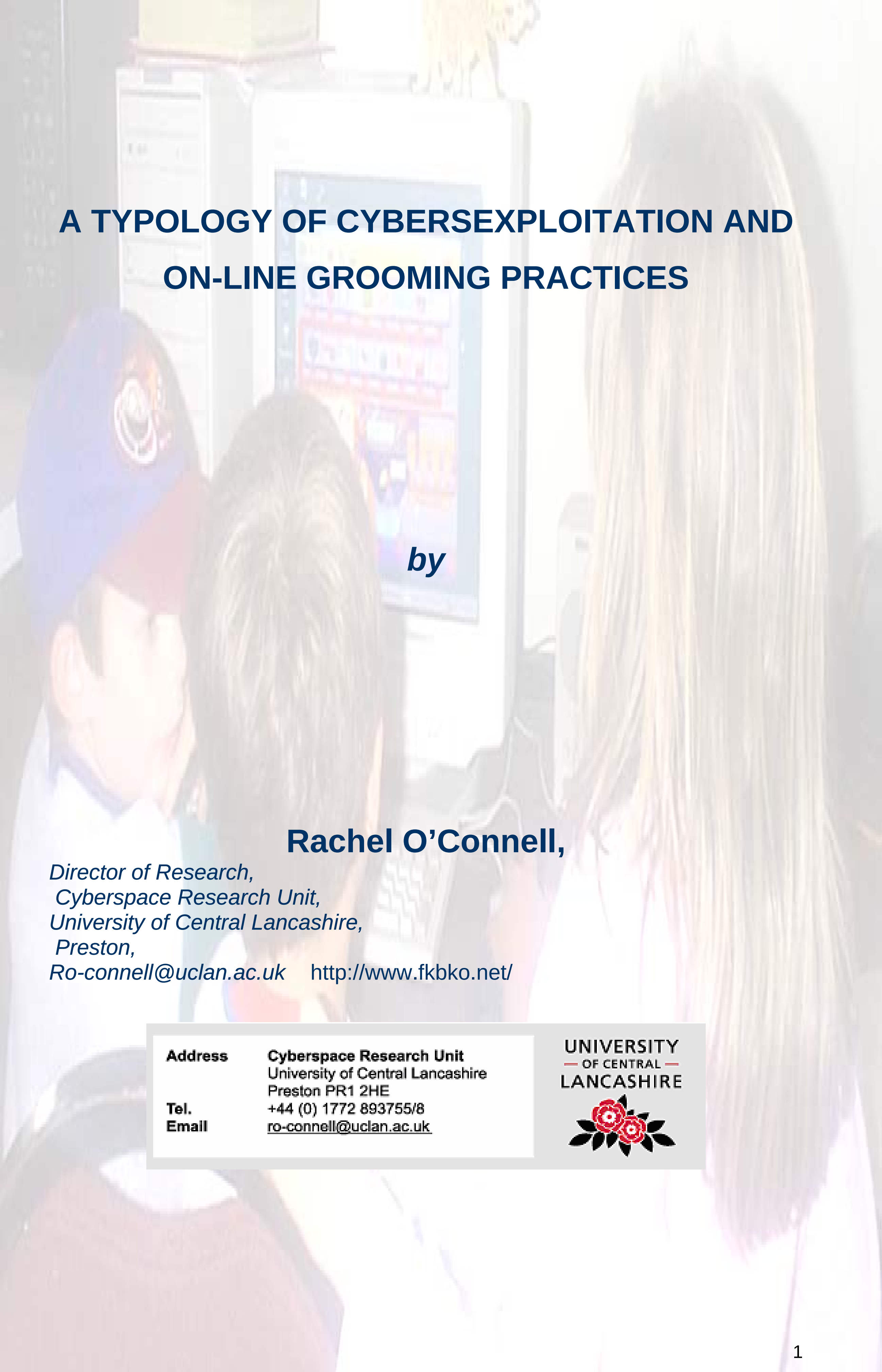


A TYPOLOGY OF CYBERSEXPLOITATION AND ON-LINE GROOMING PRACTICES

by

Rachel O'Connell,

Director of Research,
Cyberspace Research Unit,
University of Central Lancashire,
Preston,
Ro-connell@uclan.ac.uk   http://www.fkbko.net/

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

UNIVERSITY
— OF CENTRAL —
LANCASHIRE

Introduction

The purpose of this introduction is to provide a brief overview of both the scope of the program of research, which has given rise to this paper and the methodology employed for the particular research reported in this paper. This paper summarises a section of a key-note address at the Netsafe conference to take place in Auckland, New Zealand, July 2003. The following paragraphs provide a general background to the area of research and a rationale for the investigation is outlined. A summary of the main findings are outlined in the Executive Summary and the implications of this research are provided followed by recommendations for further action in this area.

Background

The program of research began in October 1996, at University College, Cork, Ireland, as part of an M.Phil. programme and shortly after was converted to a Ph.D. Parts of this program of research are ongoing at the Cyberspace Research Unit, University of Central Lancashire. The main aims of the research were as follows:

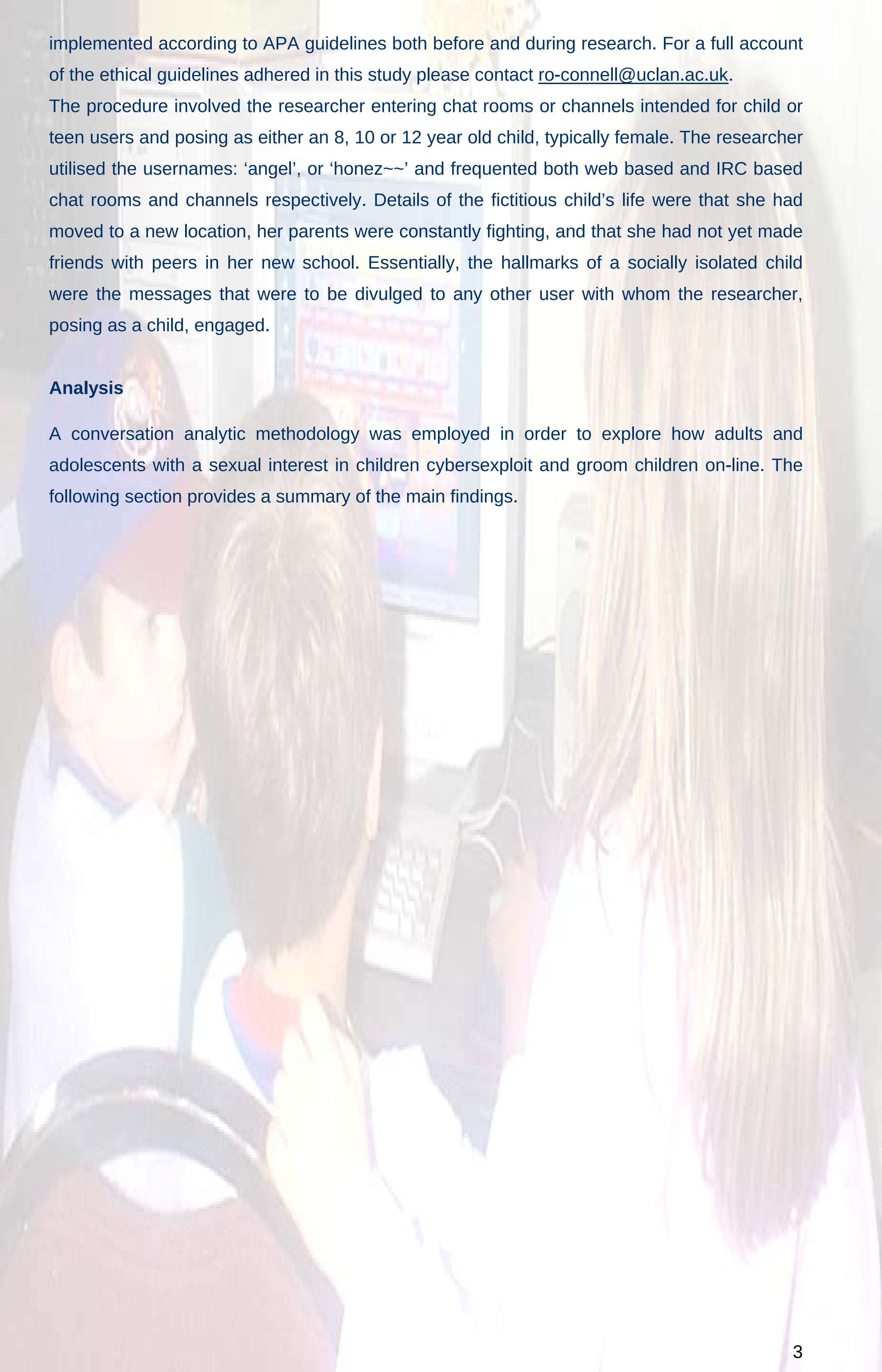
To explore the structure and social organisation of paedophile activity on the Internet:

1. To investigate the nature and qualities of child sex-related activities such as collection, dissemination and trading of child erotica and child pornography.
2. To explore, using qualitative research techniques, particularly discourse analysis, the psychological structures underlying adult sexual interest in children.
3. To inform and improve the capacity of law enforcement organisations to more effectively deal with this important social problem.

The methods employed to explore paedophile activity on the Internet combine both qualitative and quantitative research methods. The following paper focuses on the findings of one part of this program of research, i.e., an exploration of both cybersexploitation and grooming practices employed by adults and adolescents with a sexual interest in children when operating in chat rooms intended for either children or teenagers. In cases of cybersexploitation and grooming, language is a tactical implement, which is used by adults with a sexual interest in children to identify, deceive, coerce, cajole, form friendships with and also to abuse potential victims.

Methodology

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 guidelines both before and during research. For a full account of the ethical guidelines adhered in this study please contact ro-connell@uclan.ac.uk.

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.

Analysis

A conversation analytic methodology was employed in order to explore how adults and adolescents with a sexual interest in children cybersexploit and groom children on-line. The following section provides a summary of the main findings.

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'.

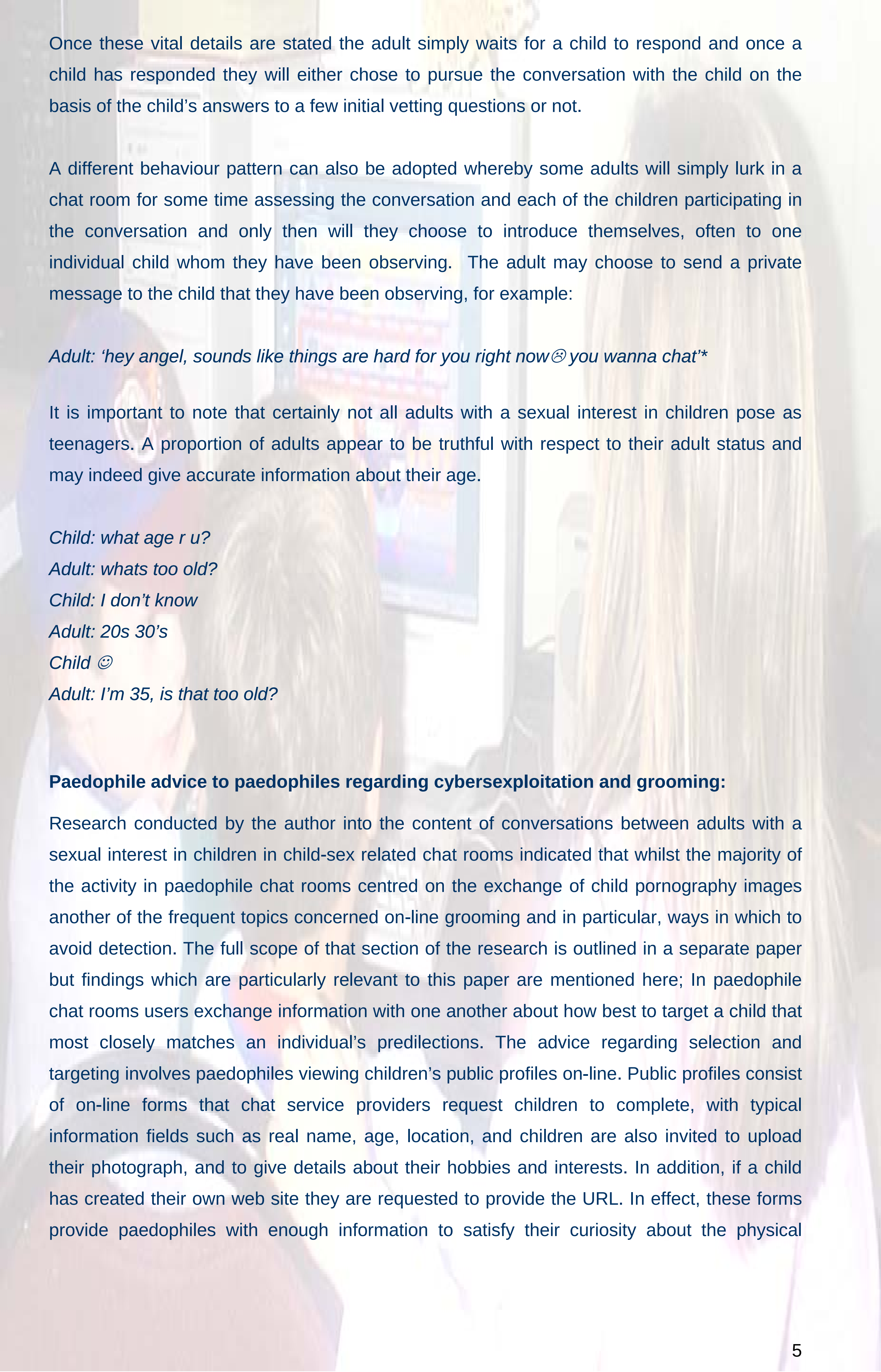
For the purposes of providing a broader outlook the anticipated impact of 3G mobile phones was considered when drafting these recommendations and a range of both pre-emptive strategies and proposals for policy makers in relation to 3G are included here. For a fuller account of the capabilities and risks 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[1]: '14/m/uk'

[1] 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 chose 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 cybersexploitation 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 cybersexploitation 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 cybersexploitation 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 meetings 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.

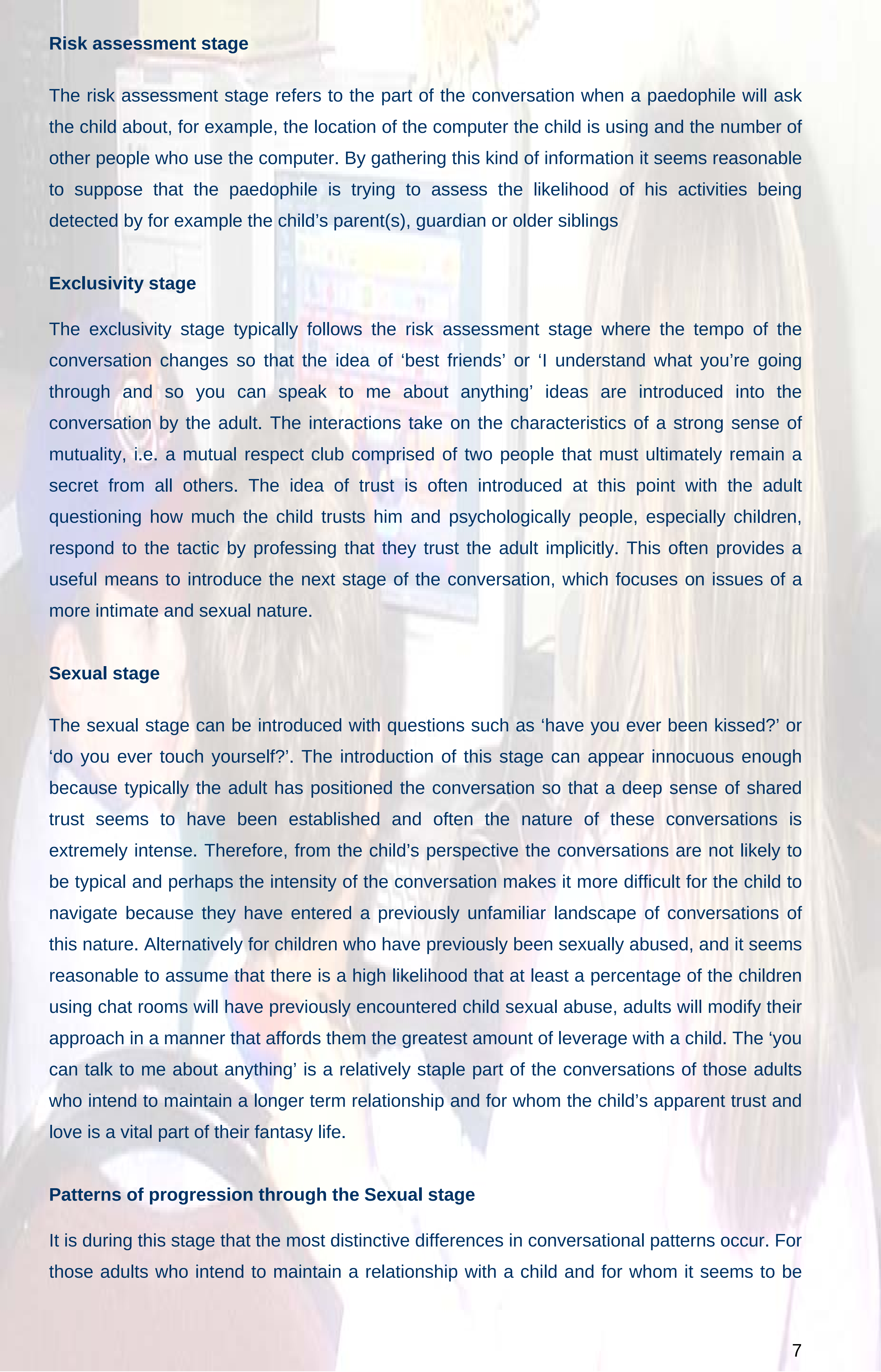
The following paragraphs provide a summary of the findings of an ongoing program of research, which aims to explore the possibility of developing socio linguistic profiling techniques designed to analyse the speech employed by people who engage in on-line grooming.

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.

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 between 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.

Cybersexploitation: 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

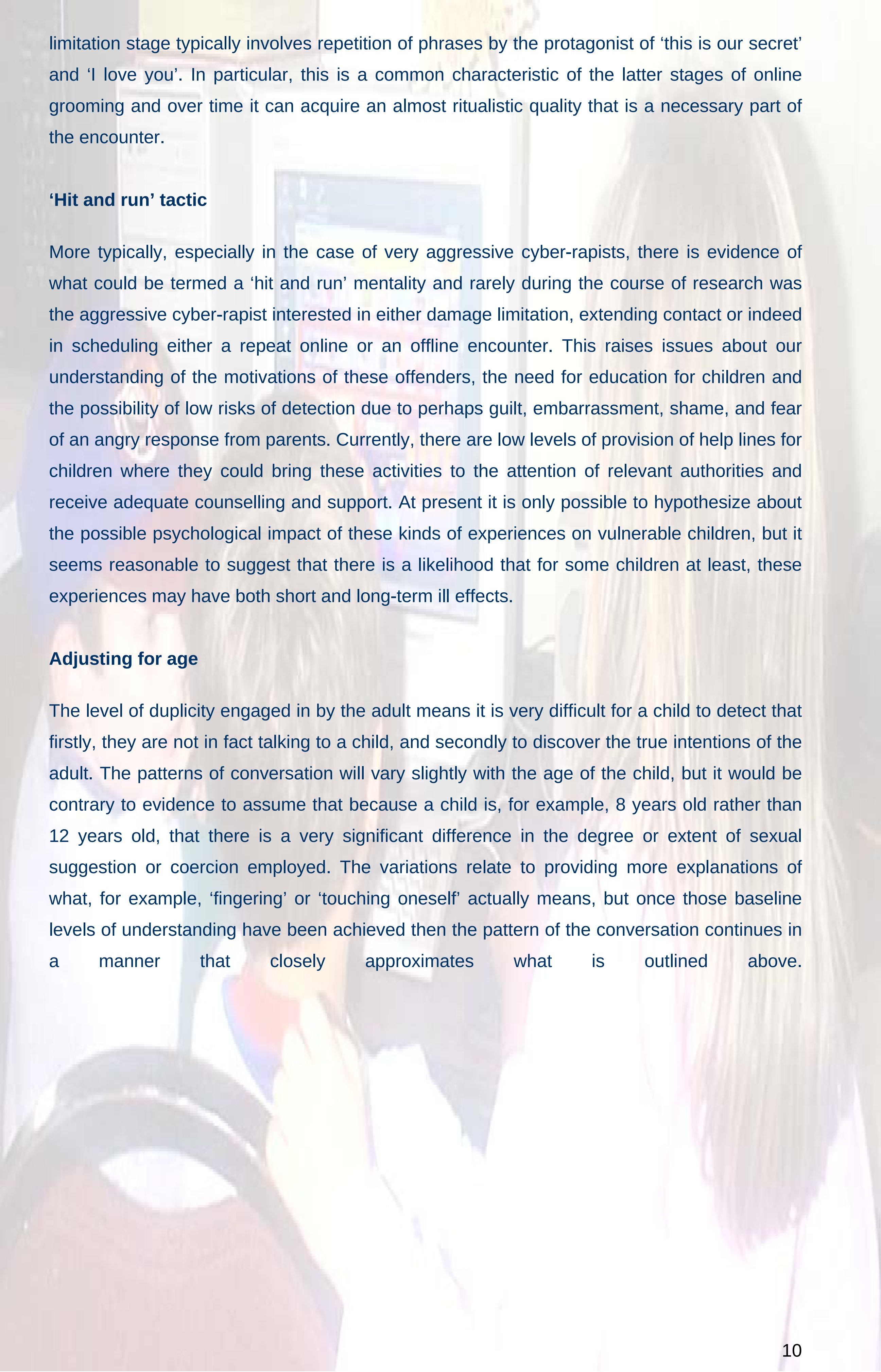
Furthermore, some individuals will resort to the use of aggressive phrases to coerce a child and this method will be replaced with a much more directive and aggressive commands, e.g.

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

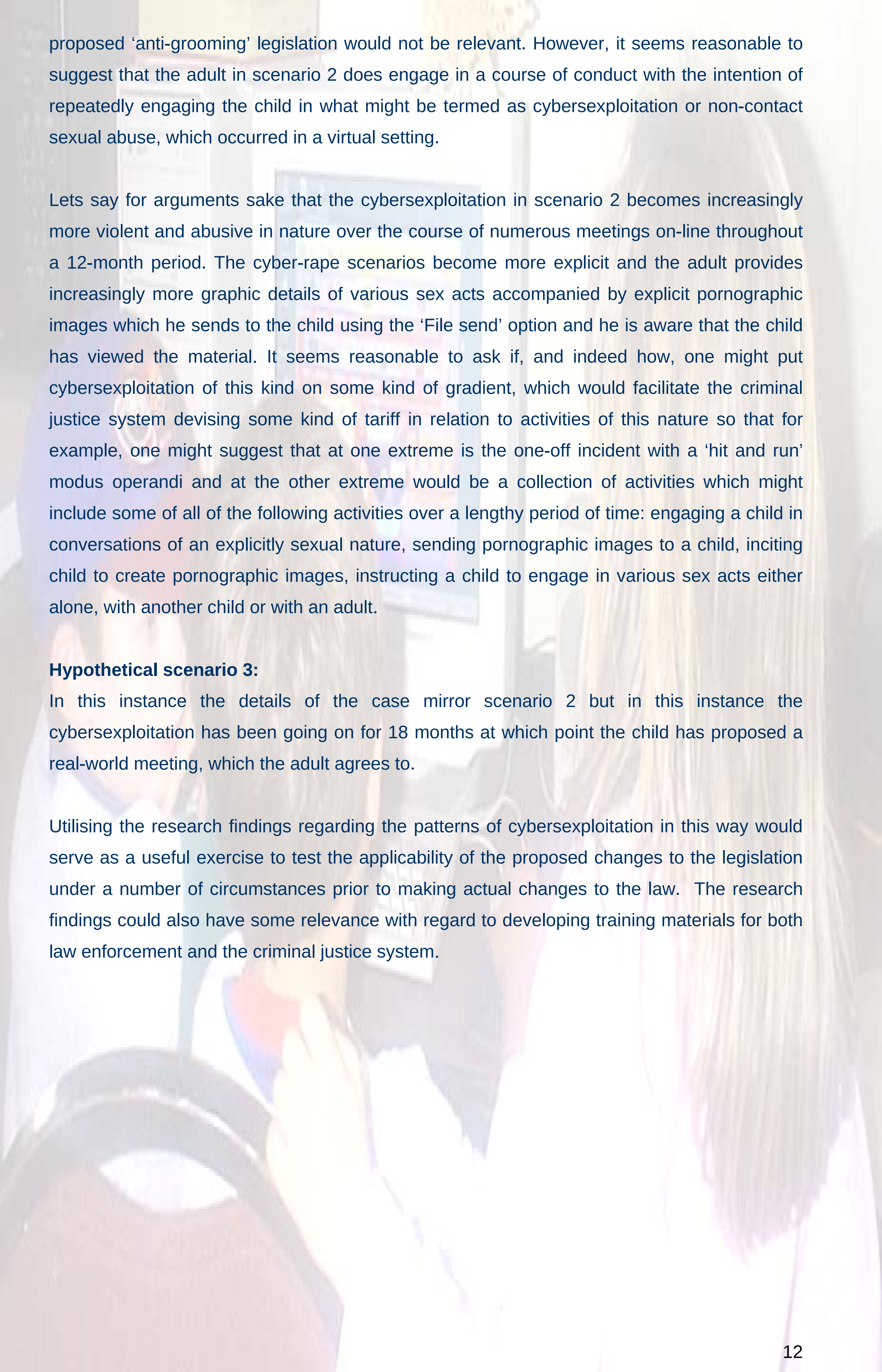
Growing out of the research findings outlined in this paper, in particular the typology of cybersexploitation and grooming practices, which have relevance on a number of levels, the following recommendations relate to a number of those levels; i.e. legislative changes, operational policing strategies, strategic management of reports of cybersexploitation and grooming, and also a proposal detailing the parameters of longer term programs of research designed to increase our working knowledge of the processes that underpin both cybersexploitation and grooming. Whilst this list of recommendations is certainly not exhaustive, it serves as a useful starting point to initiate discussion about possible ways to strategically combat these illegal and harmful activities. A comprehensive rationale behind the recommendations follows each individual recommendation.

Recommendation 1: Test proposed changes in legislation

A review of the findings of this research with regard to cybersexploitation 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, this process might expose potential loopholes, which might be unwittingly be built into the process.

Hypothetical scenario 1 might include the following features:
An adult with a sexual interest in children engages in cybersexploitation of a 10 year-old girl, involving the child in the enactment of a particularly violent rape fantasy, utilising an overtly coercive approach counterbalanced by aggression. However, throughout the whole conversation no mention is made about an intention to meet with the target victim in the real world. Scenario 1 concludes with this adult employing a 'hit and run' method to end the conversation and seemingly makes no further contact with the 10 year old girl.

Hypothetical scenario 2,
Which, for illustrative purposes, is the same in every respect to scenario 1 except that at the end of the Fantasy Enactment stage instead of terminating contact the adult in this scenario does make an effort to reassure the 10 year old girl and goes through what has been termed the 'Damage Limitation' stage before scheduling a number of repeat meetings on-line which involve cybersexploitation. Similar to scenario 1 the adult in scenario 2 never mentions a real world face-to-face meeting and it might seem therefore that proving a course of conduct indicative of the intention to meet with a child for sexual intercourse in the real world under the



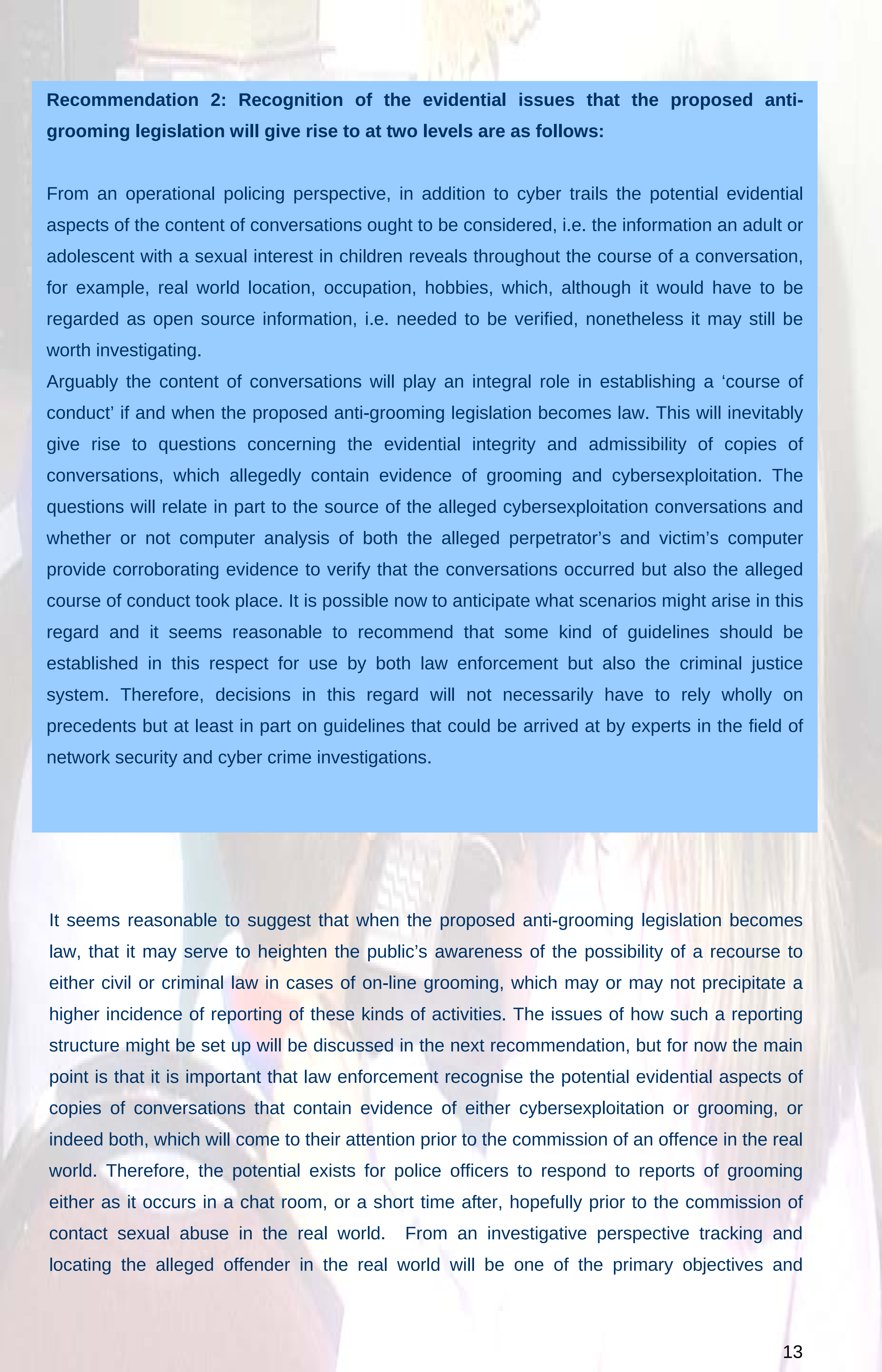
proposed 'anti-grooming' legislation would not be relevant. However, it seems reasonable to suggest that the adult in scenario 2 does engage in a course of conduct with the intention of repeatedly engaging the child in what might be termed as cybersexploitation or non-contact sexual abuse, which occurred in a virtual setting.

Lets say for arguments sake that the cybersexploitation in scenario 2 becomes increasingly more violent and abusive in nature over the course of numerous meetings on-line throughout a 12-month period. The cyber-rape scenarios become more explicit and the adult provides increasingly more graphic details of various sex acts accompanied by explicit pornographic images which he sends to the child using the 'File send' option and he is aware that the child has viewed the material. It seems reasonable to ask if, and indeed how, one might put cybersexploitation of this kind on some kind of gradient, which would facilitate the criminal justice system devising some kind of tariff in relation to activities of this nature so that for example, one might suggest that at one extreme is the one-off incident with a 'hit and run' modus operandi and at the other extreme would be a collection of activities which might include some of all of the following activities over a lengthy period of time: engaging a child in conversations of an explicitly sexual nature, sending pornographic images to a child, inciting child to create pornographic images, instructing a child to engage in various sex acts either alone, with another child or with an adult.

Hypothetical scenario 3:

In this instance the details of the case mirror scenario 2 but in this instance the cybersexploitation has been going on for 18 months at which point the child has proposed a real-world meeting, which the adult agrees to.

Utilising the research findings regarding the patterns of cybersexploitation in this way would serve as a useful exercise to test the applicability of the proposed changes to the legislation under a number of circumstances prior to making actual changes to the law. The research findings could also have some relevance with regard to developing training materials for both law enforcement and the criminal justice system.

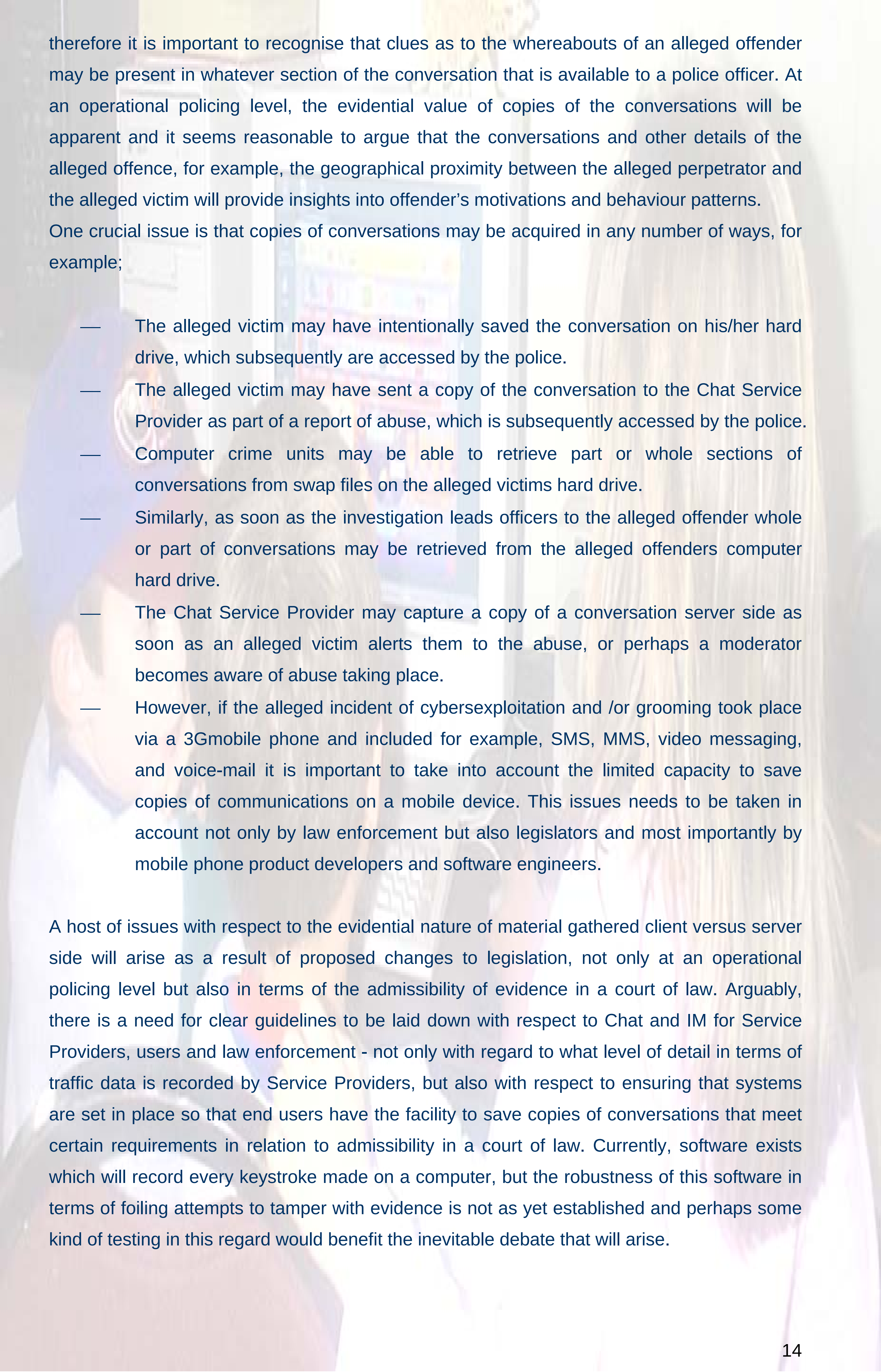


Recommendation 2: Recognition of the evidential issues that the proposed anti-grooming legislation will give rise to at two levels are as follows:

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.

Arguably the content of conversations 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 cybersexploitation. The questions will relate in part to the source of the alleged cybersexploitation conversations and whether or not computer analysis of both the alleged perpetrator’s and victim’s computer provide corroborating evidence to verify that the conversations occurred but also the alleged course of conduct took place. It is possible now to anticipate what scenarios might arise in this regard and it seems reasonable to recommend that some kind of guidelines should be established in this respect for use by both law enforcement but also the criminal justice system. Therefore, decisions in this regard will not necessarily have to rely wholly on precedents but at least in part on guidelines that could be arrived at by experts in the field of network security and cyber crime investigations.

It seems reasonable to suggest that when the proposed anti-grooming legislation becomes law, that it may serve to heighten the public’s awareness of the possibility of a recourse to either civil or criminal law in cases of on-line grooming, which may or may not precipitate a higher incidence of reporting of these kinds of activities. The issues of how such a reporting structure might be set up will be discussed in the next recommendation, but for now the main point is that it is important that law enforcement recognise the potential evidential aspects of copies of conversations that contain evidence of either cybersexploitation or grooming, or indeed both, which will come to their attention prior to the commission of an offence in the real world. Therefore, the potential exists for police officers to respond to reports of grooming either as it occurs in a chat room, or a short time after, hopefully prior to the commission of contact sexual abuse in the real world. From an investigative perspective tracking and locating the alleged offender in the real world will be one of the primary objectives and



therefore it is important to recognise that clues as to the whereabouts of an alleged offender may be present in whatever section of the conversation that is available to a police officer. At an operational policing level, the evidential value of copies of the conversations will be apparent and it seems reasonable to argue that the conversations and other details of the alleged offence, for example, the geographical proximity between the alleged perpetrator and the alleged victim will provide insights into offender's motivations and behaviour patterns.

One crucial issue is 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 subsequently are 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 cybersexploitation 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. This issues needs 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 guidelines 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. Currently, software exists which will record every keystroke made on a computer, but the robustness of this software in terms of foiling attempts to tamper with evidence is not as yet established and perhaps some kind of testing in this regard would benefit the inevitable debate that will arise.

Recommendation 3: A networked reporting structure designed to deal with reports of cybersexploitation and grooming that contributes to a central repository ought to be established

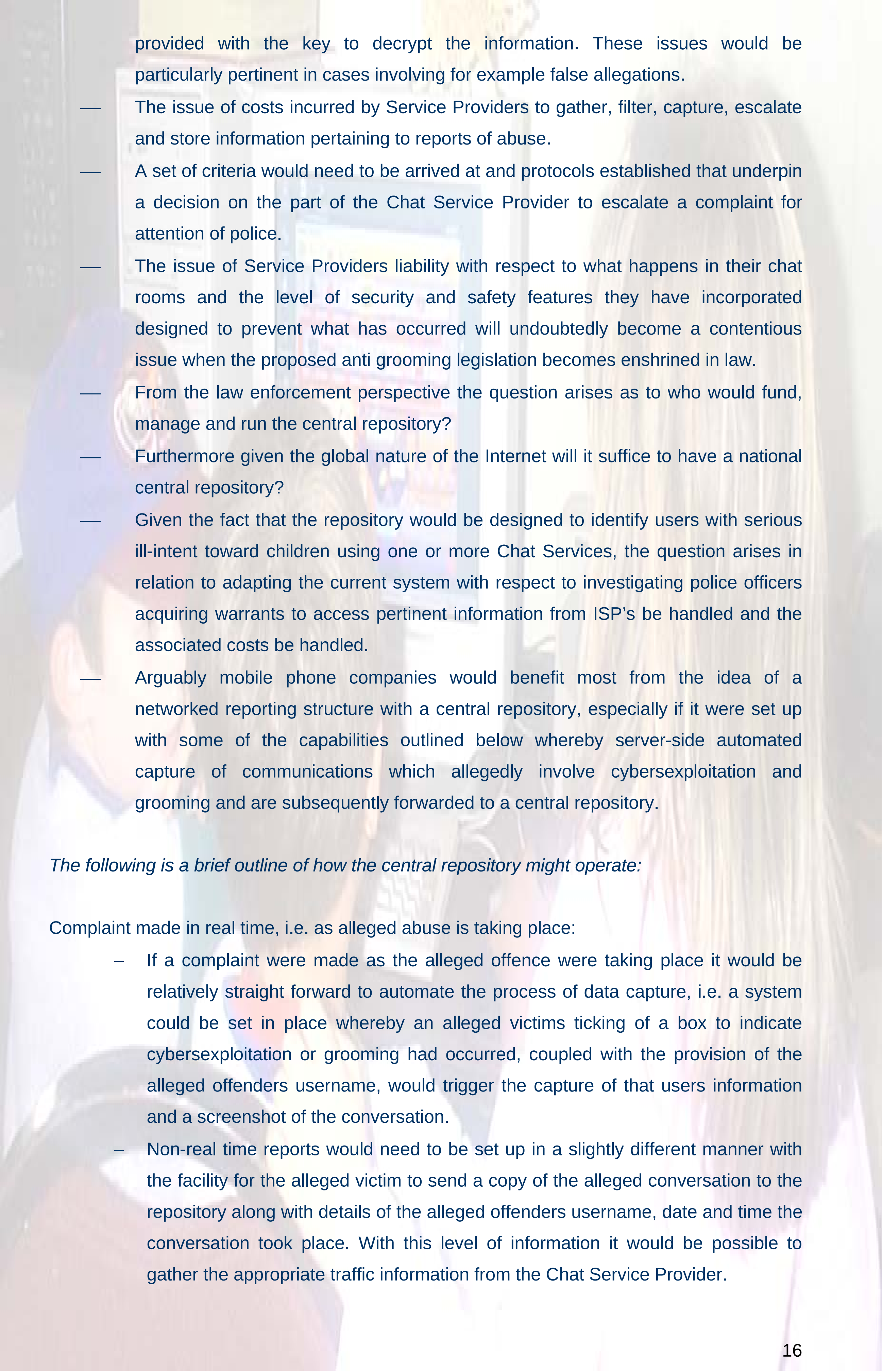
The fact that individual adults or adolescents with a sexual interest in children utilise a number of strategies to avoid detection, including using different Chat Service Providers to target victims, combined with the large number of possible Chat Service Providers, suggests the need for a networked 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 identify 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.

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.

From an operational perspective the proposed networked reporting system recommended here would involve each Chat Service Provider filtering and processing details of complaints of cybersexploitation sent by alleged victims to a central repository. The details might include for example, the alleged victims report, a saved copy, or screen shot of the conversation, and the relevant traffic information of the alleged offender, i.e. IP address, Caller line ID, Username, Date and Time stamp. In addition the Chat Service Provider ought to provide details of any action that has been taken in response to the compliant.

The suggested model for such a database ought to be developed in conjunction with, for example, software engineers who are familiar with a range of real-time communication applications and programs. Clearly the proposed networked reporting system with a central repository would raise a myriad of issues from a number of perspectives for example;

— Data protection with respect to chat users personal details and on-line interactions, and these issues would need to be explored. One possible solution to this issue would be to encrypt information that the Data Protection Act deems ought not be readily available until such time as the police had established reasonable support for the suspicion of criminal activity and upon securing a warrant they would be



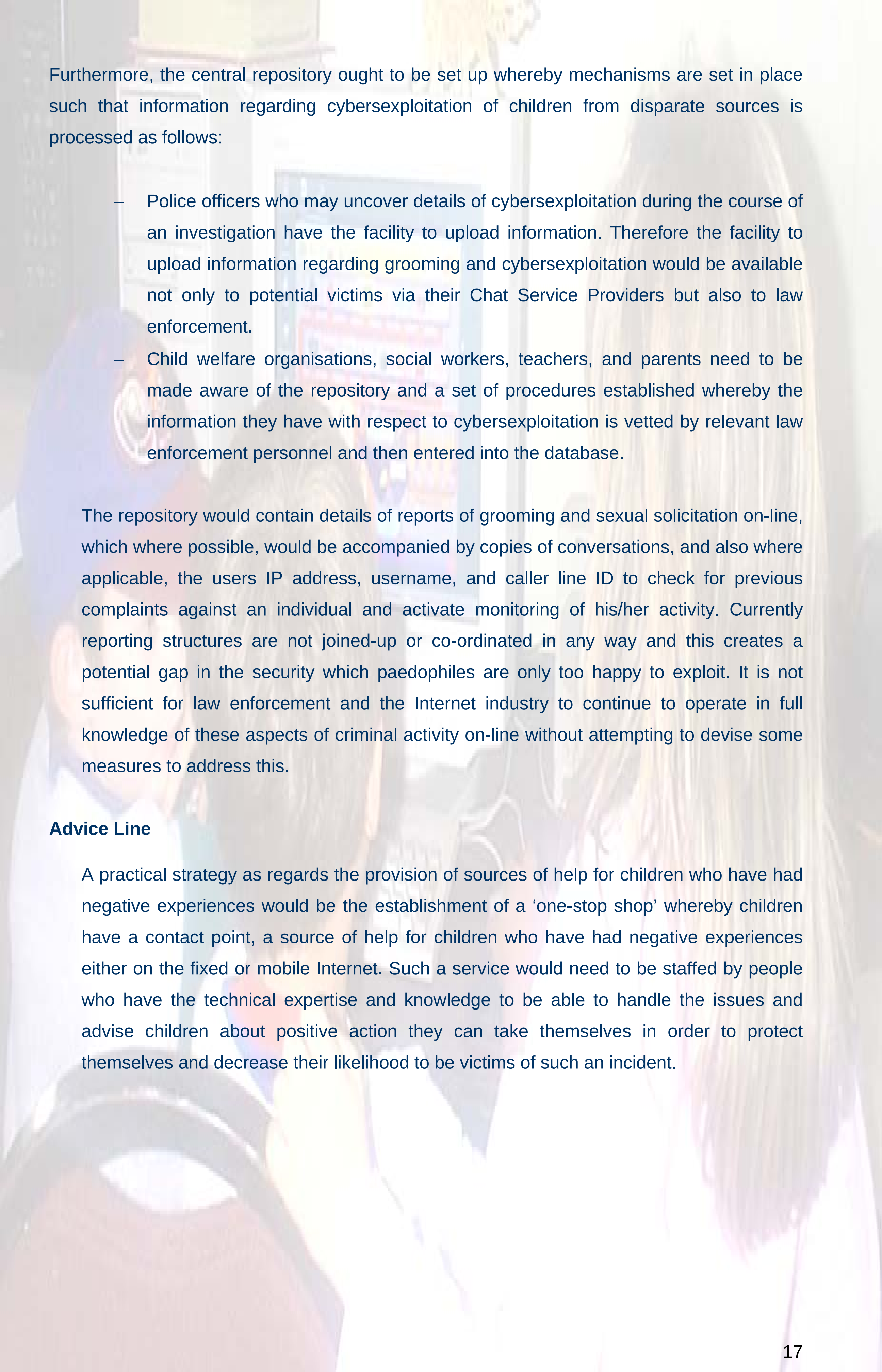
provided with the key to decrypt the information. These issues would be particularly pertinent in cases involving for example false allegations.

- The issue of costs incurred by Service Providers to gather, filter, capture, escalate and store information pertaining to reports of abuse.
- A set of criteria would need to be arrived at and protocols established that underpin a decision on the part of the Chat Service Provider to escalate a complaint for attention of police.
- The issue of Service Providers liability with respect to what happens in their chat rooms and the level of security and safety features they have incorporated designed to prevent what has occurred will undoubtedly become a contentious issue when the proposed anti grooming legislation becomes enshrined in law.
- From the law enforcement perspective the question arises as to who would fund, manage and run the central repository?
- Furthermore given the global nature of the Internet will it suffice to have a national central repository?
- Given the fact that the repository would be designed to identify users with serious ill-intent toward children using one or more Chat Services, the question arises in relation to adapting the current system with respect to investigating police officers acquiring warrants to access pertinent information from ISP's be handled and the associated costs be handled.
- Arguably mobile phone companies would benefit most from the idea of a networked reporting structure with a central repository, especially if it were set up with some of the capabilities outlined below whereby server-side automated capture of communications which allegedly involve cybersexploitation and grooming and are subsequently forwarded to a central repository.

The following is a brief outline of how the central repository might operate:

Complaint made in real time, i.e. as alleged abuse is taking place:

- If a complaint were made as the alleged offence were taking place it would be relatively straight forward to automate the process of data capture, i.e. a system could be set in place whereby an alleged victims ticking of a box to indicate cybersexploitation or grooming had occurred, coupled with the provision of the alleged offenders username, would trigger the capture of that users information and a screenshot of the conversation.
- Non-real time reports would need to be set up in a slightly different manner with the facility for the alleged victim to send a copy of the alleged conversation to the repository along with details of the alleged offenders username, date and time the conversation took place. With this level of information it would be possible to gather the appropriate traffic information from the Chat Service Provider.



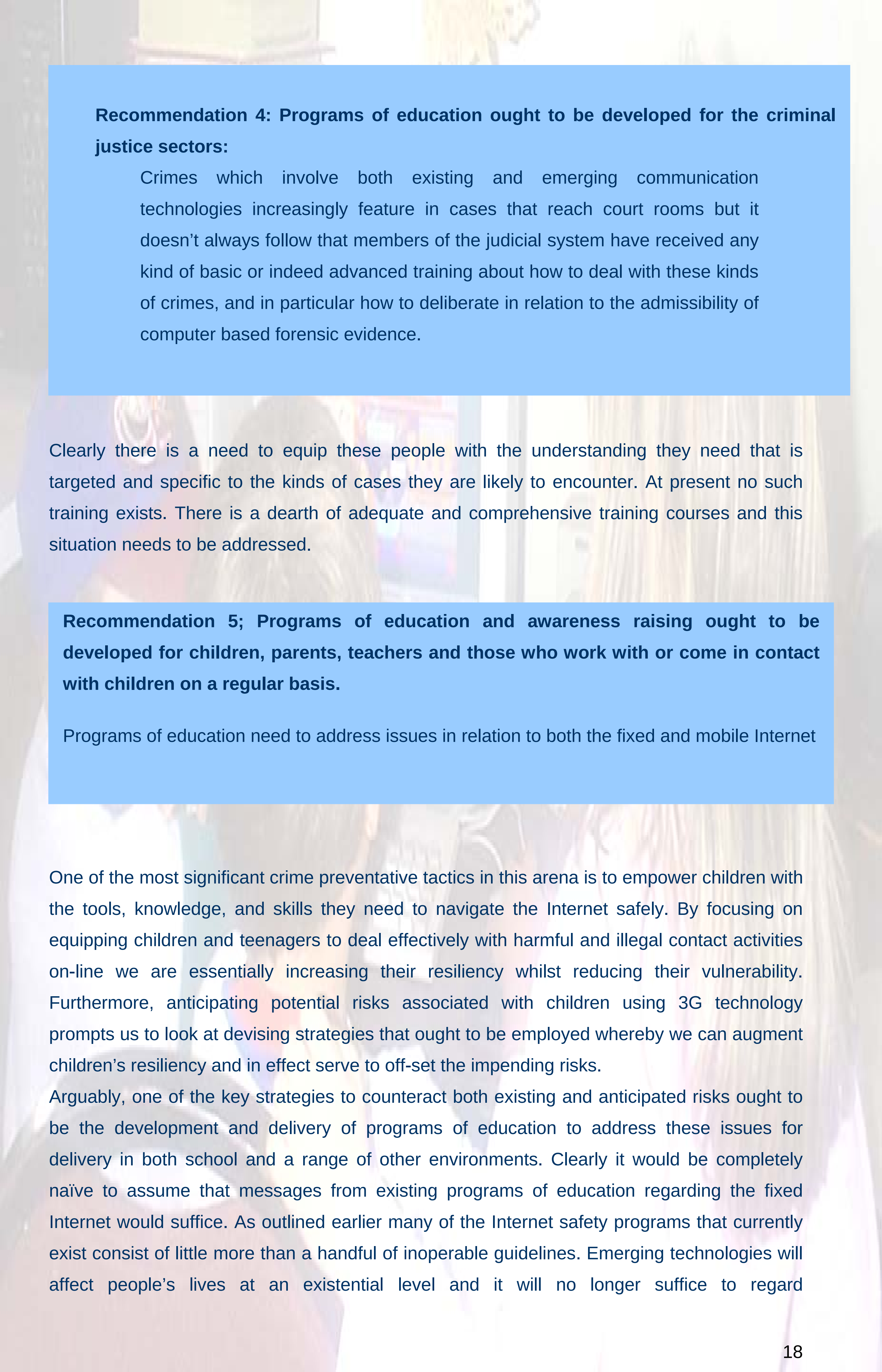
Furthermore, the central repository ought to be set up whereby mechanisms are set in place such that information regarding cybersexploitation of children from disparate sources is processed as follows:

- Police officers who may uncover details of cybersexploitation during the course of an investigation have the facility to upload information. Therefore the facility to upload information regarding grooming and cybersexploitation would be available not only to potential victims via their Chat Service Providers but also to law enforcement.
- Child welfare organisations, social workers, teachers, and parents need to be made aware of the repository and a set of procedures established whereby the information they have with respect to cybersexploitation is vetted by relevant law enforcement personnel and then entered into the database.

The repository would contain details of reports of grooming and sexual solicitation on-line, which where possible, would be accompanied by copies of conversations, and also where applicable, the users IP address, username, and caller line ID to check for previous complaints against an individual and activate monitoring of his/her activity. Currently reporting structures are not joined-up or co-ordinated in any way and this creates a potential gap in the security which paedophiles are only too happy to exploit. It is not sufficient for law enforcement and the Internet industry to continue to operate in full knowledge of these aspects of criminal activity on-line without attempting to devise some measures to address this.

Advice Line

A practical strategy as regards the provision of sources of help for children who have had negative experiences would be the establishment of a 'one-stop shop' whereby children have a contact point, a source of help for children who have had negative experiences either on the fixed or mobile Internet. Such a service would need to be staffed by people who have the technical expertise and knowledge to be able to handle the issues and advise children about positive action they can take themselves in order to protect themselves and decrease their likelihood to be victims of such an incident.



Recommendation 4: Programs of education 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 doesn't always follow that members of the judicial system have received any kind of basic or indeed advanced training 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.

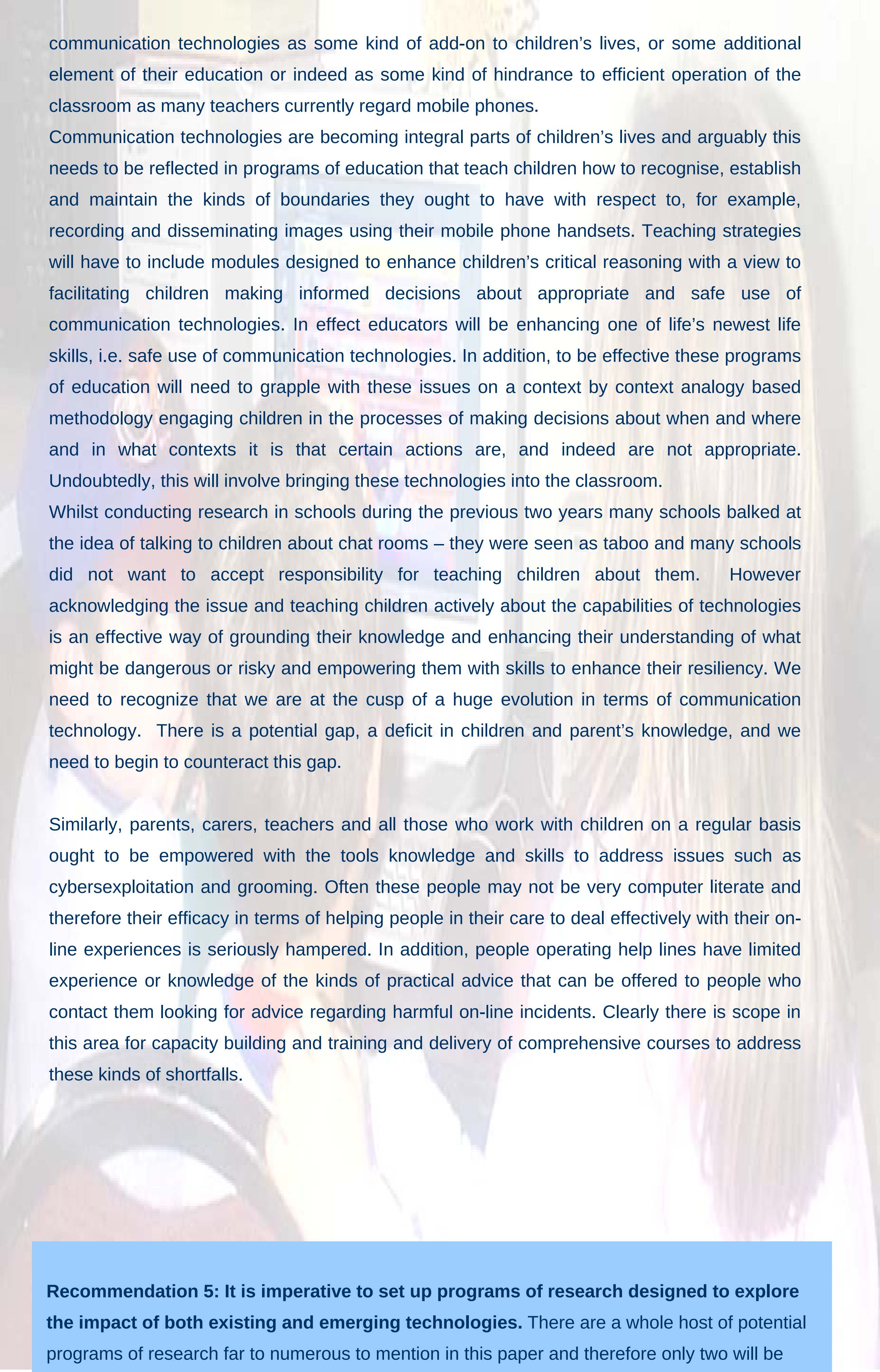
Clearly there is a need to equip these people with the understanding they need that is targeted and specific to the kinds of cases they are likely to encounter. At present no such training exists. There is a dearth of adequate and comprehensive training courses and this situation needs to be addressed.

Recommendation 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.

Programs of education need to address issues in relation to both the fixed and mobile Internet

One of the most significant crime preventative tactics in this arena is to empower children with the tools, knowledge, and skills they need to navigate the Internet safely. By focusing on equipping children and teenagers to deal effectively with harmful and illegal contact activities on-line we are essentially increasing their resiliency whilst reducing their vulnerability. Furthermore, anticipating potential risks associated with children using 3G technology prompts us to look at devising strategies that ought to be employed whereby we can augment children's resiliency and in effect serve to off-set the impending risks.

Arguably, one of the key strategies to counteract both existing and anticipated risks ought to be the development and delivery of programs of education to address these issues for delivery in both school and a range of other environments. Clearly it would be completely naïve to assume that messages from existing programs of education regarding the fixed Internet would suffice. As outlined earlier many of the Internet safety programs that currently exist consist of little more than a handful of inoperable guidelines. Emerging technologies will affect people's lives at an existential level and it will no longer suffice to regard



communication technologies as some kind of add-on to children's lives, or some additional element of their education or indeed as some kind of hindrance to efficient operation of the classroom as many teachers currently regard mobile phones.

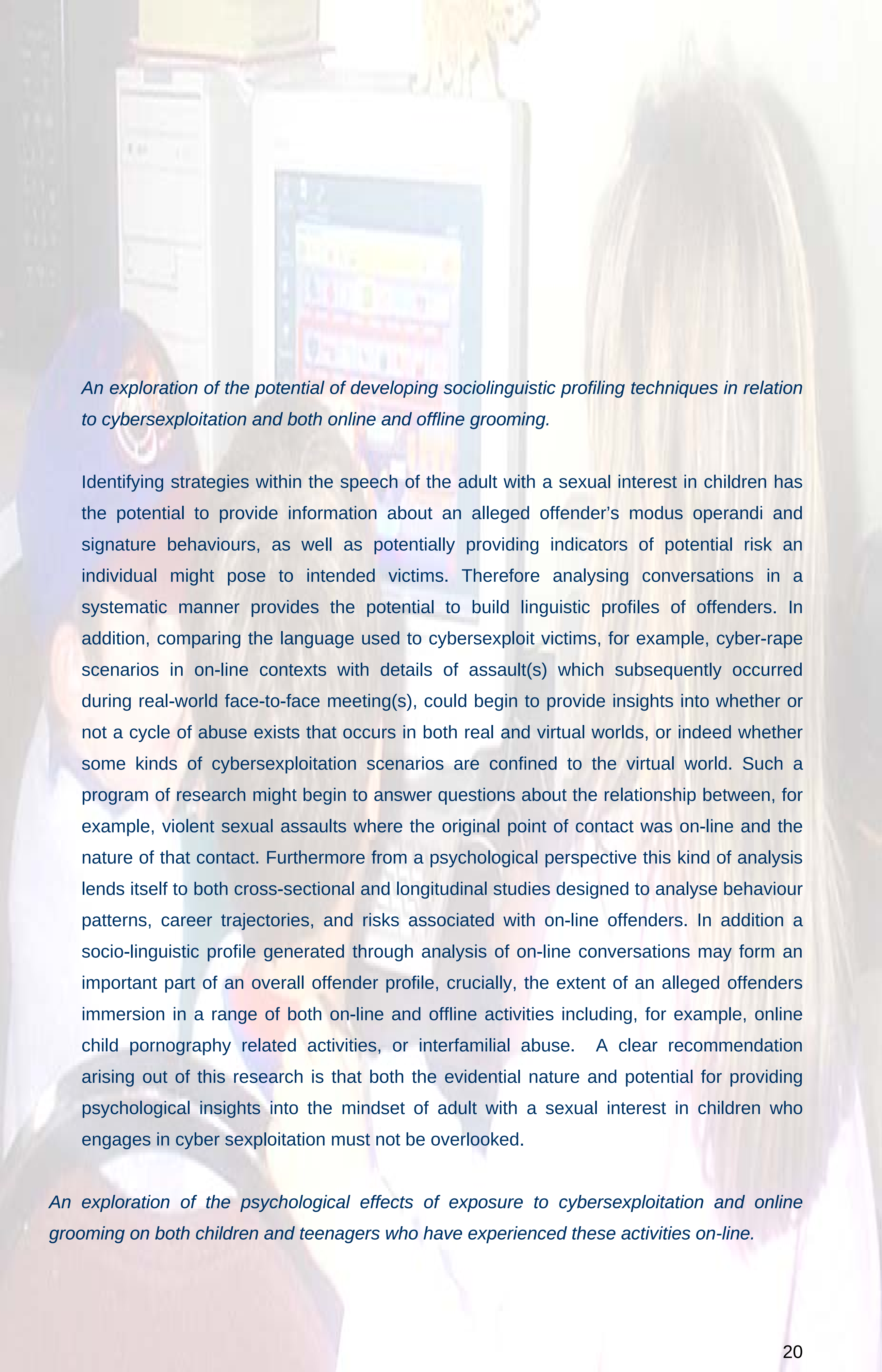
Communication technologies are becoming integral parts of children's lives and arguably this needs to be reflected in programs of education that teach children how to recognise, establish and maintain the kinds of boundaries they ought to have with respect to, for example, recording and disseminating images using their mobile phone handsets. Teaching strategies will have to include modules designed to enhance children's critical reasoning with a view to facilitating children making informed decisions about appropriate and safe use of communication technologies. In effect educators will be enhancing one of life's newest life skills, i.e. safe use of communication technologies. In addition, to be effective these programs of education will need to grapple with these issues on a context by context analogy based methodology engaging children in the processes of making decisions about when and where and in what contexts it is that certain actions are, and indeed are not appropriate. Undoubtedly, this will involve bringing these technologies into the classroom.

Whilst conducting research in schools during the previous two years many schools balked at the idea of talking to children about chat rooms – they were seen as taboo and many schools did not want to accept responsibility for teaching children about them. However acknowledging the issue and teaching children actively about the capabilities of technologies is an effective way of grounding their knowledge and enhancing their understanding of what might be dangerous or risky and empowering them with skills to enhance their resiliency. We need to recognize that we are at the cusp of a huge evolution in terms of communication technology. There is a potential gap, a deficit in children and parent's knowledge, and we need to begin to counteract this gap.

Similarly, parents, carers, teachers and all those who work with children on a regular basis ought to be empowered with the tools knowledge and skills to address issues such as cybersexploitation and grooming. Often these people may not be very computer literate and therefore their efficacy in terms of helping people in their care to deal effectively with their on-line experiences is seriously hampered. In addition, people operating help lines have limited experience or knowledge of the kinds of practical advice that can be offered to people who contact them looking for advice regarding harmful on-line incidents. Clearly there is scope in this area for capacity building and training and delivery of comprehensive courses to address these kinds of shortfalls.

Recommendation 5: It is imperative to set up programs of research designed to explore the impact of both existing and emerging technologies. There are a whole host of potential programs of research far to numerous to mention in this paper and therefore only two will be referred to here.

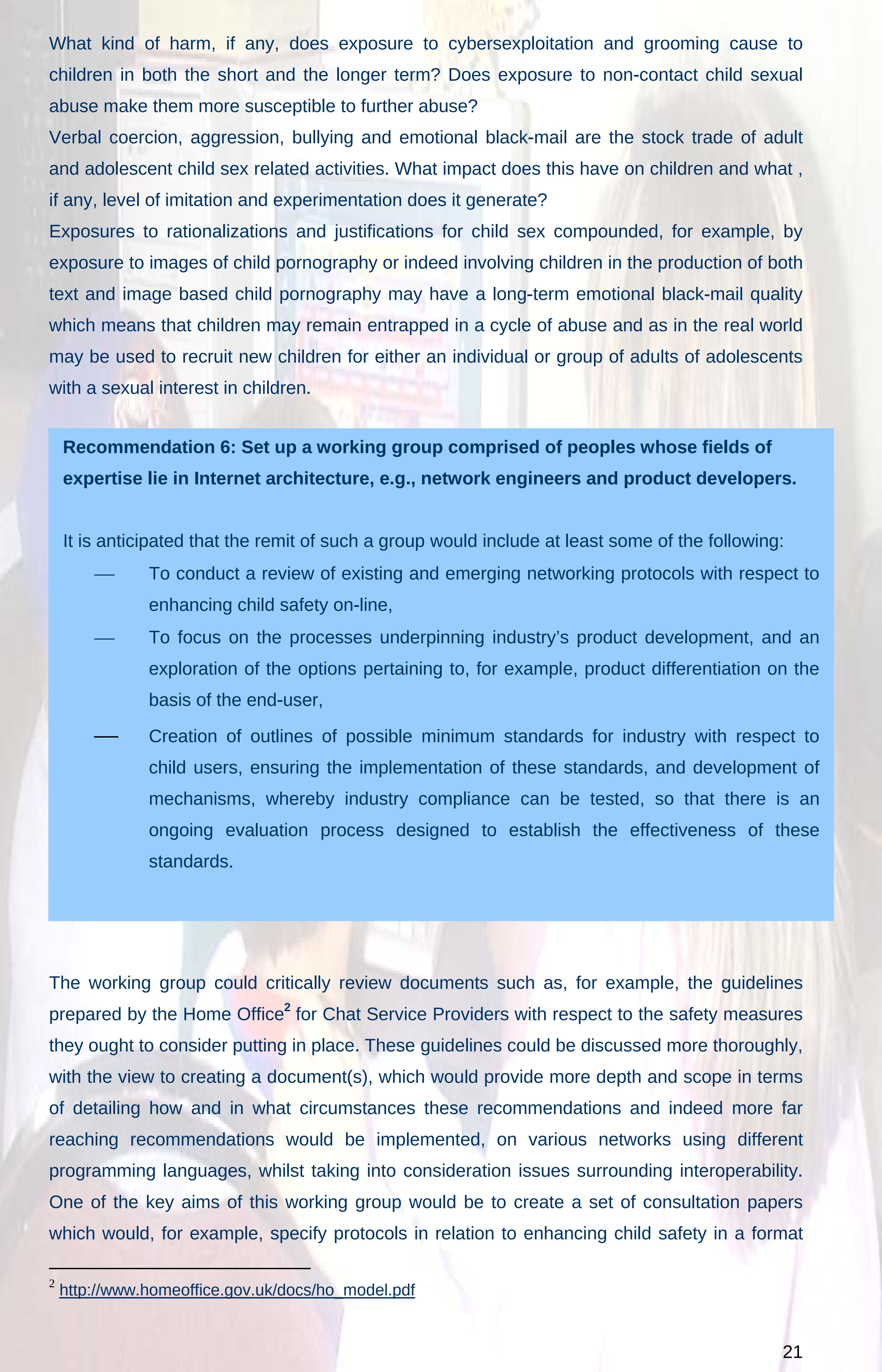
— An exploration of the potential of developing sociolinguistic profiling techniques in



An exploration of the potential of developing sociolinguistic profiling techniques in relation to cybersexploitation and both online and offline grooming.

Identifying strategies within the speech of the adult with a sexual interest in children has the potential to provide information about an alleged offender's modus operandi and signature behaviours, as well as potentially providing indicators of potential risk an individual might pose to intended victims. Therefore analysing conversations in a systematic manner provides the potential to build linguistic profiles of offenders. In addition, comparing the language used to cybersexploit victims, for example, cyber-rape scenarios in on-line contexts with details of assault(s) which subsequently occurred during real-world face-to-face meeting(s), could begin to provide insights into whether or not a cycle of abuse exists that occurs in both real and virtual worlds, or indeed whether some kinds of cybersexploitation scenarios are confined to the virtual world. Such a program of research might begin to answer questions about the relationship between, for example, violent sexual assaults where the original point of contact was on-line and the nature of that contact. Furthermore from a psychological perspective this kind of analysis lends itself to both cross-sectional and longitudinal studies designed to analyse behaviour patterns, career trajectories, and risks associated with on-line offenders. In addition a socio-linguistic profile generated through analysis of on-line conversations may form an important part of an overall offender profile, crucially, the extent of an alleged offenders immersion in a range of both on-line and offline activities including, for example, online child pornography related activities, or interfamilial abuse. A clear recommendation arising out of this research is that both the evidential nature and potential for providing psychological insights into the mindset of adult with a sexual interest in children who engages in cyber sexploitation must not be overlooked.

An exploration of the psychological effects of exposure to cybersexploitation and online grooming on both children and teenagers who have experienced these activities on-line.



What kind of harm, if any, does exposure to cybersexploitation and grooming cause to children in both the short and the longer term? Does exposure to non-contact child sexual abuse make them more susceptible to further abuse?

Verbal coercion, aggression, bullying and emotional black-mail are the stock trade of adult and adolescent child sex related activities. What impact does this have on children and what , if any, level of imitation and experimentation does it generate?

Exposures to rationalizations and justifications for child sex compounded, for example, by exposure to images of child pornography or indeed involving children in the production of both text and image based child pornography may have a long-term emotional black-mail quality which means that children may remain entrapped in a cycle of abuse and as in the real world may be used to recruit new children for either an individual or group of adults of adolescents with a sexual interest in children.

Recommendation 6: Set up a working group comprised of peoples whose fields of expertise lie in Internet architecture, e.g., network engineers and product developers.

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

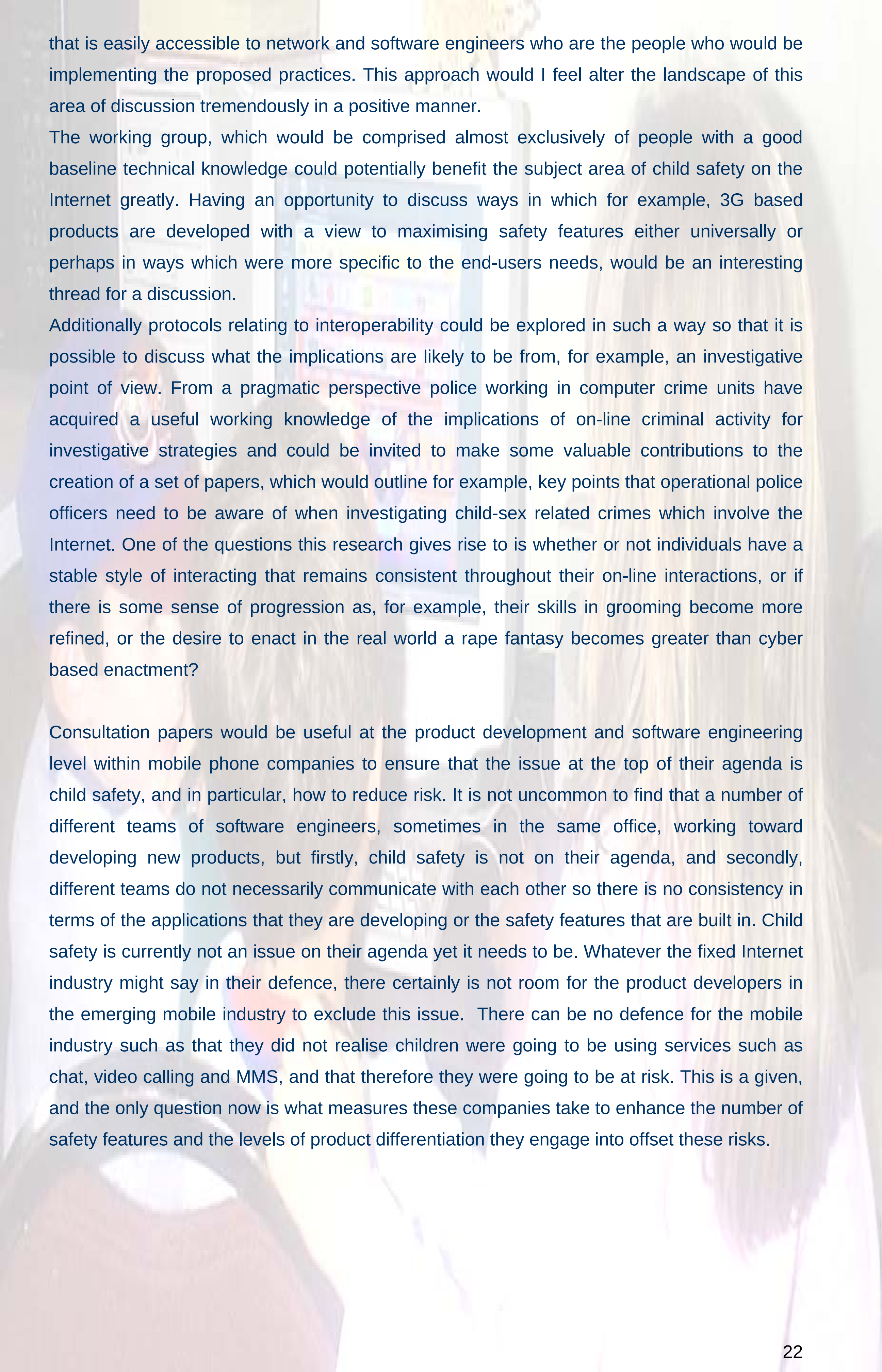
— To conduct a review of existing and emerging networking protocols with respect to enhancing child safety on-line,

— 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.

The working group could critically review documents such as, for example, the guidelines prepared by the Home Office[2] for Chat Service Providers with respect to the safety measures they ought to consider putting in place. These guidelines could be discussed more thoroughly, with the view to creating a document(s), which would provide more depth and scope in terms of detailing how and in what circumstances these recommendations and indeed more far reaching recommendations would be implemented, on various networks using different programming languages, whilst taking into consideration issues surrounding interoperability. One of the key aims of this working group would be to create a set of consultation papers which would, for example, specify protocols in relation to enhancing child safety in a format

[2] http://www.homeoffice.gov.uk/docs/ho_model.pdf



that is easily accessible to network and software engineers who are the people who would be implementing the proposed practices. This approach would I feel alter the landscape of this area of discussion tremendously in a positive manner.

The working group, which would be comprised almost exclusively of people with a good baseline technical knowledge could potentially benefit the subject area of child safety on the Internet greatly. Having an opportunity to discuss ways in which for example, 3G based products are developed with a view to maximising safety features either universally or perhaps in ways which were more specific to the end-users needs, would be an interesting thread for a discussion.

Additionally protocols relating to interoperability could be explored in such a way so that it is possible to discuss what the implications are likely to be from, for example, an investigative point of view. From a pragmatic perspective police working in computer crime units have acquired a useful working knowledge of the implications of on-line criminal activity for investigative strategies and could be invited to make some valuable contributions to the creation of a set of papers, which would outline for example, key points that operational police officers need to be aware of when investigating child-sex related crimes which involve the Internet. One of the questions this research gives rise to is whether or not individuals have a stable style of interacting that remains consistent throughout their on-line interactions, or if there is some sense of progression as, for example, their skills in grooming become more refined, or the desire to enact in the real world a rape fantasy becomes greater than cyber based enactment?

Consultation papers would be useful at the product development and software engineering level within mobile phone companies to ensure that the issue at the top of their agenda is child safety, and in particular, how to reduce risk. It is not uncommon to find that a number of different teams of software engineers, sometimes in the same office, working toward developing new products, but firstly, child safety is not on their agenda, and secondly, different teams do not necessarily communicate with each other so there is no consistency in terms of the applications that they are developing or the safety features that are built in. Child safety is currently not an issue on their agenda yet it needs to be. Whatever the fixed Internet industry might say in their defence, there certainly is not room for the product developers in the emerging mobile industry to exclude this issue. There can be no defence for the mobile industry such as that they did not realise children were going to be using services such as chat, video calling and MMS, and that therefore they were going to be at risk. This is a given, and the only question now is what measures these companies take to enhance the number of safety features and the levels of product differentiation they engage into offset these risks.