TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 296 April 2005

# International Police Operations Against Online Child Pornography

Tony Krone

*Online child pornography is an unintended aspect of the widespread adoption of information and communications technologies. Child pornography involves the sexual abuse of children on a global basis. It appears that a once limited trade has seen remarkable growth, with the potential to intrude into the homes and workplaces of all those connected to the internet. Occasionally, exposure to this form of pornography may be unintended, but in most cases it is deliberately sought out, retained and traded worldwide. There have been many instances of law enforcement action, both locally and internationally, targeting those involved in the possession or distribution of online child pornography, some of which have involved thousands of suspects. This paper looks at 31 well-publicised operations and considers the law enforcement implications of these for future operations. It starts to fill a significant gap in our understanding of online child pornography.*

**Toni Makkai**
**Director**

The amount of media attention given to the issue of child pornography has risen dramatically. A search of a global English-language newspaper archive showed that between 1976 and 1989 there were 2,095 articles that referred to child pornography, between 1990 and 1994 there were 4,573 articles, between 1995 and 1999 there were 21,507 articles and between 2000 and September 2004 there were 51,270 articles (Factiva 2004). To some extent, the results of the search are affected by changes to database recording practices over time. The dramatic increase in media coverage also reflects a number of other developments: the proliferation of material through the use of digital information and communications technologies; the introduction in many countries of specific offences of possessing child pornography; increased police activity in response to new laws; and a fascination with the aspects of international networking and the numbers of persons involved.

There has been a steady stream of reports of various police operations that have led to the identification of tens, hundreds and even hundreds of thousands of possible suspects, involving a confusing array of individuals, networks and police operation code-names. This paper analyses major operations that have been reported since the early 1990s following the advent of the internet and the widespread enactment of child pornography possession offences.

## Methodology

The following English-language sources were searched for reports of police operations against online child pornography:

- the Factiva database of English-language newspapers from 1976 to 2004;
- an Australian media digesting service, a Google media alert service, the Cybercrime-alerts service and the Computer Crime Research Center alert service (to collect reports in the period from August 2003 to September 2004); and
- governmental and non-governmental agency reports on the policing of online child pornography.

Because this research was based on English-language searches, the material derived is principally from Australian, Canadian, United States and United Kingdom sources. The research does not seek to provide a comprehensive global survey or a representative sample of police operations against online

AUSTRALIAN HIGH TECH CRIME CENTRE

ISSN 0817-8542

ISBN 0 642 53876 X

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends & issues in crime and criminal justice series, visit the AIC web site at: http://www.aic.gov.au



**Project no. 0074**

child pornography. This study provides a basis for analysis at least for those police operations that have been reported on.

The reports considered are not exhaustive. Media reports must be treated with caution, as they may be incomplete or misleading. The details of the matters considered here are therefore drawn from a variety of sources wherever possible. Information, such as the number of persons involved as suspects, persons arrested and persons convicted, should be treated as indicative only. Other limitations of the material presented are: many networks are international and span differing laws against child pornography; media attention is directed to major cases; and there are too many police stings to catalogue here.

Given that policing in relation to child pornography is usually covert and may involve intelligence gathering rather than leading to specific arrests, it is acknowledged that publicised operations represent only a portion of police work in this area. Information provided in the public domain may be limited so as not to compromise ongoing investigations. Issues that are potentially sensitive include the manner of offending, the means of police detection and investigation and even the severity of the offences. This paper has been prepared in consultation with the AHTCC and is informed by that process. Online security issues and obstacles to police investigation are only described in general terms so as not to provide a manual for offenders.

The purpose of this paper is to place various reports of online child sex abuse image offending into perspective, to provide an analysis of trends, and to draw out the implications for law enforcement. The police operations can be categorised according to whether the offenders targeted have been involved in networked behaviour or not, and the types of networks that exist. This paper identifies four distinct targets of investigation that emerge from the available reports: individuals, covert groups, web site subscribers and those caught in police stings. Each of these will be discussed in turn, with reference to major operations reported.

## Individuals

Individuals may possess digital child pornography without being involved in networked behaviour. According to Taylor & Quayle (2003), a large quantity of child pornography was produced in the 1970s and has been circulated worldwide since then. Individuals may possess digital child pornography that they have converted from non-digital formats. Others may produce new material such as text, photographs and film in digital format for personal use. The use of child pornography by individuals may come to police notice in a number of ways (Smith et al. 2004: 71–74):

- a complaint from a victim of actual physical abuse may lead to the discovery of child pornography produced in the course of committing offline abuse, or sourced elsewhere and used as part of the sexual repertoire of the offender for self-stimulation or to 'groom' a child for sexual abuse;
- another person with access to the defendant's computer may discover the offending material, for example through sharing physical space at home or in an office, or as a computer repairer; and
- a hacker may look remotely at the defendant's computer online.

A notorious case of an individual prosecuted for possession of child pornography is that of Paul Gadd, also known as Gary Glitter. In 1999, Gadd was convicted of possessing some 4,000 pornographic photographs of young children and sentenced to four months imprisonment. He had left his computer at a computer repair shop. The technician discovered child pornography files in the course of effecting repairs and reported this to the police (BBC News 1999).

## Covert groups

A number of police operations have targeted covert groups of offenders. Those involved may come to police attention in the ways suggested above for individuals. In addition, the discovery of one person in a group may lead police to other members through the use of computer forensic techniques, or through evidence disclosed by identified group members. Alternatively, police may obtain intelligence about the existence of a group and use forensic procedures to identify its members.

The scale of groups and their visibility is often a function of the ways in which they communicate, as shown in Table 1. This includes wide, anonymous, large-scale applications and narrower, small-scale applications. Covert groups have varying levels of security in place, depending on how widely those operating them wish to reach people interested in their content. Covert groups often employ sophisticated security measures in order to avoid detection or infiltration. Some group members are prepared to abuse their own children, further limiting the potential for exposure, as was the case with the group exposed in Operation Hamlet (Weiss 2003).

Non-members, including internet service providers, may discover a group and report it to police. In some instances, the police may uncover a group through covert operations. Connections to a group may also be made through the investigation of individual allegations of offline child sexual abuse.

As Taylor and Quayle (2003) indicate, some, but not all, of those with a sexual interest in children engage in compulsive behaviour in relation to collecting images of sexual abuse. This often leads to those persons being involved in more than one group to satisfy their craving. At times, police will investigate a person as part of one group and uncover other groups through that suspect. Very often there will be no indication at the commencement of an investigation as to which suspects are more likely to be members of multiple groups. Intelligence-sharing and international police cooperation in the investigation of networked offending is therefore important.

The number of people involved in child pornography is difficult to determine. Often figures are given for 'records' or 'subscribers' uncovered by police investigators. This does not equate to the actual number of individuals involved. To the extent that other groups may exist it is an under-reporting. Where separate records in fact relate to the same individual, then there will be an over-reporting of persons involved. Because the records uncovered by police cannot always be equated with separate individuals, the term 'lead' is used in this paper wherever a number has been reported, without indicating whether it represents the number of actual suspects involved.

**Table 1: Communication technologies**

| Technology | Characteristic |
|---|---|
| World wide web | Web sites provide online access to text and multimedia materials identified and accessed through the uniform resource locator (URL). |
| Usenet | A distributed electronic bulletin system. Many newsgroups are dedicated to sharing digital images. |
| Peer-to-peer file sharing | Internet applications operating over peer-to-peer networks enable direct communication between users. Used largely for sharing of digital music, images and video, applications include BearShare, Gnutella, LimeWire and Kazaa. |
| Email | Email allows the transmission of messages over a network or the internet. Users can send emails to single recipients or broadcast them to multiple users. Email supports the delivery of attached files, including image files. |
| Mailing lists | Groups based on a centrally maintained email mailing list of persons sharing a mutual interest. |
| E-groups | Usually centrally controlled groups that communicate collectively by email, but which may also offer other services on either an opt-out or opt-in basis. |
| Instant messaging | Instant messaging is not a dial-up system like the telephone; it requires that both parties be on line at the same time. Users may exchange files, including image files. |
| Chat and internet relay chat | Chat technologies allow computer conferencing using the keyboard over the internet between two or more people. |

Adapted from: Koontz 1993: 7; Ferraro & Casey 2005: 21–40

The most notable investigations in the category of covert groups are known by the names Starburst, Blue Orchid, Candyman, Artus, Landmark, Cathedral (Cheshire Cat in the United States), Twins, Hamlet and Orchid Club (see Table 2). While the numbers of leads and arrests need to be treated as indicative only, the largest number of reported leads were in a series of operations beginning in 1992 with 900 members of the Longarm bulletin board system, followed in 2001 by the 6,700 members of the Candyman groups, the 10,000 addresses connected to Landmark and, in 2003, the email-based Marcy group of 26,500 users. These large groups were made possible by the extended reach of communication facilities such as bulletin board systems, newsgroups and email that are not limited to real-time exchanges.

Four groups involving fewer than 50 leads gained prominence in the period between 1995 and 2003. These tighter groups involved peer-to-peer or real-time chat room communications rather than bulletin boards. They also tended to use stricter access controls with passwords and other forms of security. However, they included people prepared to boast of their exploits. In the Starburst operation in England in 1996, police were alerted to the activities of Father Adrian McLeish of Durham, who anonymously admitted on the internet to his sexual activities with children. McLeish was identified and subsequently convicted on representative counts of indecent assault committed on four boys; two were aged less than 10. When the police raided his presbytery they found the largest collection of child pornography to have been seized at that time (Akdeniz 1997).

In the middle-sized groups the number of reported leads ranged from 91 to 399. The 91 suspects identified in Operation Innocent Images in 1992 used bulletin boards to communicate. The W0nderland club, with some 180 suspects reported worldwide, was a relatively large clandestine group. It had an entry requirement designed to bind each member to the secrecy of the group in that each member was required to submit 10,000 new child pornography images to join. This form of mutually assured destruction for members meant that obtaining offender cooperation could be a tremendous breakthrough in an investigation. It also raises the prospect of group members going to extraordinary lengths to prevent information leaking from any members. In the Zandvoort group one member allegedly killed another in Italy. Police had attended the apartment of the deceased member following his death and initially had not noticed anything suspicious. However, they were alerted to the existence of the group when other members of the group were caught trying to steal the deceased's computer from the apartment (Akdeniz 2001a). In Operation Twins, British police uncovered a 12-year-old girl being sexually assaulted by her father in the Republic of Georgia. The group employed a number of sophisticated security measures.

In this category of covert groups there are 16 operations shown. In 10 operations the figures given refer to the number of leads, and amount to 45,685. The figures given for persons arrested total 692.

## Web site subscribers

Web sites are the most visible means of gaining access to child pornography and they provide the widest coverage. A key element in the provision of web site access is profitability for the persons providing the offending web content rather than the sharing of a common interest among offenders. Web site subscriber groups, as shown in Table 3, are primarily based on a provider–consumer relationship.

Large numbers of people have become enmeshed in sites that offer, either exclusively or partially, online child pornography. Web site subscribers can be distinguished from smaller specialised groups on the basis of the relative ease of access. It may be that subscribers are less experienced offenders. Operation Auxin in Australia (Fairfax Digital 2004) shows that many offenders were willing to sign up with their personal credit card details to obtain access to web sites containing child pornography.

In 1996, police in San Jose investigated a complaint against a man who had sexually molested and photographed a 10-year-old girl at a children's party given by that man's adult daughter in her home. It was discovered that the images had been transmitted via the internet to members of what turned out to be the Orchid Club. The investigation into that club extended to a number of countries including the UK, where a search warrant was executed on the home of a man in East Sussex in 1998. Examination of his computer revealed links to the Orchid Club and, with the cooperation of the offender, the police uncovered computer links to the W0nderland Club. The W0nderland Club was a group of about 180 persons using password protection and encryption to hide their activities. Members of the Orchid Club and the W0nderland Club were pursued in a worldwide police investigation. Subsequently, in 2001 investigation of another group referred to as Roundtable led to the discovery of three previously unknown members of the W0nderland Club (Deutsch Welle 2002; Associated Press 1998).

In order both to secure payments and to protect the originators of the offending web sites, who are often in less well-regulated economies such as Russia and other former eastern bloc nations, intermediaries may be established in the United States or other regulated economies to collect fees on behalf of the web site owners and to repatriate those fees to them. Given the time involved in mounting a major investigation of a large group of persons who may have accessed a site containing child pornography, there will inevitably be a time lag between the point at which a site is first accessed and any subsequent police action. Because of the large numbers involved and the difficulty of properly investigating and establishing a sufficient case against all subscribers, other measures (such as formally cautioning suspects) have been introduced, for example in the UK in response to Operation Ore (Leydon 2003).

One web site subscriber operation involved the Landslide site in the US, which was a portal to about 300 sites located primarily in Russia and Indonesia. Subscribers provided credit card details to obtain access. In Operation Ore, which was the UK portion of this investigation, an offender was convicted in 2004 of the possession of over 495,000 images of children in a collection of 10–20 million pornographic images. Among those investigated was the former rock performer Pete Townsend whose name was placed on the sex offenders register in England following an official police caution in lieu of prosecution.

In this category of web site subscribers are nine prominent operations, six of which relate to the principal US investigation known as Landslide. Auxin is the Australian component of the Falcon operation. Using the main figure for Landslide and Predator leads, to avoid double-counting the numbers in subsidiary operations, the total number given for leads is 353,606. In relation to seven operations, figures are given for the numbers of persons arrested and the combined figure for arrests is 6,601.

## Police stings

Police sting operations involving police actively soliciting offenders on the internet are shown in Table 4. The first most notable sting operation was mounted in the US in Operation Rip Cord in 1997. Rip Cord commenced after a bookseller involved in the adult pornography trade in New York approached the New York State Attorney General about the widespread availability of child pornography online. In conjunction with the US Customs Service, a sting was mounted in which law enforcement officials posed as trading partners online for the sale of child pornography. Some 1,500 leads worldwide sought child pornography from them.

The Italian police operation known as Amantideibambini shadowed an internet-based child pornography group based in Russia. Members of that group were enticed to join Amantideibambini and when the sting was conducted there were 1,032 subscribers under investigation. The sting was apparently set up to capture those accessing a Russian child sexual abuse site, which supplied hard-core video material. It was reported that the Russian site involved children abducted from orphanages, circuses and public parks who were filmed while being forced to perform sexual acts.

Operation PIN represents the adoption of a cooperative preventive approach by police from Australia, Canada, the UK and the US. In this ongoing operation the police maintain a 'honeypot' web site that presents itself as offering explicit child pornographic content. As browsers click

**Table 2: Covert groups**

| Year | Operation | Countries | Numbers |
|---|---|---|---|
| 1992 | Longarm | US investigation, Denmark-based group, Australia | 900 members; 34 arrests in US; 2 in Victoria |
| 1993 | Innocent Images | US-based | Initially 91 arrests as at 1997; in ongoing process over 10,500 investigations and more than 3,000 convictions by 2003 |
| 1995 | Starburst | Hong Kong, US, South Africa, Germany, UK | 37 worldwide; 9 in UK |
| 1996 | Orchid Club | US-based | 16 arrests in the US; members in 9 US states and 3 foreign countries |
| 1998 | Zandvoort | The Netherlands, Germany, Israel, Ukraine, UK, Russia, US | No detail |
| 1998 | Cathedral/Operation Cheshire Cat in the US (W0nderland Club) | Australia, Austria, Belgium, Finland, France, Germany, Italy, Norway, Portugal, Sweden, UK, US | 180 members; 107 arrests; 750,000 images; 1,800 videos; 1,236 children |
| 2000 | Blue Orchid | Russian-based, US, Denmark, Sweden, The Netherlands | 80 suspects; 4 arrested in US and 5 in Russia |
| 2001 | Candyman (3 Yahoo groups: Candyman, Shangri-la, Girls 12-16) | United States | 6,700 members of 3 groups: 103 arrests |
| 2001 | Artus | Germany | 46 suspects; 12 arrests in 10 countries; 3 members were previously unknown members of the W0nderland Club |
| 2001 | Landmark | UK and others | 1,500 newsgroups; 30 sites carrying paedophilia-related material; 10,000 internet protocol addresses (IPAs) accessing these sites; 400 IPAs distributing paedophilic images |
| 2001 | Operation Twins Odysseus in Europe | Australia, Belgium, Canada, Denmark, Germany, Italy, The Netherlands, Romania, Norway, Peru, Spain, Sweden, UK, US | Group of about 100; 50 arrests in 7 countries |
| 2002 | Eurololitas | Italy | 399 suspects under investigation |
| 2002 | Operation Hamlet | Denmark and 9 other countries | 45 children; 19 charged in US; 12 arrests in other countries |
| 2003 | Marcy (Magdeburg) | Germany | 26,500 internet users; 166 countries |

through screens warning of the explicit nature of the content, they come to a screen that announces that their attempt to obtain online child pornography has been tracked and will be reported to local police. The purpose of this operation is not simply to capture those who might come to this particular site but to undermine the presumed anonymity of the internet.

The police stings shown in Table 5 are representative of police investigations based on the monitoring of internet traffic. It is notable that the Greater Manchester Police in the United Kingdom made an early commitment to implement this type of monitoring activity. The numbers of arrests reported are similar to other types of operations investigating private groups.

## Conclusions

Of the four types of police operations, the targeting of web site subscribers tends to involve very large numbers of leads and suspects, which creates major logistical difficulties for the police. In the UK the police came under heavy criticism in relation to the time involved in resolving Operation Ore, which was associated with the US Landslide investigation. One difficulty for police is that even where credit card transaction records are available, further investigation is necessary to connect a suspect with the use of that card to obtain access to child pornography. While there is little doubting widespread community concern about online child pornography, investigation priorities must be set. In a wider sense, police must balance the allocation of resources to this one aspect of high tech crime with the need to deal with other high tech offences.

On the one hand, it is important to act quickly to capture ephemeral computer data such as ISP records, and on the other hand, careful and painstaking work is required to draw an investigation together and prove a link between an individual offender and an instance of offending. International and national law enforcement cooperation is important to share criminal intelligence concerning the operation of networks, to share investigative leads on individuals accessing child pornography, to work together to identify victims and to prosecute perpetrators of abuse offline who can be identified from digital images.

**Table 3: Web site subscribers**

| Year | Operation | Countries | Numbers |
|---|---|---|---|
| 1999 | Avalanche (US), ALSO Genesis (Switzerland 1,300 leads), Pecunia (Germany 1,400 leads) | US and 59 other countries | 250,000 subscribers; revenue of US$9.2m; profit of US$2.9m; 100 arrests in US |
| 2001 | Site-key | US (Dallas Texas, and Santa Clara California) | 23,000 customers; 51 convictions |
| 2002 | Ore | UK | 7,200 suspects; 4,100 searches; 3,500 arrests; 1,670 people charged; 1,230 convicted |
| 2002 | Amethyst | Republic of Ireland | 100 suspects |
| 2003 | Snowball | Canada | 2,300 leads; 100 arrests |
| 2004 | Falcon | US, France, Spain, Belarus | Regpay – 100,000 leads; 270,000 credit card records; 2,300 arrests |
| 2004 | Viola | UK – Thames Valley Police Operation | 200 suspects |
| 2004 | No detail | Czech Republic | 100 customers |
| 2004 | Auxin | Australia | 706 suspects; more than 150 arrests as at 30 Sept 04 |

There is also a need to maintain confidentiality in the midst of an investigation of possibly linked offenders.

The civil liberties implications of law enforcement activities against online child pornography must be considered. In this respect it is important to ensure that the type of material being investigated is clearly child pornography and that the exercise of powers of search and seizure and of arrest are properly founded and based on evidence rather than impressions and speculation. However, evidence of serious and widespread abuse may fall unpredictably from what at the outset, may appear to be a routine limited investigation. It is therefore necessary to consider how best to balance the competing interests involved while ensuring that children are protected most effectively.

Police stings and monitoring activities are a valuable supplement to other operations because they destabilise and disrupt notions of anonymity on the internet. Despite this value, it is important that police do not compromise their own integrity in order to secure convictions. While Australian law does not recognise a defence of entrapment, clear guidelines are required to prevent police breaking the law to obtain evidence, as this could lead to the possible rejection of that evidence in the subsequent prosecution of an offender. An informed public debate is also required as to how far the police should be allowed to go to catch those who seek child pornography online. Two quite separate issues in relation to the police keeping child pornography material require clarification. The first is the extent to which such material may be used for investigative purposes, or to identify victims of abuse and perpetrators shown in the images. The second is whether the police should be able to use any child pornography material for the purpose of conducting undercover operations.

Remarkably, there is limited publicly available and independently assessed data on global police operations against online child pornography, despite the large-scale nature of the problem. Only with greater understanding of existing police operations can we hope to achieve better outcomes in future operations. Important issues to address are to define

**Table 4: Police stings based on an active web presence**

| Year | Operation | Countries | Numbers |
|---|---|---|---|
| 1997 | Rip Cord (Tholian Web by US Customs Service) | US | 120 US suspects and 1,500 worldwide |
| 2000 | Amantideibambini | Italy | 1,032 subscribers to site; 1,491 charges |
| 2003 | Operation PIN virtual global taskforce | Australia, Canada, UK, US | Not available |

in detail the profiles and ways of offending of those caught out in the four different styles of police activity described above. We need to know more about interconnected offending and to discover how offenders operate within and between various groups. In addition, the large numbers quoted ought to be seen in perspective to enable a reasoned and rational response to this issue. The involvement of multiple jurisdictions means that continued police and other agency cooperation and information-sharing is required to ensure that police actions are effective and shown to be so.

## Acknowledgments

The Australian High Tech Crime Centre funded this research.

## References

AGI 2003. *Italy: huge police operation against paedophilia*. http://www.saferinternet.org/news/safer24.htm

Akdeniz Y 1997. The regulation of pornography and child pornography on the internet. *Journal of information law and technology* 1. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1/

——— 2001a. *International developments in regulation of child pornography on the internet*. http://www.cyber-rights.org/reports/interdev.htm

——— 2001b. *United Kingdom in regulation of child pornography on the internet*. http://www.cyber-rights.org/reports/ukcases.htm

——— 2001c. *United States in regulation of child pornography on the internet*. http://www.cyber-rights.org/reports/uscases.htm

——— 2003. *Regulation of child pornography on the internet*. http://www.cyber-rights.org/reports/child.htm

Ashcroft J 2004. Statement of Attorney General on the regpay child pornography indictment. Press release 15 January. http://www.usdoj.gov/opa/pr/2004/January/04_ag_021.htm

Associated Press 1998. *Disgrace follows child porn bust*. 7 November. http://www.ishipress.com/wonderla.htm

BBC News 1999. Glitter jailed over child porn. *BBC News* 12 November. http://news.bbc.co.uk/1/hi/uk/517604.stm

——— 2001a. Swoop on suspected paedophiles. *BBC News* 27 March

**Table 5: Police stings based on monitoring internet traffic**

| Year | Operation | Countries | Numbers |
|---|---|---|---|
| 2001 | Appal | UK – Greater Manchester Police | 48 arrests |
| 2001 | Barcela | UK | 14 arrests |
| 2002 | Magenta | UK – Greater Manchester Police | 27 arrests |
| 2004 | Baglan | UK – Greater Manchester Police | 45 suspects |

——— 2001b. Fourteen held in child porn raids. *BBC News* 30 October. http://news.bbc.co.uk/1/hi/uk/1627992.stm

——— 2002. Operation Candyman: investigating child porn. *BBC News* 13 September. http://news.bbc.co.uk/1/low/england/2255243.stm

——— 2003. Police to trap online paedophiles. *BBC News* 18 December. http://news.bbc.co.uk/1/hi/uk/3329567.stm

——— 2004. Internet porn police arrest 45. *BBC News* 14 July. http://news.bbc.co.uk/1/hi/england/merseyside/3892701.stm

CNN 1997. *FBI cracks down on child pornography on the internet*. http://www.cnn.com/US/9704/07/briefs.pm/fbi.child.porn/

Cullen D 2003. Typical child porn user is white male IT pro. *The register* 22 October. http://www.theregister.co.uk/2003/10/22/typical_child_porn_user/

Department of Homeland Security 2003. *Fact sheet: Operation Predator* 9 July. http://www.dhs.gov/dhspublic/display?content=1067

Deutsche Welle 2002. *Child porn ring busted* 21 March. http://www.dw-world.de/english/0,3367,1434_A_481259,00.html

End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT) International 2004. *Internet-based child porn ring that drew thousands is uncovered*. Press release 27 April. http://www.ecpat.net/eng/Ecpat_inter/IRC/newsdesk_articles.asp?SCID=1348

Fairfax Digital 2004. *Nationwide blitz on child porn*. 30 September. http://www.smh.com.au/articles/2004/09/30/1096401703339.html

Federal Bureau of Investigation 2004. *FBI Cyber Division arrest*. Press release 3 March. http://www.fbi.gov/pressrel/pressrel04/monroe030304.htm

Hancock J 2004. 1,491 charged in international internet pedophilia case. *Silicon Valley news* 28 October. http://www.operationlookout.org/lookoutmag/1491_charged_in_international_in.htm

Internet Hotline Providers in Europe (INHOPE) 2003. *INHOPE tip leads to breakup of largest global child porn ring*. Press release 20 September. http://www.meldpunt.org/files/INHOPE%20Press%20Release%20-%20Operation%20Marcy1%5B1%5D.pdf

Interpol 2004. *Interpol applauds Nordic raids on users of child pornography, pledges further cooperation and support for such operations*. Media release 26 May. http://www.interpol.com/Public/ICPO/PressReleases/PR2004/PR200423.asp

Koontz L 1993. *File sharing programs: users of peer to peer networks can readily access child pornography*. US General Accounting Office. http://frwebgate.access.gpo.gov/cgi-bin/multidb.cgi

Kyros K undated. *Operation Innocent Images*. http://cybercrimelawyer.com/pages/childporno/innocentimages.html

Leydon J 2003. Child porn-lite users to wriggle free from court hook. *The register* 16 June. http://www.theregister.co.uk/2003/06/16/child_pornlite_users_to_wriggle/

News24.com 2004. *Czech porn ring busted*. 29 April. www.news24.com/News24/World/News/0,,2-10-1462_1519547,00.html

Muriel D 2004. Child sex abuse back in focus. *CNN.com* 2 March. http://www.cnn.com/2004/WORLD/europe/03/02/child.porn/

O'Connor C undated. *Online service and child sexual assault*. http://hnb.dhs.vic.gov.au/commcare/yafsinte.nsf/obj/S3_26/$FILE/S3_26.PDF

O'Keeffe C 2004. Nationwide swoop followed FBI tip-off. *Irish examiner* 24 April. http://archives.tcm.ie/irishexaminer/2004/04/24/story399145757.asp

Reuters 1995. *British police break child pornography ring*. 26 July. http://www.cpsr.org/cpsr/lists/listserv_archives/cyber-rights/950802

——— 2000. *1491 charged in internet paedophile case*. http://www.ecpat.net/eng/Ecpat_inter/IRC/articles.asp?articleID=48&NewsID=12

Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Taylor M & Quayle E 2003. *Child pornography: an internet crime*. Hove: Brunner Routledge

US Immigration and Customs Enforcement 2004. *ICE arrests Clifton boy scout volunteer-substitute teacher for child pornography*. Press release 29 January http://www.ice.gov/graphics/news/newsreleases/articles/volunteerarrest.htm

US Postal Inspection Service 2001. *The US Postal Inspection Service teams with Internet Crimes Against Children Task Forces in Operation Avalanche*. http://www.usps.com/postalinspectors/avalanch.htm

Weiss D 2003. *Major child pornography stings*. 28 May. http://www.family.org/cforum/fosi/pornography/facts/a0026237.cfm



**Dr Tony Krone is a high tech crime research analyst in the Global, economic and electronic crime program at the Australian Institute of Criminology**

**General editor, Trends & issues in crime and criminal justice series:**
**Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601**
**Note: Trends & issues in crime and criminal justice are peer reviewed**