Jayawardena, Kasun P. and Broadhurst, Roderic (2007) Online Child Sex Solicitation: Exploring the feasibility of a research 'sting'. *International Journal of Cyber Criminology* 1(2):pp. 228-248.

Online Child Sex Solicitation: Exploring the feasibility of a research 'sting'

Kasun Jayawardena and Roderic Broadhurst*

*School of Justice, Queensland University of Technology, Email: r.broadhurst@qut.edu.au

The authors gratefully acknowledge the assistance of Nick Chantler, Warren Reed and Peter Grabosky for helpful comments on an earlier draft.

Draft - 21 August, 2007 – 9590 words

Abstract

A small scale test of the integrity of Internet Web 2.0 social network sites was undertaken over several weeks in 2007. The fictional identities of four female underage children where posted on three network sites and later introduced to relay chat forums in order to explore the impact of apparent vulnerability on potential selection of Internet victims. Only one of the three social network sites in the study recognised that the postings violated child protection policies and subsequently closed down the underage postings.

Two basic identities were created: one that engendered a needy and vulnerable characterisation of a child while the other identity was created to represent a happy and attached child character. The number of contacts and suspicious contacts were monitored to test assumptions about child 'vulnerability' and risks of unwanted sexual solicitations. The characters created also included either an avatar and/or contact details. These variants of the experiment showed that the inclusion of an image or access details increased the likelihood of contacts, including suspicious contact regardless of 'vulnerability'. This small experiment noted that although vulnerable children with additional cues maybe at more risk all children who posted details about themselves on social network sites faced the risk of contact by predators. The need for further research and better means of regulating such sites was suggested.

Introduction

The online exploitation of children is no longer a novelty or a risk that can be addressed by expose alone. The form of exploitation is also not confined to sexual abuse although these have attracted the most alarm. Various forms of commercial exploitation will also become so ubiquitous that measures such as the Australian government's $189 million NetAlert (Salek 2007) National Filtering Scheme for libraries and households and other screening or monitoring will be essential even though they may offer less protection than hoped (Minow 2004). Although child pornography is now universally outlawed it may be still be viewed by thousands via the Internet (Grabosky 2007: 6) and will continue to generate demand for young victims. This paper provides an initial exploration of the role Web 2.0 network technology may play in providing access to underage victims who may be vulnerable to on-line sexual predators.

Fears about the potential risks of the Internet, especially for children have been long held, however, the advent and rapid uptake of websites such as *MySpace* have added to these fears (Pascu et. al. 2007). A growing understanding that the Internet is lawless is now widely acknowledged. "Without a seamless web of mutual legal assistance and comity between nations, and without public/private partnerships, policing the information superhighway will be impossible and the 'frontier' of cyberspace will be as lawless as any wild west." (Broadhurst, 2006: 11). MySpace.com, for example, found from among the approximately 180 million profiles on their popular social networking website more than 29,000 registered US sex offenders who also had profiles on the site (*Sydney Morning Herald*, July 25, 2007). This presumably excludes those who may have sought to hide their real identities. In these circumstances how can we minimise the risks for children and what governments, schools, parents and the Internet industry can do about increasing safety on the internet superhighway?

Many studies have been undertaken from the criminological, psychological and sociological perspective on child abuse and paedophilia. Freud opened the way with his initial theory of childhood sexual abuse and the more controversial concept of repressed memories created as a result of that abuse. Much work has been done since to psychologically profile paedophiles, to categorise their behaviour, as well as to characterise both victims and predators (see Goldstein 1999). The focus has recently been about identifying risk factors and media-induced, especially Internet moral panics about stranger-danger. Also recent research addressing the controversy about the role of Web search engines and logs has found that sex and pornography as a major topic for search engine users has declined from about 16.8 percent of Web inquiries in 1997 to less than 4 percent by 2004 (Spinks, Partridge and Jensen 2006). The willingness of males to visit such sites may also be exaggerated. Spinks et. al. 2006 also cites Bogaert (2001) who reports a number of studies exploring what sort of sexually explicitly material men (undergraduates) choose to see. When given the opportunity half did not want to see any sexually explicit material while only 4 percent chose violent pornography and 3 percent child sexual activity.

In many ways, however, the implications of the Internet for child sexual abuse, both in a real-world context and an online context, are yet to be comprehensively and systematically studied. The increasing commercialisation and privatisation of the Internet also pose complex regulatory questions as earlier versions of the 'free' Internet are colonised by identity and information miners of all stripes (Sarikakis, 2004). Studies so far have tended to concentrate on identifying various technologies and Internet areas that paedophiles utilise. Though now dated, the Forde and Patterson (1998) – *Paedophile Internet Activity* – by the

Australian Institute of Criminology, is a good example. It identified and explored dimensions of online child sexual abuse and exploitation from a technical, law-enforcement viewpoint. It examined paedophile activity online (using websites, newsgroups[1], Internet Relay Chatrooms and so forth) to document and analyse ways in which paedophiles use these services to target victims, to publish child pornography and to network with each other. While this research was thorough, Forde and Patterson (1998:1) nevertheless acknowledge that: 'There is a need for reliable information and competent investigation because a sophisticated level of technological competency was demonstrated by many paedophiles.'

Existing research concentrates on the *extent* and *nature* of online paedophilia and child abuse, focusing overwhelmingly on the use of certain Internet technologies. An example is Bilstad's (1996) study, *Obscenity and Indecency on the Usenet: The Legal And Political Future of Alt.Sex.Stories*, which explores the use of newsgroup/bulletin board technologies as a way of publishing obscene material. It also includes written forms of child pornography. Similarly, Stanley's (2002) study, *Child Abuse and the Internet*, covers the psychological profiles of at-risk victim groups and paedophiles as well as exploring the methods and technologies used in the solicitation of children. Both studies are useful. guides about the nature of the problem, but fail to provide direct evidence of how these bahaviours manifest and offer no tests (experiments) on theories involving grooming work with 'at risk' children..
Mitchel, Finkelhor and Wolak's (2001) study, *Risk Factors for and Impact of Online Sexual Solicitation of Youth*, goes a long way towards bridging this gap. The work is based on a telephone survey of 1501 youths aged between 10-17 and explores the 'demographic and behavioural characteristics associated with solicitation risk and distress due to solicitation'. Through logistic regression, the study found that:

Nineteen percent of youth who used the Internet regularly were the targets of unwanted sexual solicitation in the last year. Girls, older teens, troubled youth, frequent Internet users, chat room participants, and those who communicated online with strangers were at greater risk (Mitchel, et. al. 2001:3011).

The higher risk for 'troubled' youth than 'non-troubled' youth has been a focal point for various studies of online child abuse. Troubled youth are defined by Mitchel et. al. (2001:3012) as:

… a composite variable that includes items from a negative life events scale (death in the family, moving to a new home, parents divorced or separated, and/or a parent losing a job); from the physical and sexual assault items on a victimization scale; and a depression scale (≥5 depression symptoms in the past month).

It is important to note that the authors go on to point out that these risk factors should not be overstated, as 75% of those who were sexually solicited online were not classed as 'troubled'. But one of the inherent flaws in this type of research is that the respondents may not respond truthfully; within this subject-matter especially, and since parental consent has to be given for an interview to proceed, children may not admit to having been solicited online due to the sensitivity of the subject. They may also fear that their Internet privileges will be withheld if their parents are alarmed.

[1] Newsgroups are discussion groups that utilise Usenet, a worldwide, non-centralised group of services that stores messages and files and forwards their content to other servers on demand. Alt.Sex.Stories is one of many discussion groups within Usenet. Newsgroups are accessed through Newsgroup Readers software, which is designed to use access Usenet (see M. Feather, 1999).

Nevertheless, a real risk of victim selection via the routine scanning of social network sites and chat rooms does exist and dissemination about victims also can occur via private bulletin boards involving password control. These technologies of anonymity enable one to create a false identity and it is possible for participants in such bulletin boards never to have met face to face, and not to know each other (Grant et. al. 1997, Grabosky 2007). For example, a recent case involved three men who had never met in person and knew each other only online. All three were convicted in a London Court of a conspiracy to rape a girl under 16, based on a discussion in an internet chat room (Choo & Smith 2007:4).

Such closed networks are also ideal vectors for both dissemination and sale of child-related sexual exploitation. For example, Operation Cathedral was one of the first major international investigation of child pornography that targeted the Wonderland Club, a network operating in at least 14 nations in Europe to North America to Australia and involving over 100 offenders. The Club periodically rotated servers in order to avoid detection, and access to the system was password-protected. The commercialization of child pornography has also led to the involvement of credit card payment processing companies to manage the revenue generated. In 2004, a major investigation called Operation Falcon led to indictments against two companies as well as a number of individuals (Ashcroft 2004 cited in Grabosky 2007).

The Research Problem

The answer to the difficulties of obtaining useful data about potential risks on the Internet can be partly overcome by applying a similar model to the one used by Demetriou and Silke (2003) in their study, *A Criminological Internet Sting: Experimental Evidence of Illegal and Deviant Visits to a Website Trap*. This experiment utilized a purpose-built website, with real legal and fake illegal/pornographic content, to record and track which areas visitors accessed in order to 'determine whether people who visited for the purpose of gaining access to legal material would also attempt to access illegal and/or pornographic material.' They found about 7% (58) of the 803 persons who had visited the site over an 88 day period attempted to access illegal pornography (although no actual materials were provided). The 'sting' is similar to the activities of law-enforcement officers in detecting and apprehending paedophiles online.

The necessity of such methods has been upheld by the Australian High Court. The court found in 2002 that the effective investigation of certain crimes such as drug importation needed to show '… subterfuge, deceit and the intentional creation of opportunity to commit an offence.' (*Ridgeway v R*, 2002 cited in Dixon 2002). This decision was reflected in Queensland law when the *Criminal Code* was amended to include using electronic means to solicit a child under 16 or expose a child under 16 to pornographic material.

Approaching the problem from another direction is the investigative journalism of *The New York Times*' Kurt Eichenwald (2005) in, *Through His Webcam, a Boy Joins a Sordid Online World*. Here, the reporter makes contact with a former under-aged amateur 'porn-star', an 18-year-old man who started doing live strip-shows through his webcam at the age of 13. He then progressed to more and more obscene material until he ended up recording sessions with prostitutes. The reporter engages in an explorative study with the subject, helping him move away from his lifestyle while documenting the process by which he was first solicited for sexual content by online paedophiles and drawn into the world of webcam child pornography. Eichenwald's investigation is one of the most compelling into online solicitation, child sexual grooming and exploitation. The methods used by paedophiles and victims and the characteristics of both are explored in a direct way.

This sort of explorative and scientific research into the use of the Internet by paedophiles is where future research may show promise, perhaps in close cooperation with law-enforcement agencies carrying out sting operations online. Monitoring past Internet activity of paedophiles – as with the Forde-Patterson study – is not enough. Researching crimes as they are committed, from initial contact, through to solicitation and sexual grooming, then to the manipulation of the victim leading to a potential real-world meeting is vital. Only this will help us to identify and understand the methods, thought-processes and characteristics of victims that make them particularly attractive to paedophiles.

Future research needs to be practical and aimed at law enforcement and crime-prevention, especially now that the world is beginning to look beyond issues of jurisdiction and national boundaries in fighting online child abuse. With the growing Web 2.0 phenomenon and the corresponding growth of social networking platforms (O'Reilly 2005; Appendix A), it is vital that sting-oriented experimental research be utilised to discover the risk factors and dangerous behavioural patterns that lead to online solicitation. The study presented in this paper explores the online environment by conducting such research and assessing the feasibility of such an approach.

A simple sting experiment has been used, which sets up four profiles of 12-year-old girls on various social networking platforms. We test three variables: vulnerability, and two other related variables: the effect of avatars, or personal photos, and the presence of a direct method of contact, in this case an email address. These profiles were advertised on various IRC (Internet Relay Chat[2]), chat-rooms which young girls would likely frequent.

The aim of this research was threefold: (a) to explore the feasibility and dimensions of research utilising a criminological sting design; (b) to gain knowledge of the dynamics and security of social networking platforms present at the current stage of the Web 2.0 phenomenon and (c) to gain an understanding of which personal characteristics tested are more likely to be attractive to paedophiles.

For the purposes of this study, it should be noted that the scope is intentionally limited to explorative pilot research and raises the ethical issue of deception in the design and the unavoidable absence of consent by the 'participants' who contacted our fictional children. On balance we argue that we have not harmed or exposed to unnecessary risk any person and indeed mimic what is now common practice among police tasked with monitoring the internet for such activities.. Also the names of the social networking platforms involved have been fictionalised and the email addresses and other details of respondents removed to ensure anonymity.

Methodology

Four fictional identities or profiles were set up on three social networking platforms, Adulescentia.com (*Adulescentia*), Osirus.com (*Osirus*) and Horizon.com (*Horizon*). The objective was to discover how best to conduct a direct, experimental sting. The secondary objectives, though necessarily constrained due to the nature of this pilot study, were to discover which sets of variables are most attractive to paedophiles and whether the security of social networking platforms make it easier or harder for underage users to set up profiles and for paedophiles to find and solicit them. These fictional profiles are described in table 1 and were named as follows: *Alicia* (profile 1), *Michaela* (profile 2), *Kate* (profile 3) and *Kelsey*

[2] Internet Relay Chat (IRC) is a protocol using TCP communications between computers and servers, facilitating chat-rooms (called channels), which are used for group communication (see Feather, 1999).

(profile 4). The control group in this experiment are *Michaela* and *Kelsey*, created without an avatar or photo and without an openly displayed email address. These profiles represent underage users, both vulnerable and non-vulnerable, who do not have the two risk-factors being tested for.

Variables applied to the profiles

The profiles chosen display the three main variables for the research as noted: vulnerability (referred to in the Mitchel, et. al, 2001 study as the characteristic of being 'troubled'), the presence or lack of an avatar or photo and the ease of direct contact, measured by the presence or lack of an openly displayed email address. Table 1a summarises the variables and how they are used in each profile. Table 1b and c describe the profiles as displayed on the Internet sites. The constants in all four profiles are the age (12 years), location and sex (all females for the purposes of this pilot study). Although paedophiles target boys as well as girls the majority of child sexual abuse is perpetrated by adult males against underage females (see Finkelhor, 1994). Further research should use both male and female profiles as variation based on the gender of target is likely. All cases were stated to be located in Brisbane, Australia. Each of the profiles was given different personal content to reduce the risk that they may have been detected as fakes. Instead, they were kept broadly true to the variables and constants, while the situation of each profile was different. A small focus group of female undergraduate and high-school student assisted in developing "authentic" profiles.

Vulnerability included factors such as the relationship with immediate family, a quiet disposition, lack of friends, self-esteem issues, a reliance on an Internet-oriented lifestyle, and an identification with the 'Emo', 'Goth' and other 'alternative' sub-cultures that are stereotypically regarded as having depressive or anti-social tendencies (in this case, through the act of listening to music associated with these sub-cultures).

Profiles on social networking platforms such as *Adulescentia* and *Osirus* allow for a user to select an image, which is one associated with the profile's public presentation. This image could be a photograph of the user, which is common in social networking platforms, or an avatar, which is more common in forums[3] and other such websites. An avatar can be a picture, graphic or other image, which represents the person using it. The effect of a profile including a graphical avatar to draw attention, as opposed to one without, would be of interest to law-enforcement stings especially, as well as Internet users of the at-risk category. Two avatars were created from an online 'doll-maker' program, which allows the user to customise a human figure with clothes and other items. The figures created represented the personalities of the two profiles involved. These avatars were used initially and then replaced with photographs digitally manipulated to disguise their true identity.

The set-up of social networking platforms such as *Adulescentia, Osirus* and *Horizon* allows for communication by members via a private-messaging system, which is akin to an email service exclusively used between the members of the website. Members are generally discouraged from revealing their actual email addresses on their profile. Some do however, thus providing easier access to inexperienced Internet-users, especially children who may consider it exciting to be emailed. Openly displayed email addresses may create a more attractive target for solicitation.

[3] Forums are discussion groups that use IP-based communication and present a graphical interface for messages and discussions to be read. Information is usually stored in a single location, within a database. Forums can be accessed through a browser's normal HTTP protocol and is presented as a website, albeit one with dynamic content.

Table 1a. Summary of variables in each fictional identity

Profile 1: Alicia	**Profile 2: Michaela**	**Profile 3: Kate**	**Profile 4: Kelsey**
Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable
Avatar/Photo	No Avatar/Photo	Avatar/Photo	No Avatar/Photo
Contact (email)	No Contact (email)	Contact (email)	No Contact (email)

Table 1b. Fictional profiles of vulnerable child

Profile 1: Alicia	Picture: Avatar/Photo	Email: star.struck_95@hotmail.com	Female age 12
Headline: Quiet and plotting. **About Me:** Well not much to know really ... I'm actually 12 years old (hush, I just wanted a public profile), I'm kinda quiet, I like reading, writing and listening to music. I'm also addicted to the Sims. I live with my mum, who thinks I should be just like her (perfect) and my older sis (kill me now, please), but I try not to pay too much attention to them. I spend most of my time on the net, and probably the rest of my time at school, which sucks most of the time … star.struck_95@hotmail.com **I'd Like to Meet:** People who'd actually listen to what I say instead of what's in their heads. **Interests:** Reading and writing bad fanfics, listening to music, avoiding mum and sis **Music:** Guy Sebastian, Good Charlotte, Powderfinger ... all kinds of stuff. **Films:** Loved Spiderman but shh, I wasn't suppose to see it. **Television:** Don't get to watch much, mum and sis watch boring crap. I prefer the net. **Books:** Harry Potter (yum yum), Diary of Anne Frank (saddest book ever) **Heroes:** Spiderman … wish I could get an upside down kiss.			
Profile 2: Michaela	Picture: None	Email: None	Female age 12
Headline: Lonely girl on a lonely planet **About Me:** I'm really 12 years old (shh), I'm a bit of a loner, I like books and music and watching cool movies, I'm fairly quiet and I don't make friends easily (who needs 'em, right?). I'm an only child who lives with my parents who I don't get on with much, I live on the world wide interweb and I like chatting and annoying people. **I'd Like to Meet:** New people to chat to. **Interests:** Listening to awesome music, brooding, reading and writing. And chatting. **Music:** I have a lot of music but mostly like Wolfmother, Avril Lavigne and Coldplay. **Films:** Too many to count. **Television:** I like House (yummy!) and Supernatural (two yummies?). **Books:** So many books and not enough time. Currently reading The Queen of the Damned by Anne Rice. **Heroes:** House! :p			

Table 1b Fictional profiles of non-vulnerable child

Profile 3: Kate	Picture: to be supplied	Email: Powered_by_cheese@hotmail.com	Female age 12
Headline: Look at me, I'm awesome, cool and sooo modest! **About Me:** Hey all :) I'm really 12 (whisper whisper), female, and decidedly awesome (of course!). I'm part of a wonderful and large family (one older brother, one younger sister, two parents (not three, and four is right out), one really cool grandmother and two Doberman Pinschers) and I like going places and doing things. Apparently to an annoying extent. I like abseiling, netball, skiing (in Australia, which is mostly desert … typical, huh?) and swimming. I also like chatting to new and interesting and weird people! … powered_by_cheese@hotmail.com **I'd Like to Meet:** Outgoing, awesome strange beings of the Internets. **Interests:** Repeating myself :p abseiling, swimming, skiing, netball, going on runs with two huge doggies, family get-togethers (seriously awesome fun when I have such a huuuuuuge family!) and hanging out with friends. **Music:** I like all kinds of music, from classical stuff to R&B **Films:** Latest one I watched and liked was 'Lady in the Water'. So touching! **Television:** Not too into TV, and I think Big Brother is silly. I don't mind admitting that I watch Home and Away with my family during dinner, kind of a tradition here, but its too soapy sometimes. **Books:** I do like reading, but never seem to have enough time to finish books! **Heroes:** My mum and dad and grandmother (yeah, I know, I'm a sap) and I guess my friends!			
Profile 4**:** Kelsey	Picture None	Email: None	Female aged 12
Headline: Average girl seeks tin can. Will open for food. **About Me:** Let's see … I'm only 12 years old (my profile is such a liar), an only child, I'm into drama (as in acting, not melodrama!) and music (I play the saxamaphooone) and I'm pretty much your basic high-flying girl … yeah sure :p I live with my mother who's annoying but really awesome and our dog Wuff (called that because when you ask "what's your name?" he makes a "Wuff!" sound!). I also like doing art and plan to go on being me for the rest of my life! Challenging, hey? **I'd Like to Meet:** Other cool and creative people. **Interests:** Music, learning how to play the piano as well as the sax, drama, reading, filling out silly profiles on here. **Music:** Evanescence, Bach, John Coltrane **Films:** Hot Fuzz. Too awesome. **Television:** I'm a big fan of Doctor Who (David Tennant is hot!!), and it's so unfair that the Brits get it first! I also like Lost and Big Brother. **Books:** Currently reading The Good Soldiers. **Heroes:** My dog Wuff!			

Social networking platforms – three examples

Three different social networking services were chosen to place the fictional profiles. They varied in terms of their scale and community orientation. As noted in this research we give them the *nom de plumes*: *Adulescentia*, *Osirus* and *Horizon*. *Adulescentia* had two layers of membership: one for the 14-18 year-olds and one for the 18+ age group. The 14-18 age group membership did not have publicly viewable profiles. Instead, the user had to allow a request from another member to be part of his or her 'friends list' for access to the full profile, or be a part of that age group membership. There was a member search function on *Adulescentia* similar to that contained in personal websites. This enabled a user to search by sex, age, relationship or marital status, and also to seek out what a member was searching for on *Adulescentia* (dating, relationships, networking or friendships), plus a host of other descriptive factors such as height and physical build. The 14-18 year-olds had access to search for members from the age of 16-68, while the 18+ age group could only search for those over the age of 18-68.

In order to test the integrity of the security that protects underage users on *Adulescentia*, *Michaela* and *Kelsey* were placed in the 14-18 age group. Both profiles stated that the user was actually 12-years-old from the outset. *Alicia* and *Kate* were placed in the 18+ age group and also stated openly that the user was actually 12-years-old.

The *Osirus* platform was originally designed for use by university students for networking purposes. It has been expanded, however, to include other interest groups and regional groups while retaining a focus on educational establishments. Profiles only become available to the groups that the user chooses to partake in: the general Australian regional group was selected which exposed the four profiles to around 52,000 members. Thus the *Osirus* platform, due to the non-public nature of their profiles, was an ideal control for the experiment. The same profile information, including the specified 'real' ages of the users, was supplied.

Horizon is a Canadian-based social networking platform with a worldwide membership and is unique in that it has no layered memberships and has completely public profiles. The lowest age permitted is 14, which is also Canada's age of consent (with certain exceptions). *Horizon* is much more community-oriented and is designed with an ethos similar to Internet forums and moderated chat-rooms than only online websites and profiles. This is reflected in its strong administrator and moderator presence. It has over 1,000,000 members, with around 300,000 of them active. A large number of its users are below the age of 18 and as such, the service is targeted more at a younger membership.

Responses of social network sites

Within the experiment and the structure of these social networking platforms, three broad responses types are available. The first is the 'friends list' feature, where members can send a request to be added to another member's list of friends. In *Adulescentia's* 14-18 age group, an acceptance of such a request gives access to the member's complete profile. It is similar to the contact list available in email software and instant messenger software[4], and as such provides a means of tracking and bookmarking the profiles of people of interest to a member.

The second response type is the private message, which is similar to an email that can only be accessed through the social networking platform and is limited to members. Private messages can be sent without members having accepted any 'friends' request, with the exception of the 14-18 age group in *Adulescentia*, where only those within a friends list can exchange messages. The third response type is a direct email using addresses supplied with *Alicia* and *Kate's* profiles.

Suspicious responses within these three types are defined as those from accounts that are not spam (advertising for musical groups or musicians, products or services) and are from members above the age of 18. The primary indicator of a suspicious response was sexual content in the first instance, or after a reply. Once sexual content is established, all contact with the responder ceased. The limited scope of this study, of course, excludes the possibility of an experienced paedophile initiating a long-term sexual grooming process or establishing one by posing as another child. Research about such responses would necessitate more in-depth and correspondingly long-term studies.

Results

Our findings are reported over the three stages of the experiment – each stage leading to more adventurous exposure of the profiles. In the first stage profiles were initially set up on *Adulescentia* and *Osirus* and left untouched for 14 days in order to ascertain the 'unencouraged lure' of young girls. Within this period, no photographs were used for *Alicia* and *Kate*. Instead, two avatars were created using an online 'doll' maker. A doll is a cartoon

[4] Instant Messenger programs are software than can be used to communicate with people who are also signed up to use the same software and are added onto a private friends list (Gross, Juvonen and Gable 2002)..

representation of a person and the software allows the user to change the doll's clothing, hair and expression. To match their characteristics, Alicia was given paler skin, a blank expression and darker clothes as well as a set of black wings, while Kate received tanned skin, a happier expression and trendier clothes in bright colours. There were no results for this initial experiment from the *Osirus* platform at all, though there were limited results from *Adulescentia*, as can be seen in Table 2,

Table 2 Responses to profiles at 14 days

	Alicia	**Michaela**	**Kate**	**Kelsey**
Total Friends Requests	13	0	24	0
Legitimate Requests	1	0	4	0
Spam Requests	12	0	20	0
Total Private Messages	2	0	3	0
Legitimate Private Messages	1	0	2	0
Spam Messages	1	0	1	0
Direct Emails	0	NA	0	NA

There were no responses for *Michaela* and *Kelsey*, which were the profiles without avatars. In fact, an examination of the count of individual visits to these profiles, listed in the profile page, showed no visits by any other member of *Adulescentia* at this stage, even by other members within the 14-18 age group. In searching for other members within *Adulescentia*, users could choose whether or not to search for members without avatars and most did not. In fact, the default option was to search only for members with avatars.

The next stage of the experiment involved answering all legitimate responses from *Adulescentia* (Table 2), to discern which were innocent or suspicious. *Alicia's* single legitimate 'friends request' proved to be innocent, with the member deleting *Alicia* off her friends list after realising her 'true' age. Her single legitimate private message, however, was suspicious. After establishing contact, the conversation rapidly turned sexual, with the member asking about masturbation and boyfriends. Three of *Kate's* four legitimate friends requests were innocent, with one proving to be a member randomly adding profiles and the other two not fully reading her profile and her true age. One, however, looked suspicious after three replies, asking for personal details about intimate clothing and requesting personal photographs, despite having again been reminded of *Kate's* age. Similarly, both of *Kate's* legitimate private messages were suspicious, with the members becoming sexual soon after the reply. This process of answering legitimate responses was carried on throughout the remainder of the experiment.

The modest response to the first stage of the experiment was indicative of the presence of paedophiles willing to track and solicit young girls. The experiment, however, required the presence of these girls on the Internet to be known, or put another way, to be 'advertised'. In a normal situation, these girls would have been heavily active in forums, chat-rooms, other networking platforms, instant-messenger programs and so on. These would all feature links back to the profiles. The experiment had to advertise the profiles in order to achieve this degree of realism. The third stage thus involved three expansions of the experiment: (a) the addition of profiles to another social networking platform, *Horizon*; (b) the use of photographs as opposed to graphical avatars and (c) the participation in Internet Relay Chat chat-rooms for advertising purposes. It must be noted that expanded research should utilise more than chat-rooms for advertising. A complete online presence must be maintained for each girl, including the activities listed above. For this explorative study, however, it is

sufficient that such advertising be tested to gain an understanding of the effect on the number of suspicious responses.

Horizon provides human security in the form of moderators who accept or reject each profile as they are created. For this reason, *Alicia's* and *Kate's* profiles were created one day before *Michaela* and *Kelsey's*, and their 'true' ages were omitted until after they had been accepted. When all were accepted into the system, *Alicia's* and *Kate's* profiles were updated with childhood photographs[5]. The childhood photographs were in turn slightly digitally manipulated to ensure the safety of the women who had provided them and to make them appear to be photographs taken from a digital camera. After the photographs were uploaded, all four profiles were changed to reflect their 'true' ages. Although receiving plenty of attention (mostly spam messages and requests), within three days all four profiles were suspended by *Horizon* staff. Although it is impossible to ascertain, this was probably done via the option for members to report any illegal profiles to the moderators.

Expanding on this, the photographs replaced the avatars on *Alicia's* and *Kate's* profiles within the *Adulescentia* and *Osirus* platforms. Both platforms were used in the advertising, with one week's advertising for each. The Undernet network of Internet Relay Chat (IRC), arguably the largest, was chosen for the advertising because of the un-moderated nature of the medium and the presence of tens of thousands of users at any given time. An IRC client called mIRC software[6] was used to access the Undernet network[7] as it was the mainstream software for IRC. The two chat-rooms chosen from Undernet's list were #Teens and #Teenchat. Other directly sexual chat-rooms for all age groups were available but were rejected for the purposes of this study because the solicitations should occur within an 'innocent' medium. Due to practical considerations involved in advertising two sets of four profiles within a short exposure period of two weeks, it was decided to sacrifice a realistic schedule (particularly due to the international nature of IRC) and to partition each day into four slots, advertising each of the four profiles six hours apart and rotating them each day into different time slots as shown in table 3 below.

Table 3 Timetable for *Adulescentia* and *Osirus* Profiles Advertised in IRC

	12:00 AM	**6:00 AM**	**12:00 PM**	**6:00 PM**
Monday	Alicia	Michaela	Kate	Kelsey
Tuesday	Kelsey	Alicia	Michaela	Kate
Wednesday	Kate	Kelsey	Alicia	Michaela
Thursday	Michaela	Kate	Kelsey	Alicia
Friday	Alicia	Michaela	Kate	Kelsey
Saturday	Kelsey	Alicia	Michaela	Kate
Sunday	Kate	Kelsey	Alicia	Michaela

Profiles were advertised both in the main chat-room and in private chat to any person who initiated a conversation. An example of an advertisement in the main chat-room would be, "Hi I'm Alicia, 12/f/Australia, bored n' lonely, anyone wanna talk or whatever add me on Adulescentia!", followed by the appropriate URL. If there was conversation going on in the

[5] Provided with the informed consent of the two adult women associates who agreed to be involved in the experiment..

[6] See T. Vonck, *Introduction to mIRC*, accessed on April 3, 2007 at http://www.mirc.com/mirc.html

[7] S. Okeefe, C. Ovidiu, J. Angliss and B.B. Adnane, *Introduction to Undernet*, accessed on May 27, 2007, at http://www.undernet.org/

chat-room, the characters would participate with the appropriate knowledge of Internet abbreviations and speech patterns. The roles of *Kate* and *Kelsey*, being the non-vulnerable profiles, were appropriately more spirited and socially aware in discussions, whilst *Alicia* and *Michaela* were shy and withdrawn. It is interesting to note that *Kate* and *Kelsey* received more attention from real or supposed younger people, whilst *Alicia* and *Michaela* attracted attention from those who didn't identify directly as young and were more dominant in conversation.

There were also many requests for photographs, with *Alicia* and *Kate* responding with links to their profiles, while *Michaela* and *Kelsey* denied having access to digital cameras. While there was plenty of suspicious attention directed at the girls within the chat-room, it was beyond the scope of this study to explore these interactions, though it is an area that needs further research. This is especially so as IRC is particularly involved with content crimes such as the trading of child pornography (Forde and Paterson 1998; Hellard 2001).

The results of this final stage in the experiment were mixed. The *Osirus* profiles attracted some attention but mostly from other young members, actual or posing, some of whom became sexual as well. *Alicia* and *Kate* received all of the responses, with *Alicia* receiving 3 'friends' requests, one of which turned sexual after 3 replies, and Kate receiving 5 friends requests, with 3 becoming sexual after a few replies. It must be noted that the chat-rooms, while primarily intended for what #Teens specified as 'clean chat', were also used by these younger people to initiate sexual discussion with the opposite sex. This has been argued by some sources, for example social worker Patrick O'Leary (cited in Munro, 2006: 23) to be a part of normal sexual exploration. Of course, as Taylor (2002) points out, these younger people could be victims of child abuse who copy the abuse they've suffered and inflict it on other children, being the result of learned behaviour (see White and Haines 2004: 60-62). The results of the *Adulescentia* profiles were more pronounced and are reported in Table 4.

Table 4 Stage 3 Results for *Adulescentia*

	Alicia	**Michaela**	**Kate**	**Kelsey**
Total Friends Requests	16	6	13	3
Suspicious Requests	7	1	5	0
Spam Requests	0	0	0	0
Total Private Messages	9	4	11	3
Suspicious Private Messages	4	2	5	1
Spam Messages	0	0	0	0
Direct Emails	3	NA	2	NA

Discussion and analysis

The main objective of this explorative study was to discern how best to conduct direct criminological research through experimentation, utilising a sting-oriented approach. Stage 1 showed that even a passive approach netted results. The results gained, however, are relevant only for a specific category of paedophile that actively sorts through profiles. But such results are still surprising in a number of ways. The objective of the experiment was to find which profile (and which set of variable characteristics, the major one being vulnerability) attracted the most suspicious contacts. Or put another way, which profile was the most attractive to online paedophiles? The research of Mitchel et. al. (2001), reiterated the common belief,

reflected in official government literature that one of the most at-risk groups are 'troubled' children (NetAlert, 2005, Stanley 2002). By Stage 2, the profile with the most suspicious contacts was Kate's, which was non-vulnerable with an avatar and a contact email, which is similar to the finding of Mitchel et. al. (2001) that 75% of those contacted were not troubled. These results, however, were limited due to the lack of advertising in the other sites of interest – chat-rooms.

By Stage 3, these results had evened out further. *Alicia* and *Kate* received the most attention and, ignoring direct emails, received 44% and 42% of suspicious responses respectively out of the total they attracted. While a lengthier study may yield more results which may show a more significant percentage increase for one or the other, the presence of public profiles and photographs seems to indicate that vulnerability may not be the key issue as has been previously thought. It must be noted though, that a vulnerable child would be psychologically easier to control and manipulate than a non-vulnerable child. More interestingly, the difference between *Michaela* and *Kelsey* was more pronounced, with the more outgoing *Kelsey* receiving 17% suspicious responses of her total, as opposed to *Michaela's* 30%.

It may be misleading to focus on the view that vulnerable children are more likely to be targeted than non-vulnerable children – comforting perhaps to think that non-vulnerable children are at low risk. Thus paedophiles who have the patience, intelligence and understanding of the psychology (or pathology) of children may succeed by undertaking the complex child sexual grooming process so succinctly summed up in NetAlert's *Paedophiles and Sexual Grooming* article (NetAlert 2005: 2). Nevertheless, even outgoing and family-oriented children such as *Kate* and *Kelsey* were at possible risk. It is important, therefore, to avoid perceiving paedophiles, especially those encountered online, as the type of sex offender who selects and only strikes a vulnerable target – a woman walking alone, drugged or drunk for example – then disappears. It is equally important to bear in mind that children are essentially vulnerable, in the sense that they are naïve and inexperienced, eager to please an adult and to make new friends.

The results for *Michaela* and *Kelsey* seem to indicate that without the presence of public profiles and photographs, the results tend to support Mitchel, et. al. (2001) concerns about 'troubled' or vulnerable children on the Internet. The presence of an email address does not seem to affect the risks to the extent anticipated, with *Alicia* receiving a 5% increase and *Kate*, a 4% increase. This seems to indicate that ease of access and a photograph spur on paedophiles, either from a rational weighing up of the ease of action and knowledge of the victim or because the presence of a photograph sparks off an attraction that overrides security and safety concerns. This would be closer to a psychologically positivistic explanation of paedophilia outlined by White and Haines (2004). The use of photographs in Stage 3 was revealing from the outset. One of the initial private messages received by *Alicia* via *Adulescentia*, for example, seems to support the positivism perspective: 'Nice pic good angle on your face. You are very cute and I would like to chat with you. Australia is one of my favourite places, have not visited yet. Hope to chat with you soon.'[8]

While the avatars made a difference, the photographs for *Alicia* and *Kate* seemed to tip the scales of interest, as seen in the results from the *Osirus* platform in particular, with *Michaela* and *Kelsey* not receiving any responses at all. From a security standpoint, the best solution seems to be to design social networking sites around forum communities rather than as an abstract service governed by rigid staff-member hierarchies. *Horizon* has by far provided the best security, with profiles being suspended as soon as the 'true' ages of the fictional girls

[8] Private message, June 12, 2007.

were revealed. This seems to have resulted from the integration of users as staff: the platform is further moderated by the users themselves. Thus, the more intense the sense of community the more likely they will intervene as responsible members of that community. The relatively small size of *Horizon* as compared to *Adulescentia* and *Osirus* too, is probably a major factor. *Horizon* though, is sufficiently large for a purely 'elitist' staff to be unable to handle all the services alone.

Had there been no media attention on child abuse within social networking platforms such as *Adulescentia* and *Horizon* (Mah 2007; Rawthorne 2007) during the time of our research and had *Adulescentia*, in particular, not upgraded the security and structure of its service as a result, it is not inconceivable that there would have been even more suspicious responses than observed. The *Adulescentia* upgrades resulted in a safer environment for the 14-18 age group. It is difficult, however, for any social networking platform to take into account the de-individuation theory which Demetriou and Silke (2003) explore in their study. In the world of the Internet, responsibility is low. It is tempting for underage users to have an 18+ profile because it is publicly viewable and has certain advantages that being in the 14-18 age group does not. It is also tempting for paedophiles to create accounts under the guise of young children to gain the trust of their chosen victims (O'Connel, Price and Barrow 2007) or to view the Internet as a safe and anonymous environment in which to freely interact with children. Further, it is tempting for both predator and prey to feel completely safe within at homes while allowing the world to visit via their computers.

Conclusion

An effective way to conduct direct research on online child sexual solicitation and the activities of Internet paedophiles is by establishing several complete Internet identities. Focusing on one medium alone – for example chat-rooms, without social networking platforms or forums – leaves an incomplete picture of underage users' Internet activities. Social networking platforms can provide a major arena for paedophile activities and when expanded with advertising, constitute an almost unexplored domain for study. Although our study provided limited exposure and advertising it did demonstrate that such techniques can yield useful data.

With the cooperation of social networking platforms, this study has shown that action oriented research could be undertaken by utilising as many different profiles and characteristics in order to discover how Internet paedophiles operate and what factors – such as avatars, photographs, publicly accessible profiles, email addresses and personality characteristics – affect their behaviour. In this case, the initial experimental design proved too passive and short-lived to be a method for attracting enough responses from Internet paedophiles.

In our small pilot study the strongest variables involved were the presence of photographs and email addresses. With these in use, suspicious responses for both vulnerable and non-vulnerable profiles were roughly equal, showing perhaps that these factors encouraged paedophiles to ignore caution and security in favour of gratification. Profiles without these variables had a more predictable outcome, with vulnerable profiles receiving more attention than non-vulnerable profiles. From these initial results, it is recommended that all underage users of social networking platforms be very cautious about placing photographs of themselves in their profiles and to avoid publication of email addresses. In general the education of both parents and children about the importance of privacy and the power of the databases underpinning much of the internet is essential (Barnes 2006)

In terms of security, *Horizon* was by far the best of the three tested and suggests that a community-based social networking platform seems to be the safest. This platform probably enabled self-policing to occur. Paradoxically, *Horizon* allows 14-year-old members to create completely public profiles. Both *Adulescentia* and *Osirus* appeared to have insufficient security in place to detect and suspend the accounts of underage members. *Osirus's* completely non-public profiles, however, did provide a measure of security as compared to *Adulescentia's* layered membership feature.

In the end, the best security must come from within the user's home and habits. Underage users such as the one in Kurt Eichenwald's investigation are at greater risk by having computers in their bedrooms and un-supervised, unlimited Internet access (O'Reilly 2005). The Australian Government's concept of the distribution of free filtering software falls short of the ever-increasing knowledge of Internet technology which children possess and the increasing role of on-line friendships or 'friending' among teens that will undermine these forms of control (Boyd 2006). The alternative of an Internet Service Provider level filter has been dismissed as ineffective in blocking all pornography (a problem with the filtering software as well) and may also limit access to legitimate sites (for example health; see Minow 2004). The impact of the associated slower internet speeds (LeMay 2006) will also be resisted by e-commerce and it is unlikely the speed of Internet connections may be sacrificed for the safety of vulnerable users. Ultimately, the best form of Internet security is parental monitoring in the form of human supervision and the education of children about the dangers posed by the Internet and the importance of privacy self-protection (Barnes 2006). We may do better to empower children to police the Internet and to recognise their rapid absorption of the changes released by Web 2.0 and the relentless privatisation and commercialisation that is now increasingly apparent.

Appendix A: Web 2.0 and Social Networking

The Internet is a vast and largely under moderated network of computers and servers stretching across most of the Earth, linked mainly via land-based telecommunications networks, though satellites are also used to transmit data from one location to another. This creates a relatively new 'data-scape' which can be used to contain and transmit almost any material conceivable – including physical goods via online market-places like EBay and Amazon – from one user to another almost instantaneously. Overcoming time and distance the Internet has created a new form of socialising and communication. The Internet thus forms a constantly evolving frontier, which law enforcement must constantly monitor in order to keep abreast. The phenomenon of child sexual grooming has evolved along with other cybercrime and has entered a phase loosely called Web 2.0. The term Web 2.0 denotes a progression in the use and capabilities of the Internet. In 2005 Tim O'Reilly and MediaLive International proposed the name for a conference on the future of the Internet (O'Reilly 2005). While the conference and the definition of the Web 2.0 phenomenon was business oriented, the term has largely come to denote – with much ongoing debate and discussion – three main advances in which the Internet is used:

1. Data Management and Integration

Websites are no longer static information-holders, but dynamic and interactive platforms that are constantly updated by the user as well as the webmaster. An example of this would be the difference between the personal homepages offered by free hosting sites such as Geocities and Yahoo and the online journals (weblogs or blogs) offered by Livejournal. Both concepts have been integrated to provide interactive, feature-rich and deeply networked profile-pages from MySpace and MSN Spaces. These companies have created products that are *services* as opposed to *artefacts*, with an on-going developmental program that often involves the user in the actual conception.

2. Users as Participants in Communities

The end-user in the Web 2.0 is also a participant in a community of users who also provide the content for the product being used. The user's role has changed from receiving a product to participating in the product itself. Thus the content of Youtube, which is a service that allows the upload of streaming videos for public consumption, is mostly provided by the consumer- user. One of the most interesting developments, and one of the best examples of this, is Wikipaedia, an online encyclopaedia that is written by users themselves, both professionals and laymen.

3. Social Networking

This incorporation of users as content and software developers has created communities reminiscent of the older message boards and Usenet discussion services, but on a vast and more complex scale. Youtube, Adulescentia, MSN Communities and Spaces, Wikipaedia, blogs: all of these services have created super-communities where people can connect to each other in a deeper way than ever before. Different services have been integrated into each to provide connected networks. An example of this would be the MySpace profile site, which offers the user a personal blog, an extensive friends list, a forum, space to upload pictures, music and videos and an instant messenger service. The search feature on MySpaceis powered by Google, which itself has integrated an email service, a mapping feature that can be integrated into websites and blogs to show certain locations down to street-number level, along with many other services (O'Reilly 2005: 2).

The result of such integration via social networking services reveals more information than a user would normally expect. MySpace, for example, actively encourages a user to advertise their online profile on other social networking services like Yahoo! and AOL Instant Messenger. Businesses, mainstream actors and musical artists have also started using MySpace as a way to communicate with their client and fan base. MySpace profiles have evolved from purely social networking between casual Internet users to a valid and acceptable online presence, comparable to official websites, business cards and company newsletters (Shipman 2007). It is not a stretch, then, to read a user's MySpace profile, collect information from the blog available, examine the user's friends list for those the user knows in real life and with the aid of Google Maps, triangulate the user's general real-life location down to the neighbourhood level. With the aid of that profile information and blog, it is quite possible for an intelligent person or agency to build up an extensive psychological profile of the user: likes, dislikes, music, lifestyle and many other factors that are listed openly.

References

Australian Government, NetAlert Limited. 2005. *Paedophiles and Online Grooming*. http://www.netalert.net.au/02333-Paedophiles-and-Online-Grooming.pdf (accessed April 23, 2007).

Bilstad, B. T. 1996. Obscenity and Indecency on the Usenet: The Legal and Political Future of Alt.Sex.Stories. *Journal of Computer-Mediated Communication*, 2 (2): 1 (accessed May 22, 2007, from Blackwell Synergy Database).

Barnes, S.B. 2006.'A privacy paradox: Social networking in the United States by *First Monday,* volume 11 (9)
URL: http://firstmonday.org/issues/issue11_9/barnes/index.html (accessed August 16, 2007)

Boyd D. 2006 'Friends, friendsters, and top 8: Writing community into being on social network sites', *First Monday,* volume 11, (12),
URL: http://firstmonday.org/issues/issue11_12/boyd/index.html (accessed August 21, 2007)

Broadhurst, R.G., 2006, 'Content Cybercrimes: Criminality and Censorship in Asia' *Indian Journal of Criminology*, Vol 34 (1&2):11-30.

Criminal Code Act 1899 (Qld).

Choo, Kim-Kwang Raymond and Russell G Smith, 2007 'Criminal exploitation of online systems by organised crime groups', paper at *Organised Crime in Asia*, National University of Singapore, June 28-29.

Da Silva, F. V. 2007. Folklore into Theory: Freud and Lévi-Strauss on Incest and Marriage. *Journal of Folklore Research*, 44 (1): 1-19. (accessed June 12, 2007, from ProQuest Database).

Demetriou, C. and A. Silke. 2003. A Criminological Internet Sting: Experimental Evidence of Illegal and Deviant Visits to a Website Trap. *British Journal of Criminology*, 43 (1): 213-222.

Dixon, N. 2002. Catching 'Cyber Predators': the Sexual Offences (Protection of Children) Amendment Bill 2002 (Qld). *Queensland Parliamentary Library*, 1-36. (accessed May 24, 2007, from Informit Database).

Eichenwald, K. 2005. Through His Webcam, a Boy Joins a Sordid Online World. *The New York Times*, December 19, 2005.
http://www.nytimes.com/2005/12/19/national/19kids.ready.html?ei=5090&en=aea51b3919b2361a&ex=1292648400&adxnnl=1&adxnnlx=1182664112-MNxnNGCw/i8IG4dD/aG5uw&pagewanted=all (accessed April 16, 2007).

Feather, M. 1999. Internet and Child Victimisation. In *Children and Crime: Victims and Offenders Conference*, 1-22. (accessed February 27, 2007, from Informit Database).

Finkelhor, D. 1994. Current Information on the Scope and Nature of Child Sexual Abuse. *The Future of Children*, 4 (2): 31-53. http://www.futureofchildren.org/usr_doc/vol4no2ART2.pdf (accessed March 15, 2007).

Forde, P. and A. Patterson. 1998. Paedophile Internet Activity. *Trends and Issues in Crime and Criminal Justice*, 97 (1): 1-6. (accessed May 24, 2007, from Informit Database).

Goodstein, S.L. 1999. The Sexual Exploitation of Children: a practical guide to assessment, investigation and intervention, 2nd Edition, CRC Press, New York.

Grabosky, P. 2007 'The Internet, Technology, and Organised Crime', paper at *Organised Crime in Asia*, National University of Singapore, June 28-29.

Gross, E. F., J. Juvonen and S. L. Gable. 2002. Internet Use and Well-Being in Adolescence. *Journal of Social Issues*, 58 (1): 75-90. (accessed June 4, 2007, from Blackwell Synergy Database).

Hellard, P. 2001. Schoolgirl Deluged with Porn. *Herald Sun*, March 23, 2001. http://web.ebscohost.com.ezp02.library.qut.edu.au/ehost/detail?vid=3&hid=21&sid=51740507-b685-4af3-867f-619bb9b53aa9%40sessionmgr8 (accessed June 4, 2007).

Horizon. 2007. *Horizon: Social Networking Website*. http://www.Horizon.com/ (accessed May 25, 2007).

LeMay, R. 2006. ISP-Level Porn Filters a Bad Idea. *ZDNet Australia News*, June 14, 2006. http://www.zdnet.com.au/news/communications/soa/ISP-level-porn-filters-a-bad-idea/0,130061791,139259795,00.htm (accessed August 17, 2007).

Mah, B. 2007. Man Guilty of Luring Teens Over Internet. *Edmonton Journal*, May 31, 2007. http://www.canada.com/edmontonjournal/news/story.html?id=cdc5a315-6b17-41a7-b361-c9817ffae455 (accessed June 12, 2007).

Mitchel, K. J., D. Finkelhor and J. Wolak. 2001. Risk Factors for and Impact of Online Sexual Solicitation of Youth. *Journal of the American Medical Assiociation*, 285 (23): 3011-3014. (accessed May 14, 2007, from ProQuest Database).

Minow, M, 2004 Lawfully Surfing the Net: Disabling Public Library Internet Filters to Avoid More Lawsuits in the United States, *First Monday,* 9 (4),
URL: http://firstmonday.org/issues/issue9_4/minow/index.html (accessed August 16, 2007)

MySpace. 2007. *MySpace: Social Networking Website*. http://www.MySpace.com/ (accessed February 26, 2007).

O'Connel, R., J. Price and C. Barrow 2004. *Cyber Stalking, Abusive Cyber Sex and Online Grooming: A Programme of Education for Teenagers*.
http://www.uclan.ac.uk/host/cru/docs/NewCyberStalking.pdf (accessed March 18, 2007).

O'Grady, R. 2001. Eradicating Paedophilia: Toward the Humanisation of Society. *Journal of International Affairs*, 55 (1): 123-141. (accessed April 16, 2007, from ProQuest Database).

O'Leary, P. quoted in I. Munro 2006. The Harm When Women Prey on Boys. *The Age*, March 18, 2006. http://www.theage.com.au/news/national/the-harm-when-women-prey-on-boys/2006/03/17/1142582526948.html?page=fullpage (accessed April 14, 2007).

O'Reilly, T. 2005. *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. http://www.oreillynet.com/lpt/a/6228 (accessed February 26, 2007).

Okeefe, S., C. Ovidiu, J. Angliss and B. B. Adnane. 2007. *Introduction to Undernet*. http://www.undernet.org/ (accessed May 27, 2007).

Osirus 2007. *Osirus: Social Networking Website*. http://www.Osirus.com/ (accessed February 26, 2007).

Pascu, C., Osimo, D., Ulbrich, Turlea, M and J.C. Burgelman, 2007. 'The potential disruptive impact of Internet 2 based technologies', *First Monday,* 12, (3),
URL: http://firstmonday.org/issues/issue12_3/pascu/index.html (accessed August 16, 2007)

Pilon, M. 2001. *Canada's Legal Age of Consent to Sexual Activity*. http://www.parl.gc.ca/information/library/PRBpubs/prb993-e.htm#CURRENT%20LAW(txt) (accessed May 25, 2007).

Rawstorne, T. 2007. Who is Your Child Talking to on MySpace? *Daily Mail*, May 27, 2007, http://www.dailymail.co.uk/pages/live/femail/article.html?in_article_id=457752&in_page_id=1879 (accessed June 12, 2007).

Ridgeway v R (1995) 184 *Criminal Law Rreview* 19.

Rind, B. 2002. Moral Panic: Changing Concepts of the Child Molester in Modern America. *Archives of Sexual Behaviour*, 31 (6): 543-546. (accessed April 17, 2007, from ProQuest Database).

Salek N., 'NetAlert helps public libraries', ITNEWS, 10 August 2007, accessed August 14, 2007, http://www.itnews.com.au/News/NewsStory.aspx?story=58624

Sarikakis, K. 2004. 'Ideology and policy: notes on the shaping of the Internet'
First Monday, 9 (8),
URL: http://firstmonday.org/issues/issue9_8/sarikakis/index.html (accessed August 16, 2007)

Shipman, A. 2007. *Polish Your Online Profile: CFOs Race into Executive Adulescentia*. http://www.accountingweb.com/cgi-bin/item.cgi?id=103656&d=883&h=884&f=882&dateformat=%25e-%25h-%25y (accessed June 13, 2004).

Smith, M. C. 1997. The Recovered Memory/False Memory Debate. *Canadian Journal of Experimental Psychology*, 51 (3): 258-261. (accessed April 17, 2007, from ProQuest Database).

Spink, A., Partridge, H., and B. J. Jansen, 2006. Sexual and pornographic Web searching: Trends analysis', *First Monday,* volume 11(9),
URL: http://firstmonday.org/issues/issue11_9/spink/index.html (accessed August 16, 2007).

Stanley, J. 2002. Child Abuse and the Internet. *Journal of the Home Economics Institute of Australia*, 9 (1): 5-27. (accessed May 14, 2007, from Informit Database).

Sydney Morning Herald, July 25, 2007: http://www.smh.com.au/news/technology/alarming-increase-in-myspace-sex-offenders/2007/07/25/1185043145104.html, accessed August 14, 2007

Taylor, M. 2002. Teenage Paedophiles Are Victims Too. *The Society Guardian*, July 18, 2002. http://society.guardian.co.uk/children/comment/0,,756822,00.html (accessed April 16, 2007).

Vonck, T. 2007. *Introduction to mIRC.* http://www.mirc.com/mirc.html (accessed April 3, 2007).