009/2010 period from a total of 60 serial classification declarations, an industry self-regulation failure rate of over 10%.[93]

Question 20. Are the existing classification categories understood in the community? Which classification categories, in any, cause confusion?
As the Unit has advocated for access disruption to Refused Classification content on the Internet, anecdotally it has found very few members of the community understand the RC category. They understand that access to child sexual abuse material is illegal. However, there is a high level of confusion between visual material that would be classified R18+, X18+ or RC. A strong part of the concern the Unit has experienced to ISPs being required to disrupt access to RC material is confusion as to what this category would include. There is suspicion in some parts of the community about the role the wider community should play, through government, in restricting the 'right' of individual adults to access whatever they like regardless of the harm this may cause to themselves or others.

It appears the poor understanding of the RC and X categories stems from the fact most people do not know what material is classified in these categories as they are not consumers of materials in these categories (and in the case of RC material, should not be consumers of such materials). There is greater familiarity with other classification categories as they are regularly experienced by most members of the community.

Question 24. Access to what content, if any, should be entirely prohibited online?
The Unit supports the existing definition of RC as adequately setting boundaries around what content should be entirely prohibited online. It is necessary that such a category will always require some level of judgement to be applied and it is not possible to provide a black and white definition in all cases. For example, material that describes or depicts rape in a way that discourages this criminal activity is very different to material advocating rape or providing information to commit rape and escape detection by law enforcement. For example, the Unit would view the online games referred to earlier in the submission (where players rape female cartoon characters) being classified as RC.

It is reasonable the RC category actually allow for shifts in community standards over time. However, it should also be consistent with the international human rights standards that Australia is a States Party to. For example, child sexual abuse materials are prohibited in 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 complaints the Unit has heard in relation to the current RC category is that it does not permit access to material instructing in suicide, euthanasia, criminal acts of graffiti or the safe use of illicit drugs. The Unit has not been able to ascertain the accuracy of these claims. However, even if accurate, in all these cases the Unit believes access to such material, especially in an unregulated way, is more likely to result in harm within the community than good. The Unit would hold access to such material is reasonably a decision the society should make, through a democratically elected Parliament, and if made available should be subject to regulation. As a matter of principle, it should not be left to individuals in a democratic society to be able to freely decide which laws they will abide by and which to ignore. The Unit notes in some of the studies of offenders, they argue it is not justifiable for

[92] Senate Legal and Constitutional Affairs Reference Committee, 'Review of the National Classification Scheme: achieving the right balance', June 2011, Chapter 4.
[93] Senate Legal and Constitutional Affairs Reference Committee, 'Review of the National Classification Scheme: achieving the right balance', June 2011, p. 34, para. 4.6.

the community to impose its standards on them in what they can access. The Unit holds that a society has the right to set boundaries on what people access, especially in relation to the need to uphold the human rights of others who may be harmed.

Question 25. Does the current scope of the Refused Classification (RC) category reflect the content that should be prohibited online?

The Unit supports the existing scope of the RC category as setting the boundaries on what content should be prohibited online. However, the Unit notes that ISP 'filtering' through a list of URLs only represents access disruption. Despite it being relatively easy to by-pass through the use of a foreign ISP not subject to Australian requirements, its utility has other uses as was outlined in the Unit's answer to Question 12. In summary, an ISP based filter protects victims of sexual abuse from re-victimisation, disrupts the ability of commercial child sexual abuse providers to build up their customer base, disrupts the cognitive distortions of potential offenders and offenders seeking to access child sexual abuse material, assists police in combating child sexual abuse material online and assists in protecting minors and adults from inadvertently accessing content likely to disturb or harm them.

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