Current situation regarding our knowledge of paedophile activity in P2P networks

MAPAP – Safer Internet Plus (ec.europa.eu/saferinternet)
Collective work – coordinated by Ethel Quayle and Matthieu Latapy
March 2008

Child pornography on the Internet

We have no idea of the number of people who offend on the Internet. We can examine conviction rates, but these reflect only the countries where possession and distribution of child pornography is both illegal and where there are either the resources or inclination to act upon detection. In the US, Wolak et al. [1] reported that law enforcement made an estimated 2577 arrests during twelve months (starting July 1st 2000) for Internet sex crimes against minors. These crimes were categorized into three mutually exclusive types: Internet crimes against identified victims (39 %); Internet solicitations to undercover law enforcement (25 %), and possession, distribution or trading of child pornography with no identified victim (36 %). Two-thirds of offenders who committed any of the types of Internet sex crimes against minors possessed child pornography, with 83 % of these possessing images of children between the ages of 6-12, and 80 % having images explicitly showing sexual penetration of minors.

Finkelhor & Ormrod [2] examined child pornography patterns from the FBI's National Incident-Based Reporting System (NIBRS). The data from 1997-2000 on 2469 crime incidents involving pornography revealed that over these three years pornography offences increased by 68 % and juvenile victim/child exploitation pornography offences increased by 200 %. But at the time of this report, only a small minority of all pornography offences known to the police was coded as involving a computer.

However, these statistics reflect only those who are caught. Other data, such as that provided by one leading UK Internet Service Provider, suggested that in July 2004 they blocked more than 20,000 attempts per day to access child pornography on the Internet. These attempts were easy to block because the material requested was from known sources.

More difficult is material that is produced with a perfectly valid reason, but which is used by others in a way that is problematic. A good example of this is provided by Lehmann et al. [3], in relation to the detection and management of pornography seeking in an online clinical dermatology atlas. During the study period, one third of the search queries related to anatomical sites and over half specified children.

From the unpublished data of the CROGA Internet self help site for people experiencing difficulties in relation to child pornography, there were 8684 users of the site between June 2004-April 2006 [4]. Similarly, in the UK the statistics from Stop-It-Now [5], suggested that between 2002-2005, 45 % of calls to their help line were from people experiencing problems in relation to their own behavior, a significant number of whom were using, or feeling a compulsion to use, the Internet. In 2007 the Internet Watch Foundation in the UK reported that, "... it has managed a 34 % increase in reports processed by its 'Hotline'. The reports led to the confirmation of 10,656 URLs, on 3,077 websites, containing potentially illegal child abuse content. 82.5 % of all the websites were apparently linked to the US or Russia, up from 67.9 % in 2005" [5].

There is little understanding of this offender group in terms of what risks they pose. Much of what we know relates to police operations, case studies and unpublished anecdotal material. Any difficulties are compounded by the different kinds of populations used (e.g. prison versus community), the time frame for the data collection (more recent accounts would suggest a greater availability of illegal images of children, through for example peer to peer networks), the ways in which the data are gathered (telephone interviews, self-report questionnaires, re-conviction rates) and the lack of longitudinal data. As researchers we are also confounded by the fact that new technologies move on, and the arena for offending changes.

Child pornography in Peer-to-Peer systems

Many studies show that a large amount of paedophile and harmful contents are distributed using P2P file exchange systems, and that the volume of such exchanges is increasing [7], [8], [9], [10], [11], [12]. Mehta et al., (2002) [13] examined 507 video files retrieved from the Gnutella network using key words that were likely to be linked to a search for pornographic material. Their data suggested that while the availability of

obscene or illegal vidoe files constitiuted a relativel small percentage of the overall set, the ease with which the material was accessed and the sheer volume of data flowing through the network was seen as a cause for concern. Video files defined as paedophile represented 3.7 % of the sample, but as millions of files were exchanged this represented a sizeable number. These authors also monitored a website (Gnutellameter) which captures data exchanged in Gnutella and provides summaries of key words most commonly entered by users. They suggest that, "the most commonly searched for files on Gnutella are either copyright protected software, movies encoded in divx format, and pornographic material, with a strong emphasis on both child and hebephilic (sexual attraction to pubescent adolescents) pornography". In a similar vein Grabowski (2003) [14] had noted that in February 2003, Palisade Systems collected 22 milion requests and queries conducted on Gnutella over a three week period and randomly selected 40000 of these. They found that 42 % of all requests monitored were for adult or child pornography. The presence of such content, and its very easy access, make the current situation particularly worrying for P2P users, in particular children.

Paedophile behaviors in Peer-to-Peer systems

There is very little knowledge on user behaviour and file exchange on peer-to-peer systems in general. A recent survey [22] classified files exchanged on P2P networks in Europe as video, audio, software, eBooks and pictures on the basis of plain text file names. On the eDonkey network (which is relevant to the current study) video was found to account for 70 % of all traffic that could be classified, with about 25 % of these files having pornographic content (as indicated by file name). Image files were found to account for less than 1 % of P2P traffic (the proportion of this that was pornographic was not determined).

Gaining an insight into the form and extent of paedophile exchanges is an aspect of P2P networking that has so far been under explored. This lack of precise knowledge is a severe limiting factor in our ability to undermine these exchanges and also in our understanding of the nature of this form of deviant user behaviour. A study [9] of paedophile contents available on the internet reveals that French law-enforcement authorities typically observe 10 to 20 persons engaged in significant paedophile P2P exchanges per day in France. A child protection report also conducted in France [8],

showed a number of files with paedophile content available via P2P systems between 200 000 and one million. Waters [23] used software which maintains a unique serial number for each installed system on a particular P2P network and tracked these serial numbers to get a global perspective of individual users in the US. Over a 7 month period (Jan-Aug, 2006) using this approach 193, 626 unique computers trafficking child sex abuse imagery in the US were located by law enforcement officers.

Understanding paedophile activity on the internet is an important social and law enforcement issue. Studies have shown that easy and/or unwanted access to paedophile content may increase or even create the user's interest for such contents [7], [24], [25]. Some theories suggest that the wide presence of paedophile content in P2P systems make these people feel safe and unattainable in these systems, and leads to a trivialisation of such content [7], [25]. In some cases it may even encourage people to try and have sexual intercourse with children [25], [26]. It has also been found that paedophile pictures are used by paedophiles to lure children into thinking that sexual intercourse between adults and children is normal [25]. Seto et al. [27] investigated whether being charged with a child pornography offence was a valid diagnostic indicator of pedophilia, as represented by an index of phallometrically-assessed sexual arousal to children. Their results indicated that child pornography offenders had almost three times the odds of being identified as a pedophile phallometrically than offenders against children. The study also suggested that child pornography offending is a stronger diagnostic indicator of pedophilia than is sexual offending against child victims.

A recent study by Hughes et al. [28] investigated deviant user behaviour on the Gnutella P2P systems. A small yet significant proportion of traffic was found to be related to illegal pornography, 1.6 % of searches and 2.4 % of answers. In addition, results point to the likely distribution patterns of illegal pornography (which in this instance includes rape, incest, bestiality and sexual abuse of children). They found a small yet particularly active sub-community of users that searches for and distributes illegal pornography ; 57 % of peers who share such material share no other material, while only 17 % share less than 50 % illegal material. The paucity of other such studies on deviant user behaviour on P2P systems highlights the need for more, preferably longer term projects to be carried out which would highlight behavioural trends and phenomena of interest.

Children as Internet users

According to the 2005 Eurobarometer Survey on Safer Internet [15], 50 % of the children of the European Union have access to the internet. A further UK study by Livingstone & Bober (2005) [16] of 1,511 children and young people aged 9–19 indicated that school access to the Internet was almost universal (92 %) with 75 % had access at home. Within this study, 71 % of children had their own computer, 38 % a mobile phone, 17 % a digital TV and 8 % a game console, all with Internet access, increasing the likelihood of exposure to violent or sexual material. In the SAFT (2003) study [17], almost one in five children had been invited to a face-to-face meeting with a stranger, and 34 % had viewed a violent website, either accidentally or on purpose. Polish research from Gemius in June 2006 was based on 831 on-line surveys made among Internet users aged 7-14. Within this sample one out of ten Internet users in Poland is between 7 and 14 years old and they stay online longer than average, largely for entertainment purposes. They generate the heaviest traffic, being very active users. Girls stay online approximately 10h per week longer than boys, although the representation of both genders is almost equal. Almost half of the children (45 %) were described as heavy users, surfing the Internet a few times a week. One third of the youngest Internet users lived in rural areas of Poland, but children living in big cities stayed online longer. With regard to web site popularity, online games were what attracted young people the most. 70 % of interviewees prefered this type of online activity, regardless of gender. Online video services (such as youtube.com) and social networking sites came next on the list of the most attractive online activities. 70 % of minors used social networking sites and girls stayed there three times longer than boys. Peer-to-peer services were used by 40,5% young Internet users [Gemius research].

Other authors have highlighted the accidental exposure of young people to unwanted sexual material on the Internet [18], [19] but have also acknowledged the fact that existing research examining the effects of exposure to unwanted sexual material had been, “almost entirely based on college students and other adults. None of it concerns children, certainly not younger than aged 14. Moreover, the existing social research is all about voluntary and anticipated exposure. No research on children or adults exists about the impact of exposure that is unwanted or unexpected”. In September 2006 the Gemius

agency, together with the Nobody's Children Foundation, conducted an online survey on young people's contacts with harmful content on the Internet. There were 2559 respondents aged 12-17 who were asked about the scale of contacts with harmful content, such as:

- Erotic and pornographic material
- Violence scenes
- Xenophobic and racist material

The aspect of parental control was also covered. The results of the research were alarming : 71 % of young respondents had contacts with pornographic content, most of them unintentionally. Unwanted contact with pornographic or erotic material was acknowledged by 74 % of girls and 46 % of boys, while 43 % of boys and 37 % of girls visited erotic sites intentionally, and spent approximately one hour there. 25 % of the children reported that their parents were not at all interested in the way they used the Internet, and only 9 % of the interviewees being accompanied by parents when on-line.

Children as Peer-to-Peer users

A study conducted in 2003 in France [8] established that 31 % of children having access to the internet were using P2P systems. The presence of harmful contents in these systems, in particular paedophile ones, therefore constitutes a worrying danger for a significant proportion of European children [17], [6], [18], [10].

Another source of concern is the fact that many fakes, i.e. files with contents that differ significantly from their names, are present in these systems. Because of this, all users, including children, face a high risk of downloading and visualising unwanted content, which may be legal or illegal [17], [6], [18]. A report from the United States General Accounting Office in 2003 [7] concluded that "child pornography is easily accessed and downloaded from peer-to-peer networks". In one search of the KaZaA P2P file sharing program, using 12 keywords known to be associated with child pornography on the internet, 42 % of titles and file names were found to be associated with child pornography pictures.

Conclusion

In this report we have reviewed recent, relevant literature published on paedophilic activity on P2P networks and the internet in general. This provides us with an up-to-date picture of the current knowledge base in the area and highlights the many gaps in our understanding of various aspects of this problem.

Overall, despite a widespread acknowledgment of the ease of availability of child pornography and the existence of paedophile activity on P2P systems, what is striking and in need of attention is the lake of knowledge of the nature of paedophilic activity and user behaviour within these systems. There is still no available filtering technique or content rating system to protect P2P users, in particular children, from harmful and paedophile content. Similarly, only a few tools exist to help law enforcement authorities and other child protection organisations in fighting P2P paedophile exchanges.

References

1. Wolak, J., Mitchell, K. J., & Finkelhor, D. (2003). *Internet sex crimes against minors: The response of law enforcement*. Alexandria, VA: National Center for Missing & Exploited Children.

2. Finkelhor, D., & Ormrod, R. K. (2004). *Child pornography: Patterns from NIBRS*. Washington, DC: Department of Justice, Office of Juvenile Justice and Delinquency Prevention.

3. Lehmann, C. U., Cohen, B. A., & Kim, G. R. (2006). Detection and management of pornography-seeking in an online clinical dermatology atlas. *Journal of the American Academy of Dermatology, 54*(4), 633-637.

4. Quayle, E. (2008). Online sex offending: Psychopathology and Theory. In D. R. Laws & W. T. O'Donohue (Eds.), *Sexual Deviance* (2nd ed.), (pp. 439-458). NY: Guilford Publications Inc.

5. Internet Watch Foundation (2007). *2006 Annual Report*. Available online from: http://www.iwf.org.uk/media/news.196.htm

6. StopItNow!UK & Ireland. (2006). Helpline report. Retrieved from: *www.stopitnow.org.uk/publications.htm*

7. United States General Accounting Office. (2003). *File sharing programs-peer-to-peer networks provide ready access to child pornography*.

8. Recommandation du forum des droits sur l'internet : *Les enfants du Net (2) Pedo-pornographie et pedophilie sur l'internet.* (2005). Retrieved from: **http://www.foruminternet.org/telechargement/documents/reco-enfance2-20050125.htm**http://www.foruminternet.org/telechargement/documents/reco-enfance2-20050125.htm

9. *Protection de l'enfant et usages de l'internet* (2005). Rapport remis au ministre en charge de la famille, France.

10. Le Bouclier. Study: Peer-to-peer: Sharing Pedophilia. Retrieved from: **http://www.bouclier.org/dossier/318.html***http://www.bouclier.org/dossier/318.html.*

11. Ropelato, J. Peer-to-peer pornography- kids know, do mom and dad? Retrieved from: **http://www.familysafemedia.com/peer-to-peer_pornography_--_ki.html**http://www.familysafemedia.com/peer-to-peer_pornography_--_ki.html.

12. Parent2parent organisation. Retrieved from: **http://wiki.morpheus.com/~p2punited/parents.php**http://wiki.morpheus.com/~p2punited/parents.php

13. Mehta, M.D., Best, D. & Poon, N. (2002) Peer-to-peer sharing on the Internet: An analysis of how Gnutella networks are used to distribute pornographic material. *Canadian Journal of Law and Technology,* 1 (1).

14. Grabowski, S. (2003) *The real cost of "free" programs such as instant messaging and peer-to-peer file sharing applications*. SANS Institute.

15. *Eurobarometer survey on safer internet*. (2005). Survey commissioned by the Directorate-General Information Society and Media.

16. Livingstone, S., & Bober, M. (2005). *UK children go online: Final report of key project findings*. London.

17. SAFT (Safety Awareness Fact and Tools). (2003). Children's study- investigating online behaviour. Retrieved from : **www.ncte.ie/InternetSafety/Publications/d1736***www.ncte.ie/InternetSafety/Publications/d1736.www.ncte.ie/InternetSafety/Publications/d1736www.ncte.ie/InternetSafety/Publications/d1736 www.ncte.ie/InternetSafety/Publications/d1736*

18. Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact and prevention. *Youth & Society, 34*(3), 330-358.

19. Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000). *Online victimisation: A report on the nation's youth. Alexandria*, VA: National Center for Missing & Exploited Children.

20. Recommandation du forum des droits sur l'internet : Les enfants du Net (1) Les mineurs et les contenus prejudiciables sur l'internet. (2004). Retrieved from: **http://www.foruminternet.org/telechargement/documents/reco-enfance1-20040211_2.htm**http://www.foruminternet.org/telechargement/documents/reco-enfance1-20040211_2.htm

21. FBI cyber education letter. Retrieved from: **http://www.fbi.gov/cyberinvest/cyberedletter.htm***http://www.fbi.gov/cyberinvest/cyberedletter.htm.http://www.fbi.gov/cyberinvest/cyberedletter.htmhttp://www.fbi.gov/cyberinvest/cyberedletter.htm*

22. P2P Survey. (2006). Retrieved from: *http://www.ipoque.com/P2PSurvey2006.html*

23. Waters, F. (2007). *Child sex crimes on the internet.* Report for the State of Wyoming Attorney General.

24. Taylor, M., & Quayle, E. (2003). *Child Pornography: an internet crime*. Brighton: Routledge.

25. Quayle, E., & Taylor, M. (2002). Child pornography and the internet: perpetuating the cycle of abuse. *Deviant Behavior, 23*(4), 331-362.

26. Taylor, M., Quayle, E., & Holland, G. (2001). Child pornography, the internet and offending. *ISUMA, The Canadian Journal of Policy Research, 2*, 94-100.

27. Seto, M. C., Cantor, J. M., & Blanchard, R. (2006). Child Pornography Offenses Are a

Valid Diagnostic Indicator of Pedophilia. *Journal of Abnormal Psychology, 115*(3), 610-615.

28. Hughes, D., Walkerdine, J., Coulson, G., & Gibson, S. (2006). Peer-to-peer: Is deviant behaviour the norm on P2P file-sharing networks? *IEEE Distributed Systems Online*, 7, 1-11.