# **Chapter 3**

## Cybercrime and Internet Paedophile activity

#### The Australian Crime Commission and child sex offences

- 3.1 The Australian Crime Commission (ACC) observed in evidence to the Inquiry that while child sex offences and Internet pornography are not directly an ACC area of operation, the ACC co-ordinates all national criminal intelligence, and that includes intelligence regarding paedophiles and crimes committed via the Internet. Further, the incorporation of the Australian Bureau of Criminal Intelligence, into the ACC has given the Commission responsibility for information and projects which concern child sex offenders.<sup>1</sup>
- 3.2 Three main areas of concern to the Inquiry emerged during the Committee hearings:
- access to the Internet and its use to transmit pornographic child sex imagery;
- the 'grooming' in chat rooms by paedophiles which can end in actual contact with the child; and
- ease of access to material unsuitable for children.
- 3.3 The dangers to children emanate from two areas: the active seeking out of children for chat room activity, and the availability of unsuitable material on the Internet for children to view.
- 3.4 Associated with this activity are the problems of investigation, detection, gathering evidence and prosecuting. The ephemeral nature of Internet material, and the absence of any requirement for Internet Service Providers (ISPs) to retain records, demands swift action before the evidence disappears. While there is a general discussion of these issues in Chapter 2, this chapter focuses on the impact on paedophile cyber activity.

## The internet and anonymity

3.5 The evidence provided to the Committee demonstrated that the Internet has brought with it a global facility which allows paedophiles to extend their activities in a clandestine way. Reports of adults preying on children through the use of Internet 'chat rooms' have periodically featured on news bulletins, and were also referred to in the course of the Committee's hearings.<sup>2</sup>

<sup>1</sup> *Committee Hansard* 18 July 2003, pp. 6 -7

<sup>2</sup> e.g *Committee Hansard* 17 July 2003, pp. 30-31; *Committee Hansard* 18 July 2003, pp. 7-8; 16-20; *Committee Hansard* 21 July 2003, pp. 6-9.

- 3.6 The pace of technological progress allows more opportunities for paedophiles to use the Internet in more sophisticated ways. In his submission to the Inquiry, Mr Darren Brookes<sup>3</sup> noted that there has been significant change in the methods of operation of paedophiles in a short time. Mr Brookes gives the example of the development of the 'web cam' which allows live images to be broadcast to chat rooms and Internet computer conferencing (known as IRC or Internet Relay Chat).<sup>4</sup>
- 3.7 A submission from Mr Doug Stead, President of a Canadian Company 'Tri-M' related an example of an Australian on-line predator who was able to co-opt a Canadian child using relatively simple technology. The example also highlighted the co-operation between Australian and Canadian police in intercepting the perpetrator. <sup>5</sup>
- 3.8 The Australian Broadcasting Authority (ABA) also referred to the increased opportunities provided by the Internet for paedophile activity and noted that this has been a focus of concern for policy makers, the Internet industry and child welfare.<sup>6</sup>
- 3.9 In their submission to this inquiry, the National Child Protection Clearing House (which operates from the Institute of Family Studies) said:

The Internet has become a popular means of recruiting children for sexual purposes because it provides easy access to children and a reduced risk to offenders of being identified.<sup>7</sup>

3.10 Similar concerns were expressed by the Victoria Police:

Millions of child pornography images and movies are available on the Internet via news groups, peer to peer sites, chat channels ... A number of commercial organised rings have been identified and those sites have turned over many hundreds of thousands of dollars<sup>8</sup>.

- 3.11 The Committee observed that the anonymity of this environment also allows the formation of web-based communities in which material can be exchanged by likeminded individuals.
- 3.12 In his submission to the Inquiry, Dr Patrick Forde from the Curtin Business School observed that email remailers (where there is an interim mail address which does not trace back to the initiating address) or hidden peer-to-peer networks are

5 Submission no 3, pp.2-3

8 Committee Hansard, 17 July 2003, p. 37

Mr Brookes is a former lecturer at Goulburn Police Academy, and more recently was the Head of the Paedophile Unit (Interactive) in the United Kingdom. He is a Fulbright Scholar who is undertaking a PhD on the characteristics of Internet paedophilia at Washington State University.

<sup>4</sup> Submission no 2, p.5

<sup>6</sup> Submission. no 15, p.6

<sup>7</sup> Submission no 7, p.3

examples of advanced Internet devices which require considerable technical knowledge to use. (A peer-to-peer network is sometimes abbreviated to 'P2P'. It refers to any group of individual computers that can communicate with one another. Some of these operate undetected under the normal Internet structure, and are extensively used by paedophiles to distribute illegal and objectionable material.<sup>9</sup>)

### Pornographic imagery: Possession and Access

- There is also the associated matter of unsolicited material sent by email and the extent to which its presence on a person's computer, even unopened, can constitute an offence of possession of pornography.
- 3.14 In its submission, Electronic Frontiers noted that:

[Not only are] Internet users confronted with unwanted material, they also face the risk of criminal conviction for possession of material that came into their possession without their knowledge or consent. Generally, recipients of this type of material suffer in silence because if they report the criminal activity to law enforcement agencies, they risk being prosecuted for possession. 10

- 3.15 In evidence, it was claimed that recipients of unwanted obscene e-mails who had reported them to the police were then charged with possession of pornography.<sup>11</sup>
- 3.16 The Committee noted that the situation outlined in this evidence has the potential to criminalise activity which may not deserve that description. The issue which arises from this is: when can an email be said to be in the possession of a person? There are several possibilities:
- when it lands in the computer mailbox;
- when it is opened by the addressee;
- when it is downloaded by the addressee and saved and printed.
- 3.17 The issue of the nature of possession of material on computers was a recurring one throughout the Inquiry.
- 3.18 The Committee observed that the law on this area varies from state to state, and there is no Commonwealth legislation which is specifically directed at this area. For example, in New South Wales, the offence of possession of child pornography (Section 578B Crimes Act 1900 NSW), is a summary offence, and the maximum penalty is 2 years imprisonment or 100 penalty units (\$11,000).

10 Submission no 4, p. 3

11 Committee Hansard, 21 July 2003, p.59

<sup>9</sup> Submission no 8, p. 1

- 3.19 In contrast, the Committee noted that under section 70 of the *Crimes Act 1958* (*Victoria*), the offence of 'knowingly possess child pornography', is indictable, and the maximum penalty is 5 years imprisonment, with no option of a fine.
- 3.20 There is currently no similar Commonwealth legislation with the exception of the *Classification (Publications, Films and Computer Games) Act 1995*, which is very limited in scope to those items unclassified or those classified RC (refused classification).
- 3.21 The nationwide (and worldwide) disparity in offence provisions, defences, and penalties is a barrier to effective control of this material. Furthermore, the jurisdictional issues raised by Internet material being circulated around the country and around the world make efficient detection of its source extremely difficult and resource intensive.
- 3.22 The Committee notes with concern that the lack of consistent legislation in this area is an impediment to detection and prevention of these offences. The differences in penalties, and in the nature of what constitutes an offence can result in activities which when perpetrated in one jurisdiction are a minor offence, but when committed in another jurisdiction are more serious. Without consistent approaches across jurisdictions the ability to eliminate this behaviour is weakened. While it is clear that there are significant jurisdictional issues involved in developing and implementing a nationally (and internationally) consistent system of offences and penalties, the Committee considers it a matter of urgency to ensure as far as possible that there are consistent sanctions and penalties applied to these offences across the country.
- 3.23 In this context the Committee notes the evidence from the Attorney-General's Department that:

the government will introduce new offences and will provide a nationwide avenue to investigate, prosecute and punish those who use the Internet for trade in child pornography. These offences would carry a maximum penalty of 10 years imprisonment which [is similar to that which] would apply for bringing in hard copies through the customs barrier.<sup>12</sup>

3.24 The Attorney-General's Department indicated that the proposed legislative amendments will be released as an exposure draft. The Committee supports the release as an exposure draft and considers that it is important that the timelines for public discussion be sufficient for informed public consideration.

## Use of chat rooms by children

3.25 Computer literate children can easily use the chat room environment. There is currently no way of effectively preventing Internet chat room activity engaged in by paedophiles and their victims. The Victoria Police noted in their submission that many

paedophiles adopt the on-line profile of a young child, <sup>13</sup> and 'groom' them for later meetings, all of which goes undetected.

- 3.26 In evidence the Australian High Tech Crime Centre (AHTCC) told the Committee that the Internet can include hundreds of thousands of potential offenders. <sup>14</sup> The nature of the offence makes control imperative but the size of the problem militates against effective detection and prevention.
- 3.27 The NSW Police told the hearing that the United States Federal Bureau of Investigation engages covertly in chat rooms to identify paedophiles. <sup>15</sup> There is no shortage of offenders, but the problem is determining who is the most dangerous, and who should be targeted first. The Committee notes that implied in this is a method of determining a profile of those most at risk as well as those who are most likely to offend.
- 3.28 Some guidance was offered by the National Child Protection Clearing House (NCPCH) who stated in their submission to the Inquiry that the ease of access and the anonymity of the Internet made it a perfect environment for a paedophile to misrepresent himself as another child or friend or a 'caring parent figure' to vulnerable children
- 3.29 The NPC Clearing House cited some limited research from the U.S. which gives some indication of those who may be at risk as victims of Internet sexual offenders. The list of profiles includes:
- children with low self esteem;
- children who have been maltreated;
- immature children with learning or social problems;
- children over 14 who had been exposed to 'negative life events' (maltreatment or depression). 16
- 3.30 The NPC Clearing House also indicated similar research has been done on the profile of typical offenders, and while urging caution, cited a UNESCO meeting of experts on child abuse and the Internet which noted a recent increase in offences by people who are sexually indiscriminate and who use children if they are available.<sup>17</sup> In evidence, the NPC Clearing House added that parents often do not realise the extent to which children access the Internet in multiple ways.<sup>18</sup> This suggests to the

5 Submission n

<sup>13</sup> Submission no 25, p.1

<sup>14</sup> Committee Hansard, 21 July 2003, p. 16

<sup>15</sup> Committee Hansard, 18 July 2003, p. 84

Submission no 7, pp.3-4, citing Finkelhor and Wolak 2001, Petraitis and O'Connor 1999, and Mitchell et al 2001.

<sup>17</sup> Submission no 7, p. 4 also citing Arnaldo 2001

<sup>18</sup> Committee Hansard, 17 July 2003, p. 32

Committee that the supervision of a child's computer use is an important factor in the prevention of child exploitation and abuse by Internet paedophiles.

3.31 The Committee notes that in the United Kingdom, the Government has acted on the use of chat rooms by paedophiles to target children. The ABA informed the Committee that the *Sexual Offences Bill* [HL] would make using a chat room or similar place for the purpose of engaging a child in paedophile activity a special offence.<sup>19</sup>

### Access to unsuitable content by children

3.32 At its Melbourne hearing, the Committee observed that the availability of unsuitable material to children is an Internet access issue. At the Ninth Australasian Conference on Child Abuse and Neglect, held in Sydney on 24 to 27 November 2003 the potential risk of this access was illustrated in the paper entitled 'Child Protection and the Internet'. The authors noted disturbing research from the Canberra Hospital which:

showed that sexually aggressive children under ten years, who have not personally experienced sexual assault but who have had exposure to sexually offensive material, are being seen at an unprecedented level. <sup>20</sup>

- 3.33 The Committee notes there is a dilemma in allowing adult access to material which should be restricted for children, but not necessarily for adults.<sup>21</sup>
- 3.34 The Committee looked at what is available for parents to monitor and control their children's use of the Internet. The ABA told the Inquiry of a number of initiatives which it has established to promote community awareness of Internet safety in Australia. They include:
- Publications for parents and children regarding the safe use of the Internet.
- Cooperative arrangements with a number of bodies, including educational authorities to distribute this material.
- A web site.
- The registration of Internet Codes of Practice.
- A complaints mechanism which can result in websites originating in Australia being removed, and those originating overseas to an international organisation. This only applies to websites, and not to chat rooms.

<sup>19</sup> *Committee Hansard*, 18 July 2003, pp 15-16

Abstract of paper 'Child Protection and the Internet' presented by Dr Janet Stanley, Ms Cassandra Tinning and Ms Katie Kovacs at the Ninth Australasian Conference on Child Abuse and Neglect at website http://www.community.nsw.gov.au/accan/viewed on 15 December 2003

<sup>21</sup> Committee Hansard, 17 July 2003, p. 30

- 3.35 The Committee was also informed about a number of filtering software packages, which can be installed on computers to block access to unsuitable material, and prevent unsuitable material reaching the user. The filters currently available do not block chat room activity.
- 3.36 There were reservations about the effectiveness of these programs. The ABA's pamphlets warn of the limited effectiveness of filters, and in evidence the ABA added that they are not the sole tool upon which parents should rely:

[A filter] either shoots too wide or it is too narrow. It lets in material that it should not, and it stops material that you would not be offended by if your children saw it.<sup>22</sup>

- 3.37 This view was also held by Symantec Australia who told the Committee that:
  - ... you will never get 100 per cent risk reduction ... you will never be able to filter out all the pornography, the bomb-making recipes, the nasty pictures or anything that is used in chat rooms ... The tools are not strong enough to be able to manage heuristics or artificial intelligence to the level that people would like to see. <sup>23</sup>
- 3.38 Symantec also took the view which was supported by other witnesses and submittors on this subject that there is no substitute for parental supervision of children's Internet use.<sup>24</sup>
- 3.39 The Committee also considers that while it is clear that Internet filtering devices can be of some use in supporting parents in their supervisory task, the evidence has demonstrated that solely to rely on these to prevent children seeing and having access to inappropriate material still risks exposing the children to that material, or inhibits adults' access to items which may be quite suitable for them, but not for their children.
- 3.40 The Committee observed that, while there are educational initiatives which publicise the dangers of children's unsupervised use of the Internet (such as those pursued by the ABA), they do not appear as yet to be as widely disseminated as they need to be in order to be effective. The Committee notes that such a public education role is not one that falls within the parameters of the ACC's functions. However, in this context the Committee is particularly mindful of the terms of The United Nations resolution no. 55/63: 'Combating the Criminal Misuse of the Information Technologies' which clearly states that the public should be made aware of the 'need

23 Committee Hansard, 18 July 2003, p. 76

For example, Submission nos 4, and 15; Committee Hansard, 18 July 2003, p.86.

<sup>22</sup> Committee Hansard, 18 July 2003, p. 21.

to prevent and combat the criminal misuse of information technologies.' <sup>25</sup> (See Appendix 4).

- 3.41 While acknowledging that there are always financial constraints on providing published resources and advertising, the Committee believes that an awareness by parents of the potential criminal use of the Internet, and in particular chat rooms, in relation to children should be promoted. Equally, there is a need for parents to accept that they have a responsibility to supervise and monitor their children's use of the Internet. The evidence provided to the Committee supported the involvement of parents in their children's Internet usage, as a measure to prevent their exposure to unsuitable content.
- 3.42 The Committee is of the view that parents and children alike need the information. It commends the work the ABA is undertaking in this respect but that work needs to be reinforced. The Committee believes that reinforcing the ABA's message should take place across a number of media and should include a community service program.

#### **Recommendation 2**

The Committee recommends that the Government investigate partnerships for establishing a multimedia public education campaign on the risks associated with and the safe use of information technology by children, including parental supervision.

## Investigating and detecting

- 3.43 The investigation of Internet paedophile activity is a challenge for law enforcement agencies and raises privacy issues which were of concern to some witnesses.
- 3.44 The Committee is aware that if inappropriate activity on the Internet which is designed to entrap children is to be a criminal offence, evidence must be obtained which will secure a conviction. The Committee heard that to obtain evidence of paedophile chat room activity, police need to have the capacity to monitor or intercept the person's Internet use.
- 3.45 There are several ways to undertake criminal investigations which involve the use of information technology. Searches can be conducted to check information stored on the user's hard drive but PricewaterhouseCoopers described a system which uses an Internet Service Provider's (ISP) log of those who have surfed the Internet through that particular ISP. It is possible to trace both the caller and the called.<sup>26</sup>

-

Resolution no. 55/63, paragraph (h), of the Un General Assembly, 81<sup>st</sup> Plenary Meeting 4 December 2000; http://ods-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17

<sup>26</sup> Committee Hansard, 21 July 2003, p.67

- 3.46 However, ISPs are not required to retain their logs for any period of time. Historically this was because of the expense and space required to store them; the cost has diminished, and it appears to be feasible to have ISPs retain records at least for a short time. While there is no legislative requirement on ISP to maintain records, there is a draft Code of Practice which seeks to establish a co-operative working relationship between the Internet industry and ISPs (see paragraphs 2.66 to 2.68).
- 3.47 The Committee heard that there is already a code of conduct for commercial television, and for Internet service providers. However, there was a view that self regulation may not be successful in protecting children effectively from undesirable contact and material. In a submission to the Inquiry, the National Child Protection Clearing House recommended:

Internet Service Providers should be required to take greater responsibility for the protection of children by moving from self-regulation to quasi regulation or explicit government regulation, both of which are common in other industries in Australia.<sup>27</sup>

- 3.48 The submission also states that the (limited) number of websites explored in compiling the submission suggests that the Australian Internet Industry does not have a significant presence in addressing child protection issues.<sup>28</sup> One solution proposed was a system of ISP accreditation which would require certain levels of operating standards such as the filtering of certain material.
- 3.49 In their submission to the Inquiry, Mr Julian and Ms Leanne Winch drew the Committee's attention to the availability in the United States of a free server-based filtering system, which customers can choose to activate as soon as they sign on to the service. The submission notes that some service providers do offer this option but recommends that free optional server-based filters should be available, and service providers who fail to offer the filter should be heavily fined.<sup>29</sup>
- 3.50 Under the current arrangements, the Committee is concerned that it appears that self regulation by the Industry in this area may not be adequate. The Committee is of the view that honouring the terms of the Code of Practice requires both an acceptance of the code and the resources to discharge the requirements. The Committee received a copy of it during the Inquiry. However, it did not receive any evidence from ISPs. This was despite attempts by the Committee to speak with some ISPs operating within Australia. The Committee therefore must question the level of acceptance of the code within the industry.
- 3.51 Notwithstanding the industry's ability to comply with Law Enforcement Agencies' (LEA) requests for records there can be little argument that the collection

28 Submission no 7, p 9

29 Submission no 31, p.1

<sup>27</sup> Submission no 7, p.1

of such evidence is critical to prosecution. While it also presents a useful avenue for detection, the records are not the only avenue.

3.52 The AHTCC told the Committee of some of the strategies used abroad. Federal Agent MacGibbon told the Inquiry that an officer from the AHTCC had been examining procedures in the UK and the US:

The Internet means that you have hundreds of thousands of potential offenders in these chat rooms, and you need to know how to filter it down to a reasonable number so that you can have the level of suspicion or belief about it that lets you do the extra, more intrusive investigative aspects — how you locate that offender and how you look at engaging them in the physical world ...

... the [Innocent Images Program is the] FBI's main child sex investigations area and which also maintains a proactive online presence, posing as children online and engaging people in conversation. <sup>30</sup>

- 3.53 The Committee notes from the AHTCC's evidence that it is allocating a high priority both to the legislative and forensic aspects of this criminal activity.<sup>31</sup>
- 3.54 The NSW Police told the Committee that the American FBI engages covertly in chat room activity in order to track paedophiles. However, the American experience has been that there is such a proliferation of paedophile activity in chat rooms, that the agents have to select which offenders they will target.<sup>32</sup>
- 3.55 In evidence, Mr Gregory Melick observed that:

To randomly try to pluck something out of the ether and interpret it to see what is going on will be almost impossible. You also have the other problems of encryption and steganography.<sup>33</sup>

- 3.56 The US experience and Mr Melick's comments suggest that any requirements placed on ISPs to provide records should be targeted with some knowledge of illegal behaviour rather than a global search the ISP records. The responsibility placed on ISPs is therefore reduced and the resource requirements in searching the material seized is also limited.
- 3.57 Any seizure of the users' hard drives for evidentiary data could also be obtained in the context of pre-existing knowledge. For law enforcement agencies to direct a more 'intrusive investigation' to a wide spectrum of users would be a costly exercise with a doubtful return.

31 *Committee Hansard*, 21 July 2003, p.16 -17

32 *Committee Hansard*, 18 July 2003, p. 84-85

<sup>30</sup> Committee Hansard, 21 July 2003, p.16

<sup>33</sup> Committee Hansard, 21 July 2003, p. 32

- 3.58 The Committee notes that seizure of suspect computer hard drives and associated records is already available under Commonwealth and State search warrant legislation.
- 3.59 The NSW Police suggested the following possible legislative changes to assist in the detection and prosecution of paedophiles: <sup>34</sup>
- amendments to the telephone intercept legislation to include child pornography and enticement;
- amendments to NSW legislation concerning possession and publication of child pornography, and
- a new offence (similar to that being contemplated in Britain and discussed in paragraph 3.31), of online grooming and luring for the purpose of a sexual act.
- 3.60 The Committee notes that the last of these initiatives in particular has considerable potential for affecting online chat room activity. However, the problem of Internet paedophilia is an interstate and national one, as is cybercrime generally, and the legislative solutions to be most effective must be nationally consistent and if possible, internationally.
- 3.61 Further, there was some concern that to extend the LEAs' powers to intercept and seize in any way would raise issues of civil liberties and rights to privacy which currently exist. The ACC itself acknowledged this in evidence.<sup>35</sup>
- 3.62 In their submission Electronic Frontiers Australia indicated that any proposal which would increase powers for law enforcement agencies should be carefully scrutinised. EFA noted that there are already provisions (under the *Telecommunications Act 1997*) which allow some law enforcement agencies to make certified and uncertified requests to a carrier or carriage service provider for disclosure about telecommunications users.<sup>36</sup> EFA considers that any extension of these powers would not be justified in the absence of evidence that the measures would have the intended impact on criminal activity.
- 3.63 The Committee did not form the view that an increase in the interception powers of law enforcement agencies to investigate paedophile activity on the Internet was warranted but it was concerned that there still is no uniform legislation governing the collection and use of evidence. The Commonwealth *Evidence Act 1995* was intended to be adopted co-operatively by all states and territories; however the Commonwealth Act applies only to Commonwealth investigations, and has been adopted as far as possible in New South Wales and applied to State investigations. The Committee was advised that Victoria is examining the proposal.<sup>37</sup> However, the

35 Committee Hansard, 18 July 2003, p.5

37 Committee Hansard, 17 July 2003, p.17

<sup>34</sup> Submission no 17, p.2

<sup>36</sup> Submission 4, p.10

Committee notes that a report was prepared for the Victorian Parliament in 1996 recommending adoption of the Commonwealth and NSW Evidence Act models<sup>38</sup> and it is yet to be implemented.

#### **Recommendation 3**

The Committee recommends that the Commonwealth Attorney-General liaises with the State and Territory Attorneys-General to ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime, which is in accordance with Australia's international obligations.

3.64 The Committee was advised that there are proposals for legislation at Commonwealth level. <sup>39</sup> It considers that, given the international experience of the proliferation of predatory paedophile behaviour using information technology, the new offence relating to 'online grooming' and luring of children for the purpose of a sexual act (proposed in the British legislation) would be a useful addition to the statute books in Australia

#### **Recommendation 4**

The Committee recommends that as part of its legislative package to detect and prosecute those who use information technology for the trade of child pornography, the Government introduce a new offence relating to luring and grooming children for sexual purposes.

3.65 Finally, the Committee notes the suggestion by PricewaterhouseCoopers relating to a keystroke logger. This logger can record every single keystroke, and thus trace the Internet activity of the user. However, the legality of this device has yet to be tested and the Committee suggests that the matter warrants further examination.

## National register of child sex offenders

3.66 It is clear to the Committee that in the light of the expense involved in this area of investigation, that resources need to be focused where they will obtain the most effective results. The Committee heard that one way this could occur would be in cases:

involving the prosecution of individuals who may have attracted the attention of law enforcement for other, perhaps unrelated reasons. In the course of investigation the evidence of other illicit materials has been found

<sup>38</sup> Report of the Scrutiny of Acts and Regulations Committee, Parliament of Victoria, 'Review of the Evidence Act' 1996.

<sup>39</sup> Attorney General's Department, Submission no 21 and *Committee Hansard*, 21 July 2003, pp 73ff.

on their computer, perhaps leading to a trail of other offenders with whom that other individual may have been in contact.<sup>40</sup>

- 3.67 The Committee considers that a national register of Child Sex Offenders would be useful in this process. The Committee is aware that the NSW Government has a database of child sex offenders which includes their names, addresses, employment and car registration details. The register is not public but is available to law enforcement agencies. Recently a meeting of Australian Police Ministers agreed to the establishment of a similar national database. The register will also allow Australia to endorse international child protection agreements.
- 3.68 The Committee was aware that the development of a national database could result in a number of situations having the potential for unintended consequences: for example, where somebody appears on the register because they were convicted under age of consent laws, rather than arguably more serious, and/or aggravated sex offences. However, the Committee, having discussed the matter with officers from the Attorney-General's Department, is confident that sufficient safeguards and redress would be included in any such register, particularly for those who might find themselves in that position. 42

#### **Conclusion**

The Committee notes that in relation to paedophiles, and children's access to unsuitable material on the Internet there are initiatives which focus on prevention and protection. The international experience suggests that information technology has been readily adopted by those who are involved in both the purveying of child pornography and the pursuit of children for sexual purposes. To assist in the detection and prosecution of these offences in Australia, the Committee has made a number of recommendations in relation to this aspect of the inquiry. However, the Committee believes that the most significant role for the ACC is in intelligence collection; the problem is, by its nature, international and subject to the vagaries and priorities of the law of other jurisdictions.

<sup>40</sup> Committee Hansard, 21 July 2003, p.2

<sup>41</sup> Committee Hansard, 21 July 2003, p.81

<sup>42</sup> Committee Hansard, 21 July 2003, p.81