AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 97

Paedophile Internet Activity

Patrick Forde and Andrew Patterson

On September 2 1998 newspaper headlines highlighted a cooperative police action in 14 countries (including in Western Australia) which resulted in raids on the homes of about 200 suspected paedophiles. Images depicting sexual abuse and actual rape of young children formed a stockpile of hundreds of thousands of items. The study reported in this paper was conducted, with the support of the Paedophile Investigation Team within the Western Australia Police Service. The study found that paedophiles were using World Wide Web pages to proclaim their lifestyles, to disseminate information and to facilitate communication. It also found evidence of international paedophile organisation where Internet anonymity techniques are used to conceal identities.

This Trends and Issues paper offers suggestions to counter this activity. However, there is a need for reliable information and competent investigation because a sophisticated level of technological competency was demonstrated by many paedophiles. Indeed, paedophiles are expected to create closed Internet communities that will be difficult to penetrate, and the use of the Internet for criminal paedophile activity will pose a continuing challenge to Australian law enforcement.

Adam Graycar
Director

In 1995, the Australian report on "Organised Criminal Paedophile Activity" concluded that there was little evidence of paedophile organisation and listed the following points within its summary:

> *While very small paedophile-support groups operated openly in Australia in the 1980s there is no evidence they currently do so...*
>
> *There is no evidence to suggest that organised paedophile groups have ever resembled what are traditionally thought of as organised crime groups in size, aims, structures, methods, longevity and so forth. Many paedophiles offend in isolation. To the extent that two or more paedophiles group together to commit offences, the numbers involved have almost invariably been very small and the groupings very much ad hoc and on a peer-to-peer basis...*
>
> *More commonly, where there are contacts between paedophile offenders, they consist of loose informal networks of peer-to-peer contacts* (PJC on the NCA 1995).

However, the Internet provides paedophiles with the opportunity to organise informal networks and peer-to-peer contacts on a global scale. Operation Starburst was a 1995 British Police investigation that identified 37 men worldwide involved in child pornography on the Internet and in September 1997 US Federal and State authorities disclosed Operation Rip-Cord which found 120 American suspects with a further 1500 suspects worldwide (Akdeniz 1997).

For the relatively small cost of reorganising their activities around personal computer technology, paedophiles are able to operate internationally. How paedophiles use the Internet is an important consideration for enforcement agencies (Scipione 1997). "The proliferation and ready availability of child pornography

November 1998

ISSN 0817-8542
ISBN 0 642 24082 5

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au
or send an email to:
aicpress@aic.gov.au

through the Internet and on-line services, and the use of these services by paedophiles and sexual predators to target and recruit children for exploitation, represent new challenges to the FBI and the law enforcement community" (Freeh 1997). Calls to monitor the "Web" are appearing in newspapers (Cleary 1998). The purpose of this preliminary study was to observe paedophile Internet activity and to comment on techniques used by the Internet Paedophile Community (IPC).

Study Method

This exploratory observation was developed with the support of an Australian law enforcement agency. Over the period November 1996 to December 1997, paedophile Internet activities were observed. Australian occurrences of paedophile activity were immediately reported to authorities, as were investigations addressing certain international incidents. Unsophisticated search strategies were initially used to locate paedophile activity. As the study progressed a number of software tools were tested to improve efficiency. Although data was captured to support particular investigations, observed materials were not archived, in accordance with local authority instruction.

The observation process was limited to five components of the Internet and within those areas only widely available tools (browsers, newsreaders, and so on) were used, so as to simulate an Internet environment accessible to the public. The intention was to observe public paedophile activity. Controlled access Internet sites were not investigated. Only publicly accessible news-servers were used to observe newsgroups. Although one news membership was tested it was used to obtain an appreciation of membership processes. The Gopher, Listserv, BBS and world wide paging chat systems were not investigated. Finally, this study was conducted on a minimum cost basis.

For the purposes of this observation, paedophile material was defined as material located at Internet venues that self-proclaimed an emotional or sexual interest in children (for example, Girl-lover, Boy-lover, "pedo" stories, binaries or sex newsgroups). Within this context, paedophiles are defined as persons who are associated with paedophile materials. (For a discussion of paedophilia definitions, refer to Wood (1997a) and PJC on the NCA (1995). Also, for a discussion of cultural implications, see Grubin (1992) who argues that "whether a sexual behaviour is criminal differs not only between societies, but across time.")

How Paedophiles use the Internet

Paedophiles use the Internet to conduct their activities (for example create communication structures, distribute child pornography and to archive their collections). An IPC was observed using five components of the Internet. WWW pages, Electronic Mail (email), File Transfer Protocol (FTP), Newsgroups (News) and Internet Relay Chat (IRC).

The global nature of the Internet enables paedophiles to congregate at virtual locations that change according to circumstance. For example, at the beginning of the study most WWW pages proclaiming an interest in boys were located in Western Europe. However, Internet Service Providers (ISPs) started withdrawing services resulting in a period of upheaval with many pages relocating to Canada. This new venue did not last long. Towards the end of the observation period, pages had returned to Europe with new venues under development in Russia. Owners of these pages were obviously internationally connected and they constructed their pages so that transferring physical locations was a trivial consideration. Even so, forced page relocations indicated that finding sympathetic ISPs appeared to be a significant consideration for paedophile activists. A major strategy was to rally support under the umbrella of free speech and to construct mirror sites (duplicate pages at other locations). In addition, some declared a stance against child pornography and argued that their intentions towards children were platonic. However, this veneer was shattered by the suggestive nature of WWW picture galleries and reference links to child pornography (for example, sex stories and newsgroups where child pornography was distributed).

Many WWW pages displayed symbols of association and provided email addresses to encourage private communication. Linked resources provided paedophiles with "up-to-date" references to Internet locations. Two of the most conspicuous examples of paedophile organisational references were "Fresh Petals" and "Boylinks". As of 17 November 1997, the e-zine (electronic magazine) "Fresh Petals", listed 53 references to WWW "little girl" sites with a list of 59 word combinations suggested for use with Internet search engines. On the same day, Boylinks detailed 230 references to "boy" related sites.

Highly explicit pornographic stories were maintained at several sites. One gay and bisexual library contained a vast array of stories involving children. Another set of "erotic stories" provided child pornography under the classification "pedo". These libraries remained stable over the period of observation and they appeared to contain items collected over a number of years. The libraries were hierarchically structured and they used mirrored locations. New additions to the libraries were received regularly (by anonymous email). Subjects ranged from stories of love and infatuation to extreme child abuse and murder. These libraries were expanding, well organised and their pages

accounted for the most blatant sources of child pornography that was available on WWW pages.

Examples of child pornographic images were very rarely encountered on WWW pages. However, this material was abundant in newsgroups. Newsgroups were used by paedophiles to distribute materials and to demonstrate the size of their collections. A number of newsgroups were regularly swamped with hundreds of pornographic images. In addition, newsgroups were used to distribute advice and to solicit partners. While it was distressing to observe some of the individual images, it was overwhelming to experience a mass posting. These events drew attention to the size of paedophile collections. In April 1997, an individual posted over 200 explicit images across three newsgroups. In November 1997, another individual posted over 350 explicit images. Paedophiles took care to post messages to newsgroups anonymously. Consequently, their actions were potentially untraceable.

Characteristic activities

Paedophiles were very concerned to conceal their identity. This was not unexpected given society's attitude to paedophilia. Many of the Internet links provided on WWW pages described anonymity and privacy techniques. Email messages sent to newsgroups took advantage of anonymity techniques. WWW pages displayed disguised e-mail addresses while newsgroup discussions exchanged information about "safe" locations and masking techniques. IRC chat sessions were conducted on private channels or chat sessions used direct "one-to-one" secure communication facilities (for example, Direct Client to Client).

Paedophiles appeared eager to demonstrate their prowess to their peers. WWW pages were used to deliver "coming out" presentations (although most presenters hid behind masked identities). These pages appeared to provide peer group status. They also acted as a vehicle for soliciting communications from other paedophiles. Background profiles and descriptions of individual interests were often detailed on the presentation pages together with samples of images from private collections. The willingness to demonstrate the extensiveness of individual picture collections was apparent in certain newsgroups. Sending pictures to newsgroups obviously enabled wider distribution to a general clientele. Newsgroup postings appeared to be most concerned with advertising the extent of personal collections.

The IPC apparently sought a mixture of anonymity and publicity. Some individuals publicly disclose their lifestyle under the cover of masked identities. However, within their community these identities were obviously recognisable.

Internet Activity and Identification

When considering paedophile use of the Internet it was useful to associate activity with anonymity and privacy implications. Individuals initiating Internet activities could be described as activity owners. Individuals receiving or participating in those activities could be described as readers.

The association between Internet activity and user identification confirmed observations that Internet components providing the strongest anonymity hosted the most extreme paedophile behaviour. Indeed, there appeared to be a relationship between the potential to be identified and the publication of explicit child pornography. The stronger the perceived anonymity the more explicit the child pornography. WWW pages offered weak anonymity for owners. While it may be possible to disguise identity when obtaining ISP facilities, maintaining pages provides ISPs with an opportunity to trace owners. Therefore, paedophiles took care not to display "offensive" pictures on WWW pages. Pornographic materials were most abundant in "sex-stories" libraries and newsgroups. The method of delivering material to both of these components was by anonymous email. Paedophiles obviously made extensive use of Remailer services. These services offered the delivery of potentially untraceable email messages (Engelfriet 1997). With the perception of little risk to their anonymity paedophiles were happy to publish explicit pornographic material on the Internet.

Enabling Access to Collections

Paedophiles seek to access and publish materials which most societies ban. They obviously collect material and seek the ability to search for more. Given the illicit nature of these materials, paedophiles were expected to be concerned about the security of their collections. Even so, paedophiles provided Internet access to their collections. The relationship between information access and reader identification can be used to describe how paedophiles arranged Internet access to their collections.

Information owners are concerned with controlling access to private material. While it may be acceptable for an unidentified reader to access publicly available information, unidentified access to private information would not be acceptable. Paedophiles provided Internet access to their collections using:

- *unidentified open access:* by constructing WWW pages without visitor logging and by distributing information on newsgroups that were available on public news servers;
- *identified open access:* by constructing WWW pages and FTP sites with reader logging capability;
- *restricted access:* by constructing WWW pages or FTP sites with passwords that were distributed within

the IPC and by distributing information on newsgroups that were only available on news services that enforced access controls;

- *authorised access:* by constructing WWW pages or FTP sites with user identified access and by communicating the location of the sites to individuals via email or IRC using encryption techniques;
- *unauthorised access:* was assumed to be discouraged. While unauthorised access was not observed many of the messages and links observed within the IPC provided advice on securing files. Paedophiles can be expected to protect their collections using encryption processes and relocation strategies (for example, storing sensitive materials at remote Internet locations).

Distribution

While paedophiles provided access to their collections they also sought to distribute their materials anonymously. When distributing these materials the relationship between owner identification and targeted audience became important.

Paedophiles used the Internet to distribute their material by:

- *anonymous broadcast:* using anonymous email techniques to submit material to public newsgroups;
- *anonymous private communique:* using anonymous email techniques to send messages to email addresses collected from WWW pages or Newsgroup postings;
- *private communique:* using encrypted email techniques and "one-on-one" IRC conversations;
- *restricted publication:* using anonymous email techniques to send messages to Newsgroups that were only available on News Services that enforced access controls;
- *personal broadcast* were not observed.

Paedophile organisation underpinned by anonymity

Individual organisation was obviously required as paedophiles embraced Internet technologies to achieve personal privacy and anonymity. However, paedophile WWW pages and links to support groups suggests collective organisation (for example, Danish Pedophile Association, European Boylover Base, NAMBLA, German Pedo Association and Pedophile Liberation Front. For a discussion of NAMBLA see De Young (1989)).

Disguised ownership of WWW pages, open access to Newsgroups, anonymous email and private IRC channels enable paedophiles to organise and distribute their material internationally. Anonymity provides paedophiles with an opportunity to create a global community congregating at virtual locations that are accessible from anywhere, at any time. This study indicates that limiting anonymity could reduce their activity. Unfortunately, restricting Internet anonymity affects users with a legitimate need for anonymity. The whole issue of digital anonymity is complex and requires careful consideration. Even though the wider ramifications of Internet anonymity are beyond the scope of this study, anonymity clearly influences paedophile Internet usage. Paedophiles are challenging society by demonstrating that they can conduct their activities in an unrestricted manner.

Addressing the Challenge

Counteracting this challenge will require cooperation. ISPs can be expected to reject a call to monitor all usage. The sheer mass of Internet transactions renders such a concept unrealistic and very expensive. And the determination of what is pornographic and what is not, is not always easy. Yet, enforcement agencies expect ISP cooperation. The Wood Royal Commission into the NSW Police Service, recommended that the Internet industry should make provision for ISPs to;

> *disclose information (the identity of account holders, dates and times of access to online services and the sites accessed) to a law enforcement agency when an authorised officer certifies that the disclosure is reasonably necessary for the* enforcement *of criminal law* (Wood 1997b, para:16.91).

It should be borne in mind that Sections 282 and 313 of the *Telecommunications Act 1997* (Cwlth) require ISPs to cooperate generally with law enforcement.

Observation indicates that ISPs could:

- protect customer confidentiality by declaring they would not release customer information unless instructed to do so in accordance with society's laws;
- insist upon adequate user identification (that is credit cards, security certificates or other third party verification processes);
- insist that users agree certain activities are not tolerated (with specific reference to paedophilia);
- require users to accept responsibility for their activities while online.

Actions like these would impact paedophile activity. Paedophiles relying on disguise would be forced to a higher level of sophistication. However, some ISPs may be sympathetic towards paedophile activists and provide services anyway (for example, FPC.Net) Remailer operators provide anonymous email services and therefore attract particular attention. The Internet community needs to consider the value of untraceable email if self-regulation is to be effective. The European

Commission suggested that self-regulation systems would include:

- a Code of Conduct for Internet service providers (access providers, host service providers and anonymous remailers);
- a hot-line for complaints from the public, with appropriate safeguards against misuse;
- an independent self-regulatory body, including representatives of industry and users, to advise on whether or not a breach of the Code of Conduct has occurred (without prejudice to the due process of law) (EC 1997).

Cooperation will be futile if the Internet community adopt "isolated global rules with different countries signing up to different rules agreed under the auspices of different international organisations" (Bangemann 1997). Close cooperation was proposed in the green paper "Protection of Minors and Human Dignity", along with the use of filtering software, rating systems, and self-regulation of access-providers (EC 1996).

The European Commission also recommended a number of actions to achieve safe usage of the Internet including to:

- alert and inform parents and teachers;
- foster cooperation, exchange of experiences and best practices; and
- promote coordination across Europe and between actors concerned (Action Plan 1997).

It should be noted that in Australia, the Internet Industry Association (IIA) is in the process of developing a code of practice which imposes obligations on subscriber ISPs with respect to a range of matters including illegal content. The code can be found at <www.iia.net.au>. In addition, the IIA are helping develop a hotline service in conjunction with law enforcement agencies, the Australian Broadcasing Authority, and the non-governmment organisation, ECPAT.

Specialised Resources

As paedophiles become more sophisticated in their use of personal computers, society will experience difficulty monitoring their activities. Paedophiles will gravitate towards technologies that maximise anonymity. Indeed, it can be expected that some paedophiles have already chosen to conduct their business within virtual private networks (VPNs). Monitoring VPNs will prove difficult because transactions will be encrypted and Internet trails will be elusive. Consequently (as the Wood Royal Commission pointed out), funding, training and inter-service cooperation will be necessary to enhance law enforcement. This includes the provision of Internet investigative specialists armed with appropriate technologies (Wood 1997b, para: 19.94). The Australian experience has "demonstrated that establishing proactive, intelligence-driven investigative units is the most effective law enforcement response to paedophilia, and this approach is being increasingly implemented by many Australian police services" (Miller 1997). Knowledge of Internet practice within paedophile networks will be essential if enforcement agencies are to effectively counteract the paedophile challenge.

Preventive Action

Society expects a response to the public distribution of paedophile material. Observing paedophile practice enables the design of tactics to counter their activity. Services that paedophiles use will be obvious candidates for close scrutiny by enforcement agencies. Since news services have been used to distribute extreme material, some suggestions for newsgroup supervision are offered for consideration:

Close Public Access to Adult Newsgroups Services: One way to reduce the amount of suspect material in the public arena is to stop public access. (For example in the same way that access to adult WWW sites are restricted.) ISPs that provide adult news-groups should close public access to their service. In countries where it is an offence to possess paedophile material ISPs carrying suspect newsgroups risk prosecution. When operating news services ISPs decide which messages they will accept. Accepted messages are then stored locally. At that point they may have possession of illegal material. Once users of their service read those messages a distribution has taken place. The danger of carrying suspect newsgroups should be brought to the attention of ISPs. Enforcement agencies should consider monitoring local news services offering suspect newsgroups.

Public News Services: ISPs that want to retain public access should carefully choose the messages they carry and reject unwanted newsgroups from their news-feed. This can be implemented by a simple parameter setting. Regular advice from enforcement agencies about newsgroups that are suspect would be very useful to ISPs. (Newsgroup Black-List).

Follow paedophile requests: Some messages seek private responses. These requests necessitate a return address. Return addresses offer the potential for identification by tracing ownership. Occasionally, real addresses were observed. They would provide an indicator to enforcement agencies because they can be quickly traced. However, disguised addresses are often used. They were obtained from free email services, probably using erroneous physical addresses and anonymous proxies. Operators of free email services could counter disguised addresses by rejecting account requests from anonymous proxies, recording IP numbers, forcing appli-

cants to acknowledge a code of conduct and requiring validated identification. Enforcement agencies should develop an effective working relationship with these ISPs. Details of illegal usage would help ISPs to improve safeguards against further abuse. Mass-poster alerts: A number of mass postings of extreme material were observed. In keeping with the need for peer recognition, pseudonyms remain constant over time. A warning to ISPs from enforcement agencies could allow the preparation of processes to exclude or isolate service requests from individual mass posters.

These suggestions draw attention to the need for reliable and timely information about illegal activity. One procedural issue for enforcement agencies is that news messages are short-lived. The volume of messages traversing the news network forces ISPs to "expire" messages. This makes the collection of evidence opportunistic whereas it should be systematic. The ability to search for trends/patterns and to measure the effect of enforcement tactics requires access to an archive of relevant messages. A specialised archive of suspect newsgroups could provide valuable research information and evidence details.

Finally, two areas for further research became apparent during this study. It would be useful to understand paedophile Internet practice and the implications of Internet anonymity. The present essay is based on passive observation. A more comprehensive study would seek confirmation and expansion of the Internet techniques used within the IPC, by seeking opinions from actors associated with paedophile Internet practice (that is paedophile activists, ISPs, enforcement agencies, policy makers). A triangulation of research could collect quantitative data, survey the opinions of actors and review the case histories of relevant convictions. Secondly, digital anonymity presents society with a range of implications for free speech, culture and social values. These philosophical issues require lengthy debate. However, the implementation of electronic funds transfers (e-funds) and the introduction of anonymous coins (e-cash) will rapidly impact the legal structures of national economies (that is, taxation, exchange control, contract enforceability, accountability). A review of the traditional role of privacy together with a projection of the social and economic implications of Internet anonymity could inform the development of Internet structure and regulation.

Despite the challenge of anonymity, paedophile activity within a complex electronic environment provides certain opportunities for law enforcement (for example, the ability to record activity in an archive and mistakes by offenders). Exploratory observation of the Internet disclosed extensive paedophile activity and organisation. It also illuminated the importance of understanding the Internet practice of those targeted by enforcement agencies.

References

Action Plan 1997, Action Plan on promoting safe use of the Internet: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, http://www.2.echo.lu/legal/en/internet/actpl-cp.html#221

Akdeniz, Y. 1997, Regulation of Child Pornography on the Internet: Cases and Materials, October, http://www.leeds.ac.uk/law/pgs/yaman/child.htm

Bangemann, M. 1997, "A New World Order for Global Communications — The Need for an International Charter", *Telecom Interactive '97*, International Telecommunications Union, Geneva, 8 September, http://www.ispo.cec.be/infosoc/promo/speech/geneva.html

Cleary, C. 1998, "Report claims evidence of paedophiles on Web", *The Irish Times .. on the Web*, http://www.irish.timesxom/irish%2dtimes/paper/1998/0323/fro3.html (28/4/98).

De Young, M. 1989, "The world according to NAMBLA: Accounting for deviance", *Journal of Sociology and Social Value*, vol. 16, no. 1, pp. 111-26.

EC 1996, Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services, Directorate-General X, http://www2.echo.lu/legal/en/internet/content/gpen-toc.html

————1997, European Commission report on Working party on illegal and harmful content on the internet, http://www2.echo.lu/legal/en/internet/content/wpen.html

Engelfriet, A. 1997, Anonymity: Remailers: Cyberpunk remailers, http://www.stack.nl/~galactus/remailers/index-cpunk. html

FPC.Net 1997, Free Paed Co-operative, a part of Free Spirits, http://www.demon.nl/freespirit/fpc/

Freeh, LJ. 1997, Statement before the Senate Appropriations Committee, Sub-committee on the Departments of Commerce, Justice and State, the Judiciary, and Related Agencies Committee on the Judiciary United States Senate, April 8, http://www.fbi.gov/congress/porn/pornsph.htm

Grubin, D. 1992, "Sexual offending: Across-cultural comparison", *Annual Review of Sex Research*, vol. 3, pp. 201-17.

Miller, K. 1997, "Detection and reporting of child abuse (specifically paedophilia): A law enforcement perspective", *Paedophilia Policy and Prevention*, Research and Public Policy Series, no. 12, ed. M. James, Australian Institute of Criminology, Canberra, p. 37.

Parliamentary Joint Committee on the National Crime Authority 1995, Organised Criminal Paedophile Activity: A report by the Parliamentary Joint Committee on the National Crime Authority, November, http://senate.aph.gov.au/committee/ncactte/ncapedo/ncapedol.html

Scipione, A 1997, cited by Meade A, "Paedophile net on *Net", The Australian On-line*, http://www.australian.aust.com/archive/28-Feb/n6.htm

Wood, J.R.T. 1997a, Royal Commission into the New South Wales Police Service, Final Report, vol. IV: The Paedophile Inquiry, August, http://www.nsw.gov.au/premiers/police_royal_commission/volume4.html, p26

Wood, J.R.T. 1997b, Royal Commission into the New South Wales Police Service, Final Report, vol. V: The Paedophile Inquiry, August, http://www.nsw.gov.au/premiers/policeroyalcommission/volume5.html

Patrick Forde is a Senior Lecturer with the Curtin Business School, Curtin University of Technology, and Andrew Patterson is a Senior Detective with the Western Australia Police Service

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.