

# A TYPOLOGY OF CHILD CYBERSEXPLORATION AND ONLINE GROOMING PRACTICES.

*By*

*Rachel O'Connell*  
*Cyberspace Research Unit*  
*University of Central Lancashire*  
[ro-connell@uclan.ac.uk](mailto:ro-connell@uclan.ac.uk)  
[www.fkbko.net](http://www.fkbko.net)

**Address**

**Cyberspace Research Unit**  
University of Central Lancashire  
Preston PR1 2HE  
+44 (0) 1772 893755/8  
[ro-connell@uclan.ac.uk](mailto:ro-connell@uclan.ac.uk)

**Tel.  
Email**



## Introduction

This paper summarises a section of a keynote address at the Netsafe conference in Auckland, New Zealand, July 2003. It also summarises sections of a paper entitled 'From Mobile to Fixed Internet: The Morphing of Criminal Activity Online', which is available on request from the author<sup>1</sup>. The following paragraphs outline the value of researching and describing a typology of online child sex related activities. Furthermore, in an effort to contextualise the findings of this research a brief outline is provided of how the capabilities associated with both existing and emerging technologies alter the parameters of paedophile activity specifically in relation to victimology and criminal activity.

A summary of the main findings of the research are outlined in the Executive Summary, followed by recommendations for further action in this area.

The value of developing a typology of child cybersexploitation, a term coined by the author to describe varying degrees of online sexual exploitation of children, lies in the fact that it will serve to uncover the nature, scope and extent of the processes which characterise cybersexploitation and online grooming. In particular, this research offers an insight into the behaviour patterns of adults and adolescents with a sexual interest in children and the varying cycles of abuse that can occur, which may for example, be manifested in repeated instances of abuse with a single victim over an extended period of time or may involve a large number of victims each involving a single instance of cybersexploitation. These research findings give rise to a plethora of questions, not least of which relates to whether individual behaviour patterns involve a mixture of those outlined above, or if there is some sense of a progression.

Research such as this has implications at a number of levels as follows:

- To provide a baseline understanding of online activities grounded in research findings, which will help to inform both existing and proposed changes to both legislation and policy strategies. At present, policy makers are operating on the basis of an understanding of grooming practices, which has been borrowed from the real world context and extrapolated to an online setting. It seems reasonable to suggest that it may be better to base any proposed changes on the basis of research findings specifically gleaned within the context of online settings, particularly as the findings indicate that the parameters of paedophile activity offline and online differ in a number of crucial respects, in particular with respect to victimology.
- At a pragmatic level the findings of this study have implications in terms of assisting the teams of people whose role involves handling reports of abuse including cybersexploitation and online grooming made by users to Service Providers. One of the key difficulties at present for abuse report teams is that there are no uniform

---

<sup>1</sup> [ro-connell@uclan.ac.uk](mailto:ro-connell@uclan.ac.uk)

protocols or best practice with regard to how these complaints ought to be handled and indeed in the cases of serious complaints, how decisions ought to be arrived at which deem that it is appropriate to escalate the complaint to the police. In addition, at present there is no networked reporting system whereby complaints made to each service provider are linked. The proposed anti-grooming legislation is a clear indication of a commitment to try to intervene before a sexual offence is committed against a child in the real world. Clearly, this avenue of action suggests that there is room for more concerted efforts by Service Providers, who in many instances are the first port of call when reporting abuse, to ensure that adequate systems are in place to facilitate the process of handling complaints and filtering those of a serious nature to the police. A number of hurdles exist which might affect the smooth operation of a networked reporting system and these relate in part to the sheer multitude of complaints that Service Providers receive on a daily basis, but also perhaps to the need for training for staff and the development of a set of criteria designed to help staff filter complaints in relation to minor digressions, complaints of a serious nature and everything in between. Certainly this is a challenging task but one that will be aided by research findings such as those outlined in this paper.

- The findings presented here provide an insight into how communication technologies can be deemed to not only have the potentiality to alter the parameters of victimology on three levels, i.e. accessibility, opportunity and vulnerability, but also to alter the dynamics of criminal activity in a myriad of ways including the ability to operate in number of virtual crime scenes.
  - Typically, whilst parents are vigilant of the people children come in contact with in the real world they are not as readily vigilant of the adults children come into contact with in virtual worlds and this clearly has an impact on the **accessibility of children**. Furthermore, there is ample evidence that the Internet affords greater opportunity for adults or adolescents with a sexual interest in children to gain access to children, oftentimes whilst the child is at home with their parents. Communication between victim and predator can take place whilst both are in their respective real world homes but sharing a private virtual space. This fact ought to have a significant impact on our understanding of the scope and nature of child sexual abuse not only online but also in general.
  - Arguably, **accessibility** and **opportunity** will be affected as more and more children move from the fixed to the mobile Internet environment. Using mobile phones, which children regard as their private property, will facilitate adults with a sexual interest in children to schedule contact with children in virtual environments. Therefore the limited amount of control that may have been afforded by advising parents to keep the computer in the living room is essentially removed because if children are accessing the internet via mobile

phones, they are potentially accessible at all times, which affords paedophiles greater opportunity to target, cybersexploit and groom children.

— The potential for children to be **vulnerable** to greater levels of abuse also seems to be associated with on-line activity. For example, the easy accessibility of child pornography affords an adult or adolescent with a sexual interest in children the opportunity to expose a victim to child pornography as a means to lower inhibitions. Furthermore, an adult with a sexual interest in children may use that exposure as a means to coerce the child into keeping the activities secret by threatening to tell the child's parents that he/she has viewed pornography. In addition, MMS and video messaging capabilities will make it more difficult for a child to decline a request for a picture. It is important to bear in mind that these are methods of approaching and assessing a vulnerable child's malleability with the view to potential abuse.

- Ongoing research into common behaviour patterns displayed by paedophiles engaged in cybersexploitation also serves to afford us a greater understanding of the areas and incidences where the traditional boundaries between victim and offender may be distorted. In particular, an adult or adolescent with a sexual interest in children may encourage a child to create pornographic material using a web cam, digital camera or video messaging capabilities which are built into the latest mobile phones, thereby contacting children via communication technologies such as Chat and IM and inciting children to create illegal content, and furthermore to disseminate the illegal content via their mobile phones or computers. This may begin as requests for images of, for example, the child's face, or the child on holiday, i.e. images that would fall under the category of erotica before moving onto sexually explicit material, which would typically include images of the child naked and in a sexually explicit position or engaged in particular sexual acts which the paedophile requests the child to record. If the child records a pornographic image of him /herself and then sends it to the adult with a sexual interest in children, strictly speaking a child may be said to have become both the producer and distributor of child pornography. Although it may be possible to argue that the child was incited to initiate the processes of production and distribution of illegal material, it seems reasonable to suggest that this could result in a blurring of boundaries. In a scenario whereby a child was found to have created and disseminated child pornography, and also has child pornography from other sources on their computer, such a discovery must surely dictate that the first point in the investigation might be an exploration into indications of cybersexploitation and online grooming.
- The developing typology outlined in this paper demonstrates the ways in which communication technologies are used as a tool for exploitation and abuse. The fact

that these tools are constantly evolving and the attendant alterations in criminal activity suggest a need for programs of research designed to both keep apace with technological changes and also to assess over the time the efficacy of both current and proposed measures designed to combat paedophile activity online.

### **Methodology and analysis**

A participant observation methodology was employed in this study, which involved over 50 hours of research in chat rooms conducted intermittently over 5 years. Methodological considerations were numerous and rigorous ethical procedures were formulated and implemented according to APA<sup>2</sup> guidelines both before and during research. The procedure involved the researcher entering chat rooms or channels intended for child or teen users and posing as either an 8, 10 or 12 year old child, typically female. The researcher utilised the usernames: 'angel', or 'honez~~' and frequented both web based, and IRC based chat rooms and channels respectively. Details of the fictitious child's life were that she had moved to a new location, her parents were constantly fighting, and that she had not yet made friends with peers in her new school. Essentially, the hallmarks of a socially isolated child were the messages that were to be divulged to any other user with whom the researcher, posing as a child, engaged. Sociolinguistic analytical techniques were employed in order to explore how adults and adolescents with a sexual interest in children cyberexploit and groom children online.

The following section provides a summary of the main findings.

---

<sup>2</sup> American Psychological Association

## Executive summary:

### A Typology of Cybersexploitation and on-line grooming practices

---

This Executive Summary outlines the main stages of cybersexploitation, i.e., adults or adolescents engaging children in varying degrees of sexually explicit conversations which may or may not progress to 'Fantasy enactment' (the enactment of sexual fantasises and in some instances to cyber-rape scenarios). A subset of cybersexploitation is grooming, which may or may not involve explicit conversations of a sexual nature, or indeed online enactment of fantasies but still falls under the umbrella of cybersexploitation because the intention is to sexually abuse a child in the real world, but one of the points of contact occurs in cyberspace. Grooming, which has been defined in the proposed 'anti-grooming legislation' announced in the November 2002 Protecting the Public White Paper refers to the following:

*'A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.*

For the purposes of providing a broader outlook the anticipated impact of 3G mobile phones was considered when drafting these recommendations and a range of both pre-emptive strategies and proposals for policy makers in relation to 3G are included here. For a fuller account of the capabilities and risks associated with 3G phones please read relevant section in the paper entitled, 'From Fixed to Mobile Internet: The Morphing of Criminal Activity Online', (O'Connell, 2003) which this briefing document summarises.

#### Victim selection methods

In teen chat rooms the activities that precede the processes of initiating direct contact with a child may simply involve the adult providing a description of himself to all of the users of the public chat room so that he is masquerading as a particular kind of child, of a particular age in the hope of attracting an equivalent age and same or opposite sex child, for example:

*Adult<sup>3</sup>: '14/m/uk'*

---

<sup>3</sup> All references to 'Adult' in excerpts from conversation refer to adults or adolescents with a sexual interest in children. In reality these users employ usernames such as, for example 'lookingforyoung', or 'bigdaddy'

Once these vital details are stated the adult simply waits for a child to respond and once a child has responded they will either choose to pursue the conversation with the child on the basis of the child's answers to a few initial vetting questions or not.

A different behaviour pattern can also be adopted whereby some adults will simply lurk in a chat room for some time assessing the conversation and each of the children participating in the conversation and only then will they choose to introduce themselves, often to one individual child whom they have been observing. The adult may choose to send a private message to the child that they have been observing, for example:

*Adult: 'hey angel, sounds like things are hard for you right now ☺ you wanna chat'\**

It is important to note that certainly not all adults with a sexual interest in children pose as teenagers. A proportion of adults appear to be truthful with respect to their adult status and may indeed give accurate information about their age.

*Child: what age r u?*

*Adult: whats too old?*

*Child: I don't know*

*Adult: 20s 30's*

*Child ☺*

*Adult: I'm 35, is that too old?*

#### **Paedophile advice to paedophiles regarding cyberexploitation and grooming:**

Research conducted by the author into the content of conversations between adults with a sexual interest in children in child-sex related chat rooms indicated that whilst the majority of the activity in paedophile chat rooms centred on the exchange of child pornography images another of the frequent topics concerned on-line grooming and in particular, ways in which to avoid detection. The full scope of that section of the research is outlined in a separate paper but findings which are particularly relevant to this paper are mentioned here; In paedophile chat rooms users exchange information with one another about how best to target a child that most closely matches an individual's predilections. The advice regarding selection and targeting involves paedophiles viewing children's public profiles on-line. Public profiles consist of on-line forms that chat service providers request children to complete, with typical information fields such as real name, age, location, and children are also invited to upload their photograph, and to give details about their hobbies and interests. In addition, if a child has created their own web site they are requested to provide the URL. In effect, these forms provide paedophiles with enough information to satisfy their curiosity about the physical

appearance of the child and proximity or otherwise of the paedophile to the child's physical location.

### **Patterns of cyberexploitation and grooming conversations**

Throughout each of the stages there are clear and easily identifiable differences in the patterns of behaviour of the individuals, and these appear to relate closely to their motivations, which will be discussed later in the paper. But, it is important to note that whilst the stages outlined here provide a summary of the possible stages of cyberexploitation and grooming conversations, not all users will progress through the stages in the conversations sequentially, i.e. some adults will remain in one stage for longer periods than other adults and some will skip one or more stages entirely. The order and number of stages will vary and these variations provide clues of the user with ill-intent's motivations. Furthermore, whereas some stages, for example the risk assessment stage, have specific and identifiable goals, the goals of other stages are psychological and relate closely to both the aims of the adult and his perceptions of, for example, how malleable a child is in terms of meeting his requirements. Very early in the initial friendship-forming stage the adult will suggest moving from the public sphere of the chat room into a private chat room in which rather than the one-to-many facility of a public arena, an exclusive one-to-one conversation can be conducted.

The following paragraphs provide a summary of the findings of an ongoing program of research, which aims to explore the possibility of developing socio linguistic profiling techniques designed to analyse the speech employed by people who engage in on-line grooming.

### **Friendship forming stage**

The friendship-forming stage involves the paedophile getting to know the child. The length of time spent at this stage varies from one paedophile to another and the number of times this stage of the relationship is re-enacted depends upon the level of contact the paedophile maintains with a child. During this stage a paedophile may ask whether or not the child has a picture of themselves and if the answer is yes they will request the picture to be sent to them. It seems reasonable to suggest that requests for pictures relate at least in part to the paedophile's desire to ensure that the child he is conversing with is in fact firstly a child and secondly one that matches his particular predilections. Furthermore, for those who choose to target children who live in their immediate vicinity the provision of a picture would serve as a useful way to identify the child in the real world. Typically, at this point in the conversation requests for pictures are confined to pictures of the child without any reference to pictures of a sexual nature.

*Adult: 'what do u look like?'*

*Adult: 'any pic?'*

### **Relationship forming stage**

The relationship-forming stage is an extension of the friendship-forming stage, and during this stage the adult may engage with the child in discussing, for example, school and/or home life. Not all adults engage in this stage but generally those who are going to maintain contact with a child will endeavour to create an illusion of being the child's best friend. More typically an initial relationship-forming stage will be embarked upon and then interspersed in the conversations will be questions that relate to the following risk assessment stage.

### **Risk assessment stage**

The risk assessment stage refers to the part of the conversation when a paedophile will ask the child about, for example, the location of the computer the child is using and the number of other people who use the computer. By gathering this kind of information it seems reasonable to suppose that the paedophile is trying to assess the likelihood of his activities being detected by for example the child's parent(s), guardian or older siblings

### **Exclusivity stage**

The exclusivity stage typically follows the risk assessment stage where the tempo of the conversation changes so that the idea of 'best friends' or 'I understand what you're going through and so you can speak to me about anything' ideas are introduced into the conversation by the adult. The interactions take on the characteristics of a strong sense of mutuality, i.e. a mutual respect club comprised of two people that must ultimately remain a secret from all others. The idea of trust is often introduced at this point with the adult questioning how much the child trusts him and psychologically people, especially children, respond to the tactic by professing that they trust the adult implicitly. This often provides a useful means to introduce the next stage of the conversation, which focuses on issues of a more intimate and sexual nature.

### **Sexual stage**

The sexual stage can be introduced with questions such as 'have you ever been kissed?' or 'do you ever touch yourself?'. The introduction of this stage can appear innocuous enough because typically the adult has positioned the conversation so that a deep sense of shared trust seems to have been established and often the nature of these conversations is extremely intense. Therefore, from the child's perspective the conversations are not likely to be typical and perhaps the intensity of the conversation makes it more difficult for the child to navigate because they have entered a previously unfamiliar landscape of conversations of

this nature. Alternatively for children who have previously been sexually abused, and it seems reasonable to assume that there is a high likelihood that at least a percentage of the children using chat rooms will have previously encountered child sexual abuse, adults will modify their approach in a manner that affords them the greatest amount of leverage with a child. The 'you can talk to me about anything' is a relatively staple part of the conversations of those adults who intend to maintain a longer term relationship and for whom the child's apparent trust and love is a vital part of their fantasy life.

### **Patterns of progression through the Sexual stage**

It is during this stage that the most distinctive differences in conversational patterns occur. For those adults who intend to maintain a relationship with a child and for whom it seems to be important to maintain the child's perception of a sense of trust and 'love' having been created between child and adult, the sexual stage will be entered gently and the relational framing orchestrated by the adult is for the child to perceive the adult as a mentor or possible future lover. Certainly a child's boundaries may be pressed but often gentle pressure is applied and the sense of mutuality is maintained intact, or if the child signifies that they are uncomfortable in some way, which implicitly suggests a risk of some sort of breach in the relationship precipitated by the adult pushing too hard for information, typically there is a profound expression of regret by the adult which prompts expressions of forgiveness by the child which tends to re-establish an even deeper sense of mutuality. During the relationship forming stage the adult may outline the rationale of the relationship to the child whilst also intimating his intentions. The rationale for intended activities may include, for example, 'forming a loving lasting relationship / friendship'. This rationale may or may not include an outline of future activities, for example 'maybe we could meet some day and I could show you how much I love you' or 'maybe you could take photographs of you touching yourself'. The nature of sexual conversation will vary from mild suggestions to explicit descriptions of, for example, oral sex. The focus may be on the child, i.e. the adult asking the child to touch itself and to explain what it feels like. The usual rationale for this approach is that the adult is somehow perceived as a mentor who will guide the child to a greater understanding of his or her own sexuality. This can sometimes be taken a little further with the promise that by engaging in these activities the child will grow to become a wonderful lover. The interaction may be about how to self-masturbate and if the adult is a different sex to the child he will explain the techniques a child could use if they were together so that the child could bring the adult to orgasm. Research findings indicate that this pattern of conversation is characteristic of an online relationship that may progress to a request for a face-to-face meeting and arguably most closely resembles the course of conduct the 'anti-grooming' legislation is designed to combat.

### **Child erotica and child pornographic image creation, exchange and distribution**

The sexual stage of the conversation may be characterised by requests for creation, exchange and distribution of child erotic and child pornographic material. Typically this involves the adult or adolescent with a sexual interest in children forwarding child pornographic images to a child in order to rationalise his requests for the child to engage in sexual activities and also to lower a child's inhibitions. In subsequent conversations, or indeed during the same conversation, the adult or adolescent with a sexual interest in children may request that a child record images of him or herself which either approximate what the paedophile has sent, or else that which matches a particular set of suggestions that he has outlined. Web cams may be utilised by children, adults or adolescents with a sexual interest in children to create, exchange and distribute images and also to video stream in real time. The MMS and video messaging capabilities of the latest mobile phones will augment the ease with which these activities can be engaged in, which arguably will precipitate an increased incidence of activities of this kind. If the child records a pornographic image of him /herself and then sends it to the adult with a sexual interest in children, strictly speaking a child may be said to have become both the producer and distributor of child pornography. Although it may be possible to argue that the child was incited to initiate the processes of production and distribution of illegal material, it seems reasonable to suggest that this could result in a blurring of boundaries.

### **Cyberexploitation: Fantasy enactment**

Fantasy enactment can be said to occur when an adult engages a child in enactment of a sexual fantasy. Typically the initial stage of fantasy enactment involve the adult describing a particular scenario, for example,

*Adult: 'I am lying naked in a warm bath and you are sitting at the edge of the bath wearing only a silk robe that falls open'*

It seems reasonable to suggest that in the majority of interactions of this nature, and this could also be said for adult to adult cybersex related interactions, the ultimate goal of fantasy enactment is the achievement of sexual gratification.

The following descriptors provide an insight into the nature and variations of online fantasy enactment.

#### **Fantasy enactment based on perception of mutuality**

In terms of fantasy enactment based activities, a range of differing approaches may be employed whereby the adult will fluctuate between inviting and emotionally black-mailing a child into engaging in cyber sex, which may involve descriptions of anything from mutual

masturbation, oral sex or virtual penetrative sex. Typically, this persuasive approach seems to focus a great deal on the child feeling loved and the desire on behalf of the adult that the child will fall in love with the adult is often openly stated. Fantasy seems to be an important element of the adult's interactions with the child and for the fantasy to work there seems to be a need for the child to appear willing to engage in on-line sexual activities.

### **Fantasy enactment: overt coercion counterbalanced with intimacy**

However, the research findings indicate that at least some of the individuals who engage a child in the virtual enactment of their fantasies may adopt a far more overt pattern of coercion, which is sometimes counterbalanced by intimacy and friendship.

For example

*Adult 'tell me how you would touch my c\*\*\*k'*

*Child "I feel uncomfortable"*

*Adult 'just do it, come on just do it, what are you waiting for?'*

*Child 'I don't want to'*

*Adult 'Don't let me down, come on now, I am touching you making you feel really good, I love you, come on you will like this, don't you want to make me happy'*

### **Cyber-rape fantasy enactment: overt coercion, control and aggression**

Furthermore, some individuals will resort to the use of aggressive phrases to coerce a child and this method will be replaced with a much more directive and aggressive commands, e.g.

*Adult " do as I f\*\*\*king say right now bitch or you will be in big f\*\*\*king trouble"*

### **Methods of concluding a cybersexploitation and /or grooming encounter.**

#### **Damage limitation**

Online grooming or cybersexploitation encounters are sometimes characterized by a set of what could be termed as 'damage limitation' exercises by the adult or adolescent with a sexual interest in children. These involve very positive encouragement and high praise for a child and it seems reasonable to conclude that the intention is to reduce the risk of a frightened child divulging details of the on-line activities to anybody else. This damage limitation stage typically involves repetition of phrases by the protagonist of 'this is our secret' and 'I love you'. In particular, this is a common characteristic of the latter stages of online grooming and over time it can acquire an almost ritualistic quality that is a necessary part of the encounter.

### **'Hit and run' tactic**

More typically, especially in the case of very aggressive cyber-rapists, there is evidence of what could be termed a 'hit and run' mentality and rarely during the course of research was the aggressive cyber-rapist interested in either damage limitation, extending contact or indeed in scheduling either a repeat online or an offline encounter. This raises issues about our understanding of the motivations of these offenders, the need for education for children and the possibility of low risks of detection due to perhaps guilt, embarrassment, shame, and fear of an angry response from parents. Currently, there are low levels of provision of help lines for children where they could bring these activities to the attention of relevant authorities and receive adequate counselling and support. At present it is only possible to hypothesize about the possible psychological impact of these kinds of experiences on vulnerable children, but it seems reasonable to suggest that there is a likelihood that for some children at least, these experiences may have both short and long-term ill effects.

### **Adjusting for age**

The level of duplicity engaged in by the adult means it is very difficult for a child to detect that firstly, they are not in fact talking to a child, and secondly to discover the true intentions of the adult. The patterns of conversation will vary slightly with the age of the child, but it would be contrary to evidence to assume that because a child is, for example, 8 years old rather than 12 years old, that there is a very significant difference in the degree or extent of sexual suggestion or coercion employed. The variations relate to providing more explanations of what, for example, 'fingering' or 'touching oneself' actually means, but once those baseline levels of understanding have been achieved then the pattern of the conversation continues in a manner that closely approximates what is outlined above.

## Recommendations

**1**

Test the current proposed strategies designed to combat on-line grooming. Develop a system to ensure the ongoing evaluation of both existing and proposed regulatory systems and structures to ensure that they continue to be adequate.

A review of the findings of this research with regard to cyberexploitation and grooming practices by those involved in discussing issues surrounding the introduction of the proposed 'anti-grooming' legislation would afford the opportunity to clarify the nature of criminal activities, which are being legislated against. It would be judicious to consider not only the fixed Internet context but also the mobile Internet when conducting the proposed review. In addition, the process of checking how well the proposed legislative framework copes with various research based scenarios might expose potential loopholes, which might otherwise have unwittingly been built into the legislative framework.

**2**

**Recognition of the evidential issues that the proposed anti-grooming legislation will give rise to at a number of levels.**

From an operational policing perspective, in addition to cyber trails the potential evidential aspects of the content of conversations ought to be considered, i.e. the information an adult or adolescent with a sexual interest in children reveals throughout the course of a conversation, for example, real world location, occupation, hobbies, which, although it would have to be regarded as open source information, i.e. needed to be verified, nonetheless it may still be worth investigating. This is particularly relevant as one of the main aims of the proposed anti-grooming legislation is to identify and apprehend alleged paedophiles prior to the commission of a real world offence and therefore in addition to cyber trails the content details revealed by an alleged offender in conversations may be particularly relevant and must not be overlooked.

Arguably, if a case reaches a court of law one of the key issues will be the *content of conversations*, which will play an integral role in establishing a 'course of conduct' if and when the proposed anti-grooming legislation becomes law. This will inevitably give rise to questions

concerning the evidential integrity and admissibility of copies of conversations, which allegedly contain evidence of grooming and cyberexploitation. It seems reasonable to suggest that decisions with regard to the integrity of evidence and Service Providers role in this respect could be arrived at by experts in the field of network security and cyber crime investigations prior to the enactment of law which would preclude the necessity to rely wholly on precedents being set in courtrooms wherein the relevant expertise may not exist.

In addition to issues surrounding the content of conversations, a crucial issue relates to the fact that *copies of conversations may be acquired in any number of ways*, for example;

- The alleged victim may have intentionally saved the conversation on his/her hard drive, which are subsequently accessed by the police.
- The alleged victim may have sent a copy of the conversation to the Chat Service Provider as part of a report of abuse, which is subsequently accessed by the police.
- Computer crime units may be able to retrieve part or whole sections of conversations from swap files on the alleged victims hard drive.
- Similarly, as soon as the investigation leads officers to the alleged offender whole or part of conversations may be retrieved from the alleged offenders' computer hard drive.
- The Chat Service Provider may capture a copy of a conversation server side as soon as an alleged victim alerts them to the abuse, or perhaps a moderator becomes aware of abuse taking place.
- However, if the alleged incident of cyberexploitation and /or grooming took place via a 3Gmobile phone and included for example, SMS, MMS, video messaging, and voice-mail, it is important to take into account the limited capacity to save copies of communications on a mobile device. These issues need to be taken in account not only by law enforcement but also legislators, and most importantly, by mobile phone product developers and software engineers.

A host of issues with respect to the evidential nature of material gathered client versus server side will arise as a result of proposed changes to legislation, not only at an operational policing level but also in terms of the admissibility of evidence in a court of law. Arguably, there is a need for clear protocols to be laid down with respect to Chat and IM for Service Providers, users and law enforcement - not only with regard to what level of detail in terms of traffic data is recorded by Service Providers, but also with respect to ensuring that systems are set in place so that end users have the facility to save copies of conversations that meet certain requirements in relation to admissibility in a court of law.

**3**

**A networked reporting structure designed to deal with reports of cybersexploitation and grooming that contributes to a central repository ought to be established.**

The fact that individual adults or adolescents with a sexual interest in children utilise a number of strategies to avoid detection, including using different Chat Service Providers to target victims, combined with the large number of possible Chat Service Providers, suggests the need for a networked reporting system which feeds into a central repository handled by law enforcement. A central repository would facilitate the systematic analysis of reports of online grooming that would assist law enforcement to not only link offences committed by individuals across different Chat Services, but also to identify distinctive modus operandi's and elements of victimology, all of which may have an important role from both a crime preventative and crime reactive perspective. Crucially such a system would serve to increase police officers opportunities to become involved in alleged cases of grooming before any offence occurs in the real world.

One of the key issues in this regard relates to the establishment of systems whereby abuse report teams are operating with a uniform set of criteria based on a gradient which incorporates a checking system whereby decisions can be reached with regard to which complaints need to be escalated to the police and which ones need to be tagged.

In addition it is important to consider the issue, as raised earlier, in relation to adolescents with a sexual interest in children and how situations where for example, a complaint is made with respect to a 15 year old cybersexploiting a 9 year old, versus a 15 year old cybersexploiting a 13 year old. Of course, it is imperative to remember that it is not possible to know the actual age of the person sitting at the computer and this really would be a matter for the police investigating the alleged crime to handle.

The author acknowledges that such a system would have to be governed by tight protocols as regards control (handling and retention) of data, access both to input and view data, and also even more fundamental issues such as defining what kind of chat services or online communities would be included in such a database.

A possible adjunct to the networked reporting structure would be a 'one-stop' advice line where children can find sources of advice about how to cope with negative experiences they have encountered either on the fixed or mobile Internet.

**4****Programs of awareness raising and training ought to be developed for the criminal justice sectors.**

Crimes which involve both existing and emerging communication technologies increasingly feature in cases that reach court rooms but it does not always follow that members of the criminal justice system and in particular, the judiciary, have received any kind of learning opportunities about how to deal with these kinds of crimes, and in particular how to deliberate in relation to the admissibility of computer based forensic evidence. Clearly this potential deficit in knowledge needs to be redressed.

**5****Programs of education and awareness raising ought to be developed for children, parents, teachers and those who work with or come in contact with children on a regular basis.**

A significant amount of work has been conducted in the field of education and awareness raising at local, European and global level, for example in the UK alone, the Home Office Internet Task Force's recent advertising campaign with respect to chat rooms, and the Department for Education and Skills' Internet Proficiency scheme for pupils aged 7-11. European Commission funded projects such as [www.fkbko.net](http://www.fkbko.net) and [www.safer-internet.net](http://www.safer-internet.net) demonstrate the high level of commitment to both education and awareness raising with respect to safe use of communication technologies. In addition, conferences such as the 2003 Netsafe conference in New Zealand which brought together experts from all over the world and other similar events serve as opportunities for information exchange and networking. Notwithstanding the work that has been conducted to date and given that the parameters of criminal activity are likely to be altered as emerging technologies affect the accessibility and vulnerability of children, there is a pressing need to ensure that existing programs of education are updated to pre-empt the risks that new technologies may present and to raise awareness of issues surrounding the risks associated with increased capabilities. For example, programs of education will have to incorporate the means to empower children with an understanding that picture-messaging capabilities, whilst incredibly fun, may have some negative aspects, which they have not foreseen. By raising users' awareness of the kind of decision making they might consider engaging in before deciding to respond to a request for a picture and thereby enhancing critical reasoning and raising their resiliency to the potential

risk prior to the widespread uptake of MMS enabled mobile devices will serve as an effective crime preventative strategy.

## 6

**It is imperative to set up programs of research designed to explore the impact of both existing and emerging technologies not only in relation to children as end users but also in relation to paedophile activity online.**

Programs of research such as these need to be embraced by the wider community, indeed Europe is recognising that in order to maintain a truly dynamic research capability, it needs to support the critical research areas for tomorrow. Advances in scientific understanding are punctuated by unexpected consequences that create new potentialities for harm. Therefore it is of paramount importance that research focuses upon investigating the rates of development and consequent implications of new and emerging internet related communication technologies – specifically mobile technologies - with regard to the exploitation of these technologies by criminals, namely those with an interest in sexually exploiting or abusing children and young people. The specific objectives of such a research program might include:

- Developing an understanding of the implications of new technologies for those who are involved in law enforcement agencies and the investigative process, in terms of the technological forensic complexities involved in monitoring criminal activity through the use of mobile technologies.
- To research how children and young people are utilising these new technologies for both educational and recreational purposes, with the view to tailoring both products and safety advice to their explicit needs.
- An exploration of the potential of developing research based profiling techniques in relation to cyberexploitation and both online and offline grooming.
- An exploration of the psychological effects of exposure to cyberexploitation and online grooming, on both children and teenagers, who have experienced these activities on-line.

Crucially, research of this nature would help to clarify and prioritise the issues that accompany the increasing availability of mobile Internet access in order to devise appropriate strategies and make the greatest impact upon target audiences.

**7**

**Create avenues of communication between product developers and child internet safety groups so that at the inception of product development child safety is one of the issues that is taken into account.**

To date, responses to online grooming have involved policy decisions which are responsive to the existing technologies and the associated risks. With the advent of 3G, WAN, IP V6, etc, there is an opportunity to engage with industry at the mission critical stage of product development to ensure that child safety issues are an integral part of the product developers' and software engineers' agendas. Currently, the Home Office Internet Task Force in the UK has been instrumental in bringing together key players from the industry, child welfare organisations, government departments and researchers to discuss ways in which to tackle issues in relation to the Internet. To this end a number of sub groups have been formed and it would seem wise either to extend the scope of one of these groups, or indeed form a new group to discuss issues from a technical perspective. It would seem timely at this juncture to suggest that these avenues ought to be explored so that product developers and software engineers, especially those of new technologies, are invited to join the discussion forum. In this way it would be possible for policy makers and educationalists to predict with greater certainty the kinds of risks that may be associated with products that will soon hit the markets and in this way it will be possible to devise some kinds of pre-emptive strategies.

It is anticipated that the remit of such a newly formed group would include at least some of the following:

- To conduct a review of existing and emerging networking protocols with respect to enhancing child safety on-line.
- To focus on the processes underpinning industry's product development, and an exploration of the options pertaining to, for example, product differentiation on the basis of the end-user.
- Creation of outlines of possible minimum standards for industry with respect to child users, ensuring the implementation of these standards, and development of mechanisms, whereby industry compliance can be tested, so that there is an ongoing evaluation process designed to establish the effectiveness of these standards.
- Working to define further both the nature and extent (as far as is possible) to which paedophiles use and exploit a variety of different communication platforms, the knowledge from which would feed into a number of areas outlined by the preceding recommendations, but crucially would enable product developers to gain a better understanding of how technologies can be exploited by adults and adolescents with a sexual interest in children.