Chat Wise, Street Wise – children and Internet chat services

A paper prepared by the Internet Crime Forum IRC sub-group

Executive Summary

The IRC sub-group was formed in June 1999 under the auspices of the Internet Crime Forum (www.internetcrimeforum.org.uk) and includes representatives from industry, law enforcement, child welfare, government, civil liberties and regulatory bodies, with the Internet Watch Foundation in the chair.

The role of the group was to identify and quantify the problems of chat services on the Internet and to consider and evaluate potential means of addressing them. The specific context of these terms of reference was the protection of children using online chat.

For the purposes of the paper, chat is defined as live synchronised communication across the Internet. This generally involves text-based realtime communication on a one-to-many basis. Any individual user with an Internet connection has the potential to access servers running chat software in order to contact other users across the world.

The most common versions of chat are Internet Relay Chat (IRC) which consists of multiple servers connected to each other, and web-based chat, which is run either on dedicated websites or on individual homepages running a chat facility. IRC is not under the control of any one organisation, and uses open standard software, enabling anyone with sufficient knowledge to write and operate an IRC program.

It is impossible to give an accurate figure for the total number of chat facilities available to UK users, but available statistics indicate that it is over 100,000.

Although some chat facilities are offered by ISPs and the major web portals, the majority of web-based chat services are lower-level hosted services set up and run by a wide range of organisations and individuals who are not part of the Internet service provider industry.

It is estimated that around 33% of the UK population are now online and nearly 5 million children are using the Internet. Chat is particularly popular among young users, especially those services provided through the major web portals and on individual websites. It offers the facility for instant and realtime access to people of all ages and backgrounds from across the world, and enables children and adults alike to interact on a level playing field, regardless of many of the social, cultural, religious, geographical or potentially discriminatory obstacles which may inhibit them offline.

However, it is essential to recognise that this facility can also be abused by a criminal minority to make contact with children with a view to establishing and developing a sexual relationship with them in the 'real world'. Such relationships can then be pursued through other media such as instant messaging, email and mobile telephones.

Risk assessment studies have identified the most likely targets of ‘online enticement’ (children being approached and groomed by paedophiles on the Internet) as being teenagers, mainly girls, between the ages of 13 and 17.

The relative scale of the risk of children being approached in this way via the Internet is extremely difficult to establish. Evidence from the United States and the UK, provided by actual incidents and cases as well as from supporting research, does appear to indicate a growth in criminal activity of this nature over recent years. It is also important to note that the number of known cases to date is currently very low in proportion to the rapidly growing rate of Internet use, and that the danger of online solicitation by a stranger is thought to be relatively much lower than offline risk from someone known to the victim.

Nevertheless, the available evidence highlights the paramount importance of recommending some preventative strategies for protecting children, in view of the opportunity for paedophile contact and the potential damage done to children.

UK legislation applies online as well as offline, and a number of existing laws cover offences which might be committed through chat room activity. However, some concern has been raised as to whether or not ‘online enticement’ of a child can be adequately dealt with by current legislation. This issue needs to be considered in the broader context of the comprehensive review of sex offences being undertaken through the “Setting the Boundaries” report. While it is beyond the scope or competence of this document to attempt a thorough critique of the existing legal framework, the various concerns about possible loopholes have been referred to the review team, and this document will be submitted to the “Setting the Boundaries” consultation.

Issues of traceability and anonymity are extremely complex, since tools which can be useful in identifying perpetrators can also be used by adults with a sexual interest in children to identify potential victims. Of particular concern is the need to protect the identity of young users connecting to the Internet through school systems and using school email addresses.

The need for Internet Service Providers to obtain and where necessary retain data on Internet users, in order to investigate misuse, has to be balanced against the requirements of both UK and EU data protection legislation and the technical capabilities. The legislation restricts the type of data which can be logged and the length of time for which it can be stored.

Software is available to users in order to help them protect their own identities and to prevent unwanted content and contact. It is important that parents and other carers are aware of the tools currently available, and that the various sectors of the IT industry continue to research better, cheaper and more user-friendly technical solutions.

Although technology can provide useful tools for helping to create a safer online environment, it should be complemented and underpinned by a range of different types of human intervention.

Moderation (supervision) of chat rooms can be provided in order to ensure that conversation is appropriate to the age range of the participants. It is essential that the recruitment, training and oversight of those appointed as moderators is adequate to ensure that such positions are not abused by those wishing to make inappropriate contact with children.

However, this kind of moderation cannot be relied on to safeguard all chat activity by children, particularly since some children may participate in adult discussions on a whole range of topics rather than limiting their activity to chat rooms designed for their own age group. It is therefore essential that parents and other carers take an interest in and oversee their children's online experience and activity.

Education and awareness are key elements in helping users, and in particular the parents of young users, protect themselves online and get the maximum benefit from the Internet. Awareness materials should be provided by a broad range of agencies, including the government, the computer and Internet industries, self-regulatory bodies such as the Internet Watch Foundation, schools and colleges, children's charities, young people's organisations and the media.

Kitemarks are a recognised and effective tool for increasing consumer confidence in the offline world. The use of some kind of kitemark for chat services would empower parents to choose appropriate services for their children's use.

It is crucial that prompt and effective reporting mechanisms are in place to enable users to report incidents in chat rooms which appear to constitute online enticement. Current research suggests that only about half of such cases are currently reported.

There are currently only a small number of specialist police officers and units equipped to deal with Internet investigations, and there is a need both for increased resources and for better co-ordination on a national and an international scale. The new National Hi-Tech Crime Unit becomes operational in April 2001, and it is essential that its remit is adequate to cover cases threatening the online safety of children.

In response to the issues outlined above and considered in detail in the full paper, a number of recommendations were agreed, and the key safety messages for children's chat room activity were identified.

Ruth Dixon
Deputy Chief Executive
Internet Watch Foundation

Recommendations[1]

(a) Children should use chat services specifically targeted at their own age range which have adequate levels of care and protection as outlined in (c) below.

(b) Relevant UK legislation should be kept under constant and comprehensive review to ensure that it can meet changing circumstances, both online and offline, to protect children from abuse.

(c) The various sectors of the IT industry should continue to research better, cheaper and more user-friendly technical solutions to the potential dangers of chat, including the identification and investigation of improved measures to ensure an appropriate level of traceability.

(d) Providers of chat services specifically aimed at children should provide a responsible standard of care to protect their users. The nature and extent of protective measures should be transparent to all users.

(e) A focussed education and awareness programme should be aimed at parents and other carers to advise them of the potential risks to children using chat services and appropriate steps they can take to protect them.

(f) All Internet Service Providers should provide clear advice to their subscribers about the potential hazards of chat and the simple safety messages (see below) to help avoid them.

(g) Industry, user groups and children's organisations should jointly explore the possibility of introducing a kitemarking scheme which would offer a simple way for parents to identify chat services committed to providing an enhanced standard of care for young users.

(h) A user-friendly reporting mechanism should be available to facilitate the prompt reporting and investigation of incidents in chat rooms.

(i) Law enforcement officers should have specialised training and increased resources to ensure a prompt and effective response to reports of incidents in chat rooms. The new National High-Tech Crime Unit should ensure that online protection of children is and remains a high priority.

[1] The order of these recommendations reflects the sequence in which the supporting issues are considered in the paper.

Safety messages - ‘Chat Wise, Street Wise’

1) Don’t give out personal details, photographs, or any other information that could be used to identify you, such as information about your family, where you live or the school you go to.

2) Don’t take other people at face value – they may not be what they seem.

3) Never arrange to meet someone you’ve only ever previously met on the Internet without first telling your parents, getting their permission and taking a responsible adult with you. The first meeting should always be in a public place.

4) Always stay in the public areas of chat where there are other people around.

5) Don’t open an attachment or downloaded file unless you know and trust the person who has sent it.

6) Never respond directly to anything you find disturbing – save or print it, log off, and tell an adult.

Chat Wise, Street Wise – children and Internet chat services

A paper prepared by the Internet Crime Forum IRC sub-group

Section A:

Introduction

1. The Internet Crime Forum[2] brings together representatives from government, law enforcement and the Internet industry. Its overall aim is "to develop and maintain a working relationship between the Internet Service Providers Industry and Law Enforcement Agencies in the UK, such that criminal investigations are carried out lawfully, quickly and efficiently while protecting the confidentiality of legitimate communications and with minimum impact on the business of the industry". The main forum meets quarterly, and also allocates specific issues for consideration by multi-agency sub-groups between those meetings.

2. The IRC sub-group was formed in June 1999 and includes representatives from the following stakeholders: industry, law enforcement, child welfare, government, civil liberties and regulatory bodies, with the IWF in the chair[3]. The group met eight times between July 1999 and November 2000.

3. The group was set up in response to a recommendation in the DTI/Home Office review of the work of the IWF[4] that government, industry, the police and other interested bodies should be brought together to discuss an approach to dealing with illegal material on chat, as follows:
"We recommend that, just as occurred in 1996 in relation to Web sites and Usenet newsgroups under the Agreement, the same bodies should come together to agree on whether the IWF should deal with illegal material on Chat, and how this can be achieved."

4. The agreed terms of reference of the IRC sub-group were:
   a) to identify and quantify the problems of chat services on the Internet
   b) to consider and evaluate potential means of addressing the problems

5. It should be noted that the specific context of these terms of reference was the protection of children using Internet chat services, rather than general issues of child safety on the Internet.

6. This document seeks to summarise the outcomes of the group's discussions. The recommendations reflect the general consensus reached in the course of extensive discussions, but not all recommendations are necessarily

[2] http://www.internetcrimeforum.org.uk/

[3] For a complete list of the members of the sub-group, please see appendix 1

[4] Review of the Internet Watch Foundation : A report for the Department of Trade and Industry and the Home Office (section 5.2.1.1)

individually endorsed by every member of the group or their nominating organisations. Additionally, some measures proposed by individual members of the group are not reflected in the final recommendations since there was no consensus on their inclusion.

Identifying and quantifying the problems

What is chat?

7. For the purposes of this paper, chat is defined as live synchronised communication across the Internet. Asynchronous message boards are not considered, although it should be noted that much of the safety advice can usefully be applied to these and other areas of the Internet.

8. Chat is generally text-based, realtime communication on a one-to-many basis. An individual user with an Internet connection has the potential to access servers running chat software, and through those servers can communicate with other users. Several different kinds of chat are available, as outlined in the following sections.

9. IRC: Internet Relay Chat (IRC) was originally written by Jarkko Oikarinen in 1988 in Finland and is now in use in over 60 countries around the world. IRC is a multi-user, multi-channel system run on computer networks. It gives users worldwide the facility to hold realtime text 'conversations' with each other, either in groups or privately.

10. IRC is not owned or run by any single organisation. IRC networks consist of multiple servers which connect to each other. There are several large independent IRC networks such as Efnet, IRCnet, Undernet, Overnet and DALnet. Although some IRC servers are run by Internet Service Providers the majority are not - of a list of nearly 400 servers visible on IRC on 15 October 2000, only 10 appeared to be located in the UK, of which just half were run by UK ISPs. Additionally, any individual with sufficient knowledge can set up an IRC server for relatively modest financial outlay – currently just the price of a PC and about £1500 per annum for the hosting costs. These servers can be independent of the main networks, and therefore the overall nature of IRC is extremely fragmented.

11. IRC uses open standard software available for anyone to use to write a program. Although a number of commercial companies produce IRC software, programming of IRC programs is relatively simple, and would be well within the capabilities of most computer science undergraduates. Many software packages can be downloaded at no cost from the Internet as shareware or freeware. It is therefore important to remember that any protective measures discussed below will require a high degree of cooperation not only from the commercial software development community but also from individual developers who produce simple software for no financial gain.

12. Channels on IRC are dynamic in the sense that anyone can create a new one - a channel is automatically created as soon as the first person joins it and it

disappears as soon as the last person leaves it. Channels are public by default, although they can be set up in such a way as to allow only invited participants or to be entirely hidden from public view. Each channel is run by a channel operator – this status is automatically given to the first person to join the channel – and this operator can confer the same status on other specified users. The channel operator can expel other users from the channel.

13. Users can talk to other users on the same server and on other servers on the same IRC network. There is no restriction on the number of people who can taken part in a channel discussion, nor on the number of channels that can be formed on IRC. Every IRC user has his or her own nickname, and communicates with other users either on a public channel - often referred to as a 'chat room' – or in a private conversation. Users can invite each other to talk privately either parallel to or instead of participating in the public chat.

14. The dynamic nature of IRC means that it is impossible to give an accurate figure for the number of servers or channels available at any one time. One website estimates that there are currently 147999 users on 37750 channels on 27 networks[5]. Another recent sample indicated that on the night of Sunday 8 October 2000 IRCNet had 28527 channels with 63575 users on 53 servers worldwide, and Efnet had 22203 channels with 51159 users on 34 servers worldwide.

15. Web-based chat: Web chat can be run either on dedicated chat websites or on individual homepages running a chat facility. These can generally be accessed through the usual browser without the need to install any special software. These services often have a particular target audience defined by age and/or topic.

16. Although some chat facilities are offered by ISPs and by the major web-portals the majority are lower level hosted services set up and run by a wide range of organisations and individuals who are not part of the Internet service provider industry.

17. It is impossible to quantify precisely the availability of web-based chat services on the Internet. Chat scripts are often used by content providers to attract users to their websites, and thousands of websites were identified through UK search engine queries on "+chat +room". A wide range of free software programs can be downloaded directly from the Internet for setting up chat facilities

18. MUD/MUSH: MUD (Multi-User Dimension) and MUSH (Multi-User Simulated – or Shared - Hallucination) programs are online, real-time, interactive, text-based virtual environments which were originally developed for role-playing games such as Dungeons and Dragons. They are run over computer networks, and the hosting servers are accessed via the telnet protocol or by means of specialist client programs. Most can be freely accessed at no cost to the user.

[5] http://www.liszt.com/chat/report.html

19. Although many MUSHes are games based around a theme derived from popular fiction or role-playing games, they are ideally suited to chat, since they offer the opportunity to interact in realtime with other users from around the world. They also enable the participants to create a total interactive environment within which to operate.

20. MUDs and MUSHes offer benefits in encouraging social interaction, creativity, and the development of problem-solving skills. However, it is also important to recognise the particular potential for children to be manipulated within role-playing scenarios.

21. Instant Messaging: this is an extremely popular form of realtime text-based communication over the Internet. Although it is essentially one-to-one, it can develop into a form of private chat room as users invite others to join in their 'conversation'. Generally only people known to each other can make contact, although many versions of instant messaging set up 'affinity' groups on the basis of information entered by users into their 'profiles', enabling them to get in touch with others sharing common interests. In addition, some instant messaging services provide a direct link to public chat areas, and the distinction may not always be clear to the user. Some instant messaging systems allow file-sharing. One of the most popular forms of instant messaging is ICQ, which allows users to see when their friends are online and to communicate with them in realtime.

22. Like chat, instant messaging is run on open standard software which can easily be programmed. Some facilities are offered through major ISPs and web-portals, but many others are also available via freeware or shareware downloads.

Internet growth

23. The number of Internet users worldwide has increased from an estimated 37 million in December 1996 to over 407 million in November 2000. Over a similar period the online population in the United Kingdom has grown from under 1 million in June 1997 (approximately 2% of the population) to nearly 20 million at the end of 2000, representing 33% of the total population[6].

24. The volume of content on the Internet has grown at an exponential rate during the same period. By way of illustration, there were approximately 9.5 million web hosts[7] in January 1996, whereas by January 2001 an estimated 106 million hosts were online[8].

Children and chat

25. There are now an estimated 4.8 million children online in the United Kingdom (more than double the number two years ago), of whom over 1 million are

[6] http://www.nua.ie/surveys/how_many_online/
[7] http://www.mit.edu/people/mkgray/net/internet-growth-raw-data.html
[8] http://www.netsizer.com/

under 14[9]. 65% of all 7 to 16 year olds in the UK have used the Web and are frequent users of email to communicate with friends, family and virtual friends. 62% of these use the Internet at home, and in addition 81% of all young users have access from school. Chat rooms are popular with 23% of children, with the highest user group being the 15 to 16 year olds, of whom 41% use chat services.

26. Internet Relay Chat is far less popular with teenagers, particularly girls, than chat services provided by portals such as Yahoo!, MSN and Excite or on individual websites. This is significant in so far as these services are owned and managed by identifiable companies or individuals who may have some powers to intervene if their services are abused.

27. There is a general trend towards girls using the Internet primarily as a communication tool whereas boys appear to view it more as an information source.

28. The image of the Internet user has changed radically over the last 18 months - according to an NOP survey published in 2000, Internet users are no longer regarded as 'geeky, strange or stupid' but are seen by their peers as 'clever, cool, fun and trendy'.[10]

29. Online chatting is one of the main attractions for this growing and increasingly sophisticated group of young users. It gives them the chance to talk to existing friends and to meet new ones at the click of a mouse. Recent research by media magazine Campaign Magazine found that teenage users spend an average 191.2 minutes a month on one instant messaging service alone[11].

30. It is important to acknowledge and affirm the positive value of chat and of many of the friendships and relationships developed via the Internet. Contrary to a common perception of the Internet as essentially a solitary and desocialising medium, in which the user's only contact is with a screen, chat is an inherently social activity.

31. The public and private benefits of this socially inclusive and interactive communication tool should not be under-estimated. There are undoubted benefits in being able to communicate directly with people from around the world. Instant and real time access to people of all ages and backgrounds means that common interests can be discussed, horizons can be broadened, and tolerance increased between both individuals and communities. Children and adults alike can enjoy the opportunity to interact on a level playing field, regardless of many of the social, cultural, religious, geographical or potentially discriminatory obstacles which may inhibit them offline. Mutual support systems can be developed for those who may be vulnerable and lacking offline support. In addition, immediate global communication can offer a tool for disseminating information which might otherwise be suppressed, for example

[9] http://www.readersdigest.co.uk/magazine/EWIS-4QFFMU.htm

[10] http://www.nop.co.uk/

[11] Source: http://www.zdnet.co.uk/news/2000/44/ns-18968.html

under oppressive regimes or in war zones. In this context the value of online anonymity – properly used and protected – should also be recognised.

Online risk

32. While the Internet offers unprecedented opportunities for communication and creative expression to millions of legitimate users across the world, it can also be a powerful new tool in the hands of a criminal minority.   A particular danger that has been identified consists in the possibility of children being approached online by adults or adolescents with the aim of developing a sexual relationship with them in the 'real world'. In some cases this activity may involve the assumption of a false identity, in particular the pretence of being a child. Other risks which may or may not form part of this process can include the following:

- Children being exposed to inappropriate conversation ;
- Children unwittingly becoming the subject of sexual fantasy;
- Children being sent indecent or obscene images;
- Children being asked to send indecent images of themselves and/or their friends;
- Children being engaged in explicit sexual talk and and/or being encouraged to perform sexual acts on themselves and/or their friends (so-called 'cybersex').

33. In assessing the possible risks faced by children and young people through online activity it is important to make the following distinction. Some of the risks faced by children and young people through Internet activity may result from and/or in criminal activity, whereas others may not involve conduct or situations which are against the law but nevertheless may cause varying degrees of concern to parents. The former fall within the remit of the criminal law and invite a public policy response, while the latter are issues properly dealt with by parents and other carers.

34. Nevertheless, it is essential in all instances for carers and children alike to be aware of the potential risks and to be empowered to protect themselves, and it is crucial to ensure that the available protective measures are adequate, whether they be statutory, technical or educational.

35. It is important to understand how preferential child molesters operate in the offline world in order to predict how they might approach children online. Expert opinion from both the United Kingdom and the United States[12]on the behaviour of preferential child molesters (those whose sexual preference is for children and who have well-developed techniques for obtaining victims) identifies a range of common behavioural characteristics and techniques, including the following:

- Skilled at identifying vulnerable victims
- Have or will gain access to children
- Identify with children better than with adults

[12] Child Molesters: A Behavioral Analysis (December 1992) – National Center for Missing and Exploited Children

- Have hobbies and interests appealing to children
- Engage in activities with children, often excluding other adults
- Seduce with attention, affection and gifts
- Skilled at manipulating children

36. Although these elements have been identified from offline behaviour, recent cases of online enticement of children do illustrate the way in which these techniques can be transferred to the Internet environment. Adults seeking sexual contact with children are likely to target those areas of the Internet where children are likely to be found, to identify potential victims from among the participants, and to use seductive and manipulative methods to approach them. Such activity has also taken place through email and websites, as illustrated in the cases in paragraph 45 below. However, the realtime nature of chat offers particular opportunities for direct and immediate contact, with the added facility to persuade the child to go off into a private conversation. The pattern of known cases tends to be that the relationship is initiated in a chat room and is then continued through instant messaging, email and telephone (often mobile) contact.

37. Although the general issue of pornography, whether involving adults or children, is beyond the scope of this document, it is important to note that a further technique employed in 'grooming' potential victims is the use of sexually explicit material. A 1997 report by Sir William Utting highlights this point: "It [pornography] is shown to children to lower their inhibitions – the children involved have always been forced to smile so that it can be claimed, especially to younger children, that they are having fun. With older children it is used to excite them and to show them that what is being done is 'alright'. It is also used to entrap children further – because of fear that others will see what they have done and because of the upset it would cause their parents. "[13] This exchange of images can be two-way – at some stage in an Internet relationship a child might be asked for sexually explicit photographs of him or herself and/or their friends. This in turn potentially increases the perpetrator's hold over the child and can be used to coerce him or her into further illegal acts.

38. It should be noted that children can be at risk from other children and adolescents as well as from adults. A Home Office research paper published in December 1998 indicates that adolescent sex offenders probably account for up to a third of all sex crime.[14] US statistics indicate that nearly half of all online solicitation cases involve juvenile perpetrators.[15]

39. The relative scale of the risk of children being approached for sexual purposes via the Internet compared with the offline environment is extremely difficult to establish. However, some data is available on general trends in cases of

[13] People Like Us: The Report Of The Review Of The Safeguards For Children Living Away From Home (November 1997) – Stationery Office

[14] Sex Offending Against Children – Understanding the Risk http://www.homeoffice.gov.uk/prgpubs/prg99bf.pdf

[15] "Online Victimisation: A Report on the Nation's Youth"- National Center for Missing and Exploited Children (June 2000) p.3

child sexual abuse. A Home Office report in December 1998 indicated that about 80% of perpetrators assault children known to them, with these offences taking place in the home of either the offender or the victim. The vast majority of sex offenders against children typically offend alone rather than in networks or 'rings'[16]. Another study prepared for the Home Office by the Law Department at Bristol University looked at 94 cases involving 124 complainants[17]. All but one of the complainants knew their alleged abusers, of whom 48% were family members or relations, 20% were family friends or neighbours, 15% were professionals (youth workers, teachers, doctors), 10% were temporary carers and 6% were acquaintances. In just one case the complainant alleged abuse by a stranger. In view of this reality, it is essential that children are taught – and constantly reminded as they use chat rooms – that online 'friends' are in fact actually 'strangers', regardless of the length of time they have 'known' each other.

Quantifying the risk

40. In order to design appropriate responses to the issue of online risk, it is important to take account both of recent cases and of supporting research about children's online behaviour and attitudes.

Examples from the UK

41. It is extremely difficult to make any accurate assessment of the level of sexual approaches to children in chat rooms in the UK, since uniform crime figures do not record any distinction between online and offline cases. In order to make an accurate estimate of the extent of the problem of children being the target of sexually inappropriate approaches on the Internet, it would be helpful to categorise crime reporting figures in this way. In addition, reports of incidents which do not lead to criminal charges are not recorded, whether they take place in a children's playground or on the Internet.

42. However, a number of cases and incidents have occurred in the UK, some of which have led to criminal proceedings.

43. In May 2000 a 33 year old man was charged with 14 offences under the Sexual Offences Act and the Child Abduction Act after meeting a 13 year old girl in a chat room. He communicated with the girl via email and mobile phone, and eventually sexually abused and raped her. He also sent indecent images of himself to his victim. While on bail the man was arrested on his way to meet another girl, aged 14, whom he had also befriended through a chat room. He was convicted in September 2000 and sentenced the following month to a five-year prison sentence on four counts of unlawful sexual intercourse. His name was added to the Sex Offenders Register for life[18].

[16] Sex Offending Against Children – Understanding the Risk
http://www.homeoffice.gov.uk/prgpubs/prg99bf.pdf

[17] An Assessment of the Admissibility and Sufficiency of Evidence in Child Abuse Prosecutions
http://www.homeoffice.gov.uk/rds/pdfs/occ-childabuse.pdf

[18] Daily Telegraph 25.10.00

44. A convicted paedophile from Newcastle was arrested in 1999 after a tip-off when he flew to the United States to meet a 15 year old girl he had befriended in a chat room.

45. Other cases have originated through other areas of the Internet. In February 2000 a 53 year old man admitted four counts of indecent assault and was found guilty on two counts of serious sexual assault on a 13 year old boy who asked him for help via a gay counselling web site. He was jailed for five years.

46. California police found evidence of a 28 year old Briton looking for young girls through a paedophile website, and the details were passed to New Scotland Yard, who arrested a man after their own undercover operation. In May 2000 he was acquitted of the charges of procurement and of attempted sexual intercourse with a girl under 13. At the same hearing the defendant was sentenced to 18 months in prison and his name was added to the Sex Offenders Register for distribution of indecent images of children and for attempting to incite another to procure a girl for sex.

47. Other recent incidents which did not result in any criminal proceedings nevertheless illustrate the potential problems of allowing online contact to lead to an offline meeting. In April 2000 a 13 year old girl arranged a meeting with her online 'boyfriend' whom she had first met in an Internet chat room. Her mother went with her to that meeting, and discovered that the '18 year old' with whom her daughter had become friends was in fact a 47 year old man. He was arrested, but was released without charge. The IWF has received a report of another similar incident which was investigated recently by police in the North East of England. This involved a 13 year old girl who had met someone claiming to be a 15 year old boy in an Internet chat room. After numerous mobile phone calls and text messages, in the course of which the 'boy' said he was in fact 27, a meeting was arranged. At this point the police were alerted, and were waiting for him when he turned up to meet the girl. A 38 year old man was released without charge.

48. In January and February 2001 the press highlighted two separate chat-related incidents, when two schoolgirls[19] left home, apparently to meet people they had been in contact with on Internet chat rooms. Whilst no criminal investigations resulted from these incidents, and both girls returned home safely after a few days, they did heighten public awareness of chat room issues.

Examples from the US

49. In the United States there has been a growth in reports of child exploitation on the Internet over the past five years. The FBI's Innocent Images initiative has seen a growth in convictions from 13 in 1995 to 214 in 2000. The total number of convictions between 1995 and 2000 was 740. Approximately one

[19] The Times 10.02.01 and Daily Telegraph 19.02.01

quarter of these relate to so-called 'traveler' (online enticement of children) cases while the rest involve child pornography or 'trader' offences.[20]

50. Other federal and state law enforcement agencies also deal with cases of child exploitation online, notably the US Postal Inspection Service and the US Customs CyberSmuggling Center. The USPIS reports[21] that the Internet is increasingly used as a tool in exploiting children, particularly in the context of child pornography: during 1997 just 33% of cases involved the use of computers, whereas this figure had risen to 77% by the year 2000. The available data also indicates that since 1997 36% of offenders caught by the USPIS were identified as having committed actual sexual abuse of children.

51. The CyberTipline in the US[22], which handles reports of child sexual exploitation online, has received 3,174 reports alleging online enticement of children since its launch in March 1998. The number of specific reports of chat room incidents has grown from 82 in 1998 to 102 in the first ten months of 2000.

52. One of the earliest and most well-known cases in the US is that of Katherine Tarbox, whose book 'Katie.com' details her experiences. In 1995 Katie met 23 year old "Mark" in a teen chat room. After developing their relationship through the Internet and on the telephone they arranged to meet. "Mark" turned out to be a 41 year old man[23]. He sexually assaulted her, and was subsequently sentenced in March 1998 to 18 months in prison. His was one of the first cases prosecuted under the Communications Decency Act of 1996, a federal law that prohibits adults from using the Internet to entice a minor into sex.

Surveys

53. The Reader's Digest/MORI survey, "Children & the Internet", was conducted with 2,000 adults (aged 15 plus) across Great Britain in June 2000[24]. It indicated that half of the respondents worry about their children accessing violent or sexually explicit material, and 43% are concerned about who their children might meet through chat rooms. Consequently, a similar proportion feels it is necessary to supervise their children while they are online, and over 80% of their children are accessing the Internet in a shared room rather than in their own bedroom.

54. Paradoxically, because of parents' worries about 'real world' stranger danger and road safety, many of them have felt much more comfortable with their children staying indoors to use computers and the Internet, believing that because this is taking place in the family home it is somehow intrinsically a safer environment. However the third wave of the NOP kids.net[25] survey

[20] A list of sample cases is available online at http://www.usdoj.gov/criminal/ceos/inves_prosec.htm
[21] Data provided by Inspector Ray Smith
[22] http://www.missingkids.com
[23] Francis Kufrovich
[24] http://www.readersdigest.co.uk/magazine/EWIS-4QFFMU.htm
[25] http://www.nop.co.uk

revealed that 29% of the 2000 children interviewed would be willing to give out their home address on the Internet, and 14% would give out their email address. This highlights the possibility that children and young people may in fact be at particular risk on the Internet because they are often accessing it from a familiar environment perceived as safe and secure, primarily at home. This can instil a false sense of security which may in turn lead to the child communicating more openly than they might do usually, or entering into a relationship which is more intimate than they would feel comfortable with in the 'real' world. It is significant that some 70% of the online approaches described in the NCMEC Online Victimisation report occurred when the children were in their own home[26].

55. Similar research from the US can provide useful supporting information for our discussions in the UK. Risk assessment studies have identified the most likely targets and victims of 'online enticement' (children being approached and groomed by paedophiles on the Internet) as being teenagers, mainly girls, between the ages of 13 and 17, ie older than the target age range for offline approaches.

56. A telephone survey published by the Crimes Against Children Research Center of the University of New Hampshire[27] interviewed 1501 young people aged 10 to 17 about their Internet experiences. Just under one in five claimed to have received some kind of sexual solicitation on the Internet within the previous twelve months. For the purposes of the survey, 'sexual solicitations' are defined as " requests to engage in sexual activities or sexual talk or give personal sexual information that were unwanted or, whether wanted or not, made by an adult." Although one in fifty was asked to meet in person, one in five hundred children received such a request from an adult over 25. 65% of the incidents occurred in chat rooms, and a further 24% through instant messaging. 70% of them affected children between the ages of 14 and 17, rather than the younger end of the age scale.

57. It should be stated that in almost all the cases the identifying information cannot be verified. However, based on the information provided by the participants, it appears that almost half of these approaches were made by other minors, while adults aged 18 to 25 were responsible for most of the rest. About 5% of the reported incidents were initiated by adults over 25.

58. No information is available on the difference in age between the adult - or other child - making the approach and the recipient. This is a significant factor since it may be necessary to distinguish between incidents between children or young adults of a similar age, and those involving a larger age gap, and therefore likely to present greater cause for concern.

Assessing the risk

[26] "Online Victimisation: A Report on the Nation's Youth"- National Center for Missing and Exploited Children (June 2000)

[27] ibid.

59. In the UK the number of instances to date of preferential child molesters making contact with children through chat rooms is currently very low in proportion to the rapidly growing rate of Internet use. In addition, online risk of sexual solicitation by a stranger is relatively much lower than offline risk from someone known to the victim.

60. Nevertheless, the evidence presented above does highlight the paramount importance of recommending some preventative strategies for protecting children. The statistics from the US indicate a growth in criminal activity of this nature over recent years, and the incidents cited illustrate both the opportunity for paedophile contact and the potential damage done to a child victim. It is imperative that timely steps are taken to protect others from being exposed to the risk of similar abuse.

61. The following section therefore considers a range of possible legislative, technical and human measures which could contribute to providing an enhanced level of care and protection for young users of Internet chat services. It should be noted that in a number of areas the proposed solutions in themselves may create additional vulnerabilities and therefore constitute additional risks. Implementation is therefore likely to be complex and to require further dialogue and, in some cases, ongoing technical development.

Legislative solutions

Current legislation

62. There are a number of existing laws which can be used to cover offences committed through chat room activity consisting of or directed towards inappropriate sexual communication or contact with a child. These include: the Obscene Publications Act 1959; the Protection of Children Act 1978; the Criminal Justice Act 1984; the Indecency with Children Act 1960; the Child Abduction Act 1984; the Sexual Offences Act 1956; the Sexual Offences (Conspiracy and Incitement) Act 1996; the Criminal Justice (Terrorism and Conspiracy) Act 1998; the Telecommunications Act 1984; the Protection From Harassment Act 1997 and the Malicious Communications Act 1988.

63. The criminal law can also deal with inchoate crimes such as conspiring, attempting, abetting, counselling, procuring, soliciting or inciting any of the offences covered by the legislation mentioned above. Actions which could take place through the use of chat services with the intention of enticing a child into an offline sexual relationship are potentially covered under such offences. However, it must be remembered that any such actions have to be 'more than merely preparatory' to committing a crime in order to constitute inchoate offences. It should be noted that the application of conspiracy to online enticement of children is unlikely, since the Criminal Law Act 1977 states that a person shall not be guilty of conspiracy to commit any offence if the only other person with whom he agrees is a person under the age of criminal responsibility. Additionally, a victim cannot be the only other party to a conspiracy (Regina v. Tyrell 1894).

64. The Obscene Publications Act, Protection of Children Act, Criminal Justice Act, Telecommunications Act and Malicious Communications Act can be applied to the sending of obscene or distressing communications to a minor.

65. The offline offences which might be initiated through chat room contact could potentially be dealt with under the Indecency with Children Act, Sexual Offences Act, Child Abduction Act, Sexual Offences (Conspiracy and Incitement) Act and Criminal Justice (Terrorism and Conspiracy) Act, depending on the exact circumstances.

66. In this context it is worth noting that section 39 of the Criminal Justice and Court Services Act 2000 (implemented on 11 January 2001) raised the age of the child against whom the offence of indecent conduct towards a young child (section1(1) of the Indecency with Children Act 1960) could be committed from under 14 to under 16. This fills a small but significant previous gap in the criminal law in dealing with conduct initiated in chatrooms. In particular, the offence includes the element of 'incitement' to a child to commit an act of indecency, which could be particularly useful in the chatroom context. Some of the previous difficulties in tackling this area may have arisen from the previous age limitation on the offence.

67. The possible use of sex offender orders may also be useful in this context. These can only be used against a convicted or cautioned sex offender. However if a sex offender were to enter a chatroom and engage a child in what might otherwise appear ostensibly innocent conversation, the police could apply to the court for an order against him if he was acting in such a way as gave them reasonable cause for concern that the public was at risk of serious harm from him. The provisions are contained in sections 2-4 of the Crime and Disorder Act 1998. An order could contain prohibitions such as forbidding him or her to enter chatrooms - the criteria for the prohibitions is that they are necessary to protect the public from serious harm from the defendant. The order is a civil order but breach is a criminal offence with a maximum penalty of 5 years in prison, unlimited fine, or both.

Proposed changes to current legislation

68. A major concern raised in connection with recent UK instances of online enticement has been the question of whether or not legislation is effective to deal with such incidents, or at least their online elements, and there has been some pressure for the law to be amended accordingly.

69. In 1999 the government initiated a comprehensive sex offences review of substantive sex offences known as “Setting the Boundaries”. Its terms of reference were “to review the sex offences in the common and statute law of England and Wales, and make recommendations that will:

- Provide coherent and clear sex offences which protect individuals, especially children and the more vulnerable, from abuse and exploitation;
- Enable abusers to be adequately punished; and
- Be fair and non-discriminatory in accordance with the ECHR and Human Rights Act.”

- 70. The review team published their report in July 2000[28]. The "Setting the Boundaries" paper, which is open for public consultation until March 2001, makes a wide range of recommendations, of which two are of particular interest to this document. Recommendation 19 states that "There should be an offence of adult (over 18) sexual abuse of a child (under 16). The offence would cover all sexual behaviour that was wrong because it involved a child". This would effectively remove the gender distinctions inherent in much of the previous legislation.

71. "Setting the Boundaries" also supports the proposed introduction of abuse of trust offences for adults who are in certain positions of trust or authority over a child, as proposed by the Sexual Offences (Amendment) Bill introduced in February 2000. As outlined in the Bill this would cover chiefly residential institutions and educational establishments (section 5)[29].

72. There is some concern that in this area the law is too reactive to events rather than anticipating them. A specific proposal has been made that it should be possible to criminalise the intent rather than the positive actions of the suspect. In particular, US federal[30]and state[31] law has been cited as an example of proceeding against a suspect on the basis of criminal intent rather than or even in the absence of a criminal act[32]. A possible new offence was suggested, namely "culpable misrepresentation to a minor" – this would consist in an adult misrepresenting himself to a child, typically but not exclusively in relation to his age, with a view to securing a physical meeting. This would give the police greater powers to act preventatively instead of having to wait for the actual offence to be committed. In response, the view has been expressed that such activity may already be covered by the existing law, since it is already an offence to attempt to incite a child to an act of gross indecency or breach the provisions of the Child Abduction Act 1984. In addition, considerable caution has been expressed in view of the general principle in English law that the criminal law should only be applied when a criminal act has taken place. Any proposal to breach this principle should be considered with extreme caution.

73. In 1980 the Law Commission[33] considered the issue of Preparatory Acts and concluded that it would be inappropriate to criminalise acts which are merely preparatory to a criminal offence. Any movement in this direction would therefore represent a significant departure from the principles previously applied in framing the criminal law.

74. The sub-group had a very productive meeting with the "Setting The Boundaries" review team in January 2001 to explore further the extent to which the existing legislative framework is adequate to deal with potential

[28] http://www.homeoffice.gov.uk/cpd/sou/set_summ.pdf
[29] http://www.publications.parliament.uk/pa/ld199900/ldbills/128/2000128.htm
[30] Title 18 s.2241c of the US Code
[31] Title 17 s.259 of the Maine Criminal Code
[32] Children, Chat rooms and the Law Alisdair Gillespie, University of Teeside
[33] http://www.lawcom.gov.uk

offences against children in chat rooms.

75. It is beyond the scope and the competence of this document to attempt a critique of existing legislation or to recommend changes. It is proposed that the “Chat Wise, Street Wise” document be submitted to the “Setting the Boundaries” team as part of the consultative process to inform the wider legislative review process. As part of its submission to the “Setting the Boundaries” review, the Sub Group will be recommending that all of the UK laws and rules of evidence which touch on Internet related issues should be continually and comprehensively reviewed to ensure that they are adequate to protect children (see Section B below).

Technical approaches

Traceability

76. Whilst anonymity can serve a useful purpose in a number of contexts on the Internet, including the protection of children’s own privacy and identity, it is important to address the abuse of anonymity for posting illegal content or making inappropriate contact, as well as for other computer misuse offences. A draft Best Current Practice paper by the London Internet Exchange (LINX) highlights the importance of preserving the right to anonymity for vulnerable users such as persecuted minorities and victims of abuse. However, it stresses that “anonymity should be explicitly supported by relevant tools, rather than being present as a blanket status quo, open to use and misuse.”[34] It also makes the distinction between ensuring that activity on the Internet can be traced back to the person responsible and the routine monitoring of online activity: “the only purpose of traceability is to allow misuse, once detected, to be rooted out.”[35]

77. Determining the source of Internet content can be done through:
1. identifying the machine
2. identifying the user.

78. The following tools can be used to identify and locate the machine by interrogating the various registry databases:
- IP address: however, shared IP addresses and dialup access with dynamically assigned IP addresses mean that it may not always be possible to identify an individual machine definitively.
- Reverse DNS: some Internet applications may refuse incoming connections where there is no reverse DNS entry (ie where IP addresses are mapped to domain names, rather than vice versa, using the IP address written in reverse order), or where the forward and reverse lookups do not match.
- For example, one of the most popular IRC programs (mIRC) will not allow private chats (so-called DCC – Direct Client to Client) to be initiated without valid IP addresses.

[34] http://www.linx.net/noncore/bcp/traceability-bcp.html
[35] ibid

79. The following methods can be used to identify users:

- Name and address
- Credit card check
- Telephone call back
- CLI (caller line identification): currently only about 80% of users are able to provide this for a variety of reasons: the rest may be using non-BT systems where the CLI is lost at the boundary; they may originate through office systems that suppress it; they may come from reseller operations which have generic rather than individual CLI; or they may originate overseas. ISPs are not able to access the more reliable and comprehensive engineering CLI system used to map calls between carriers. This is currently available only to telecoms providers, and although discussions are underway to explore the possibility of extending this to ISPs, the general principle applies that data can only be collected if it is necessary for a specific task, and that if one identifier is already available to fulfil that function it is not possible to collect others.
- Client certificates: the LINX documents suggest that digital certificates linking each user with an identifiable individual may provide traceability in the future. However, this is not yet viable, since few people have the software, and even fewer can operate it, and additionally a range of issues such as cost, reliability and the legislative framework have yet to be resolved.

80. Particular issues are raised by the availability of 'free' Internet services and anonymous access. The LINX Traceability document recommends that it is Best Practice to avoid truly anonymous accounts and to ensure that even for trial accounts some offline information is known about users and that each user has an identifiable account with its own password. It is still important that 'free' services have mechanisms for ensuring traceability, perhaps through the use of CLI or through another existing relationship with the same user. However, this issue needs to be considered in the context of the EC Data Protection Directive, which only allows communications data to be stored for business purposes, generally associated with billing requirements – strictly speaking 'free' providers therefore have no need and therefore no right to retain any such data, even for a very short period. A recent survey[36] suggests that 89% of home users in the UK are now accessing the Internet through 'free' ISPs. Few measures are in place to confirm the identity of users of such services or to ensure that they are over 18, although some ISPs will only allow users to post to the Internet if they provide their CLI.

81. With regard specifically to chat, the LINX paper highlights the fact that the IRC networks have developed with a culture in which the privacy of users is paramount. If this privacy were negated by actions on a particular "relay" (server) then it is likely that its future participation in the network would be restricted or denied. If all UK servers were to implement measures seen as contrary to this culture of privacy, then the UK could be cut off from the global IRC networks. However, an increasing number of IRC servers do

[36] http://www.ispreview.co.uk/

require users to be identified in some way and will disconnect them if they are not identified, usually by means of an Ident server.

82. IRC server software often provides users with the facility to make themselves largely invisible to server operators and limits the ability of those operators and other users to join channels which those users are running as ‘operators’ themselves. So there are both social and technical reasons why institutions operating a server within an IRC network will be unable to monitor users on their systems.

83. However, it is considered acceptable to log some information on IRC servers, namely:

- The machine from which the user connected to the server
- The time a user connected to the server
- The length of time the user remained connected to the server

84. The value of this kind of logging is limited by the fact that that when using IRC the users are know by "nicknames" and often also move between channels. Abuse will therefore be reported in terms of the user’s nickname alone, or the activity on a particular channel at a specific time.

85. The LINX Best Practice document recommends that the following extra information needs to be logged in order to provide optimum traceability:

- The time at which the user joins and leaves each forum.
- Any times at which the user changes nickname, and to what nickname.

86. The issue of traceability raises the dilemma that ideally potential victims need to be untraceable in the real world, while those who would harm them ought to be traceable. It is important to teach potential victims – in this case particularly children – to protect their identities as far as possible, and not to give out any information online which could put them at risk in the offline world. There is concern about the policy of giving school children identifiable email addresses through their schools – in a parliamentary answer in November 2000[37] Michael Wills indicated that the majority of schools are now online and that almost all have been allocated a standard domain name <school name>.<geographical area>. sch.uk. If the individual children’s names are prefixed to create email addresses, this would possibly give away their age, gender and location. He also stressed that it is the duty of individual schools to ensure that every child is safe and that no individual child should be identifiable or contactable.

87. Careful thought must be given to protecting the identities of children whilst still giving the broadest possible access to the benefits offered by the Internet. One possibility may consist in adding a layer of complexity to the email MX records in order to map ‘anonymous’ email addresses to standard addresses of the kind outlined in the answer above. There is a range of technical means already employed by educational network suppliers to offer safeguards,

[37] http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmhansrd/cm001122/text/01122w16.htm#01122w16.html_wqn0

including optionally logging emails, giving teachers and administrators extensive facilities for limiting send and receive addresses, and allowing capture of emails that contain specific words, either in the mail body or attachment. In addition, some specialist educational ISPs allow schools to turn off IRC at the school feed.

88. According to the original SafetyNet agreement which formed the basis for the role and operation of the Internet Watch Foundation, IWF would "sponsor research and development into ways of improving the detection, traceability and removal of illegal material on the Internet."[38] The agreement also recommended that service providers should work with the Safety-Net Foundation to close known loopholes and to identify and investigate a range of appropriate measures to provide facilities for better traceability and to develop new and better forms of technical counter-measures. It is important that this joint work is taken forward, and that the various sectors of the IT industry continue to research better, cheaper and more user-friendly technical solutions.

Logging - server end

89. Abuse of Internet facilities, including chat services, cannot always be detected immediately, and source information may therefore be required after an event has occurred. For this reason it is necessary to keep the logging information in case it is wanted. Details of what is and/or might be logged on IRC are given in paragraph 83 above. It should be noted that these logs would not include the actual content of chat room activity.

90. To date there has been no clear definition of the Internet as either a public or a private place. The expectations (and possibly also the legal rights) of users could be different in each case, particularly in terms of whether or not their communications are likely to be monitored and/or logged. A test case establishing the status of the Internet would be helpful in clarifying the position.

91. It is important to note that the type of data which is logged for traceability is likely to constitute personal data under the Data Protection Act (1984 and its 1998 replacement). Therefore ISPs have to register as 'data users' with the Data Protection Commissioner, and to describe the purpose for which they are holding the data.

92. The fifth principle[39] of the 1998 Data Protection Act stipulates that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. According to EU Data Protection legislation[40], traffic data should be erased or anonymised as soon as the communication ends[41]. An exception is made for processing certain traffic data for the purpose of subscriber billing and interconnection purposes, but only up to the end of the period during which the bill may lawfully be

[38] http://www.iwf.org.uk/about/r3_safety.htm, paragraphs 21 ff.
[39] http://www.dataprotection.gov.uk/principl.htm
[40] http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html: Chapter II, Section 1, Article 6
[41] http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp25en.pdf

challenged or payment may be pursued. This has been defined by the Article 29 Working Group as being ideally no longer than 3 months[42]

93. However, these measures can be restricted if necessary for the prevention, investigation, detection and prosecution of criminal offences[43]. According to the LINX Best Practice document on traceability, the logs required to provide traceability should be retained for at least three months, and traffic data which may be needed for the detection of fraud may be kept for a maximum of six months.[44]

94. Recent incidents in chat rooms which have put children at risk or led to criminal offences being committed against them (see paragraphs 43 to 46 above) have prompted some calls, both within and independent of this working group, for all chat room content to be logged and stored for up to six months. A model exists for this in the fact that ICSTIS[45] requires continuous recording for calls which fall into the category of Live Entertainment. This catches one-to-one chat services (usually sex, but not necessarily) and tarot. These recordings are kept for six months and can be used to identify the caller and other breaches of the relevant codes[46].

95. Although there was considerable discussion within the group about this issue, the data protection requirements outlined above appear to preclude any such use of routine logging of content. However, it may be possible to log sufficient traffic data to link specific user names or nicknames to identifiable individuals in the offline world so that chat room access could be tracked without logging the actual conversation or activity. (It should also be noted that since online relationships are often merely initiated in chat rooms, and then developed through other media, the content of the chat alone may be of limited value.) Web-based chat services may also be able to require identification of users through any of the methods outlined in II.2.1 above in order to ensure offline traceability. Definitive clarification of these specific issues should be sought directly from the Data Protection Commissioner.

96. In the case of web based chat services which are aimed at a certain target audience or have closed membership, the use of server end logging may be possible but should be explicitly stated.

Logging - user end

97. Given the potential difficulties of server end logging, it is important that chat users are aware of the steps which they can take as individuals.

98. The most popular IRC programs provide a facility for logging both input and output activity on public channels and queries (requests for private chats). Many web-based chat services also offer logging and/or copy and paste

[42] ibid
[43] http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html: Chapter II, Section 6, Article 13
[44] http://www.linx.net/noncore/bcp/traceability-bcp.html
[45] Independent Committee for the Supervision of Standards of Telephone Information Services:
[46] Live Conversation Services Code of Practice (March 1998), section 2.1.3

options. It is important that such mechanisms are easy to find and to use, rather than being hidden away in complicated preferences or options menus.

99. For parents of young users, it may be desirable for the enabling/disabling of logging to be password protected in the same way as content filtering systems.

100. IRC software also offers a degree of user-end traceability, for example through the /whois and /whowas commands. Chat profiles can also provide some information on other users, although this is dependent on the degree of detail which they have offered about themselves. Tools such as Nbtstat and Netstat on chat and instant messaging services can be used to identify the person on the other end. However, the use of these tools requires a reasonable degree of computer knowledge, and more user-friendly graphical interfaces may be helpful.

101. However, it must be remembered that new technology allowing perpetrators to be traced more effectively could also allow victims to be de-anonymised more effectively and therefore can also compromise the anonymity and safety of children by being used to identify potential victims. It is therefore crucial that children do not give any personal information in online profiles, since this could render them vulnerable to being identified offline.

102. IRC users should be aware of the techniques which they can use to protect themselves online, such as making themselves invisible to other users (although this does not apply within the channel where they are active, only on the wider network) or placing other users on their ‘ignore’ list, as well as using the logging and copy/paste tools.

103. Webcams and the use of desktop video-conferencing offer the facility for transmitting live images and voice rather than text conversation. The increasing simplicity and falling costs of this technology are making it more attractive and more widely available. Webcams and desktop conferencing should be avoided completely by children, other than in a supervised educational environment, since these can be used to make visual contact with them. Children should not accept or download files other than from people they know and trust offline, since they may contain self-extracting software of this kind, or viruses which could reveal personal information to the sender.

Software tools - server end

104. Automatic word recognition: this can be used in web-based chat rooms to recognise and block particular character strings – words or phrases – which contravene the acceptable use policy of the service. However, in the context of protecting children online, it is difficult to establish a definitive list of keywords which could usefully be applied. Human moderation of a developing conversation is a far more sensitive and effective tool, although even with supervision it can be extremely difficult to establish the point at which a previously innocuous conversation becomes suspect.

105. Bots: short for "robot", this is normally a script run from a client machine or a separate software program which can be used to block keywords or perform other functions to ‘protect’ the chat channel. Although in moderated chat rooms bots may be useful in alerting the moderators to potential problems, they should not be relied on to safeguard the chat activity. It should be noted that many IRC servers (particularly in the United States) ban the use of bots completely.

Software tools - client end

106. Software programs can be a useful way of enhancing the care and protection of children accessing the Internet from a family or school computer. These are available in a variety of different forms:

- Filtering tools: a range of software options is available for filtering out inappropriate content. These can be particularly useful in helping parents and carers supervise their children’s use of the Internet. Filtering and blocking programs can cover a range of different categories of content, including the provision of personal details, and the use of sexually explicit language or images. Depending on the choice of tools, filtering can cover incoming and outgoing information, and can be used in chat as well as on other parts of the Internet.
- Monitoring tools: these enable a user’s online activity to be checked without necessarily limiting his or her access. Monitoring can also be used to limit the amount of time spent online.

107. Details of many of these tools and a matrix for selecting the most appropriate choices can be found on the GetNetWise website[47].

108. In considering the use of client end software it should be noted that these tools should not be relied on to provide foolproof protection for children online. A recent survey[48] of leading proprietary brands by the Consumers Association Which? Magazine raised some concerns about their efficacy, and they should only be used as an adjunct to adult involvement and supervision and to support policies and practices which have been discussed and agreed between the adult and the child.

Supervision and awareness

109. Although technology can provide useful tools for helping to create a safer online environment, it ought not to be relied on in isolation to protect children like some kind of electronic babysitter. A range of different types of human intervention, some of which are outlined below, ought to be employed to complement and underpin the role that technology can play.

Supervision - server end (moderation)

[47] http://www.getnetwise.org/tools/

[48] See http://www.iwf.org.uk/safe/tool.htm

110. Supervision can be implemented by providers of web chat services. In this context it is usually known as ‘moderation’. (Please note: it is important not to confuse this with ‘moderators’ or ‘operators’ on IRC, who are either self-appointed or appointed by existing operators, and who maintain technical control of the channels. In that context no supervisory function is implied.)

111. Moderation may be employed for a number of reasons in chat rooms, such as protecting a commercial brand, or ensuring that a discussion remains focussed on the intended topic. A common use of moderation is in chat rooms which are particularly aimed at children, and exists to ensure that the conversation is appropriate to the age group as well as in some cases to the particular subject of discussion.

112. Chat room moderation may consist solely in human supervision, or may use automated mechanisms such as keyword recognition and blocking, or expulsion of users contravening acceptable use policies.

113. The nature and extent of human moderation varies between chat rooms, as regards (a) the level of intervention, (b) the time period covered, and (c) the allocation of moderators to different rooms.

Intervention

114. Reactive moderation involves watching the chat room activity and intervening only when the conditions of use are breached.

115. Proactive moderation requires the moderator to check all submissions before they are uploaded to the chat room. In this way unacceptable content can be filtered before it reaches the public domain.

116. Time period:

- Some chat rooms are moderated throughout the time when they are open.
- Other chat rooms offer moderation only at certain periods, but are also available to users for unmoderated chat outside these times.

117. Moderator allocation: some chat services use a dedicated moderator for each chat room. The moderator stays in the same room throughout the designated time, and is able to accumulate knowledge of the room and its users over an extended period.

118. Chat rooms can also have ‘floating’ moderators who have responsibility for a number of chat rooms, and who visit them on either a regular basis or to conduct random sampling of the activity. They are often available ‘on call’ if required in an emergency.

119. Some companies use existing personnel to perform the function of moderator on a part-time basis, while others recruit their moderators, either as volunteers or as paid staff. Moderators can also be provided on a sub-contract basis through specialist companies. The level of selection and screening varies enormously, as does the supervision of moderators. The use of remote

moderation is widespread, with the moderator accessing the chat room from his or her own home, whereas other providers require their moderators to be on site.

120. Whilst the use of moderators can be an extremely useful way of checking the conversation going on in children's chat areas, and of preventing unacceptable activity, it is essential to ensure that adequate methods are implemented for recruiting, screening, training and monitoring moderators, given their potentially influential position and their access to children.

121. Currently moderators cannot be screened for criminal records, since their job does not involve physical contact with children. However, the introduction of the new Criminal Records Bureau under Part V of the Police Act 1997[49] in March 2001 may allow companies to obtain certificates on people applying to become moderators. The CRB will be able to carry out criminal records checks using four primary sources of information: the Police National Computer (PNC), which is a centralised information point for the police forces of England and Wales; local police force records; records held by the Department of Health about people considered unsuitable for work with children or with vulnerable adults and similar records held by the Department for Education and Employment. Employers and other groups wishing to run checks will have to register with the Bureau. Smaller employers and voluntary organisations may choose to group together and seek registration through an umbrella organisation.

122. In view of the privileged and potentially influential position of chat moderators in relation to the children using the service, it is essential that an appropriate level of information is made available through the Criminal Records Bureau to companies and organisations employing chat room moderators, whether on a paid or a voluntary basis.

123. However, it must be borne in mind that the global nature of the Internet and of some of the larger chat providers mean that moderators of chat facilities available to UK users may in fact be located elsewhere, for example in the United States, and that therefore screening provisions available in the UK may not be applicable.

124. It is also important to be aware that many sex offenders are active for many years without being caught, and therefore have no criminal record. Screening alone should not be relied on to ensure that appropriate people are appointed as moderators – other aspects of the recruitment process, as well as close ongoing supervision, are also essential.

125. On the whole moderated chat rooms or 'children-only' ISPs are aimed at and cater for children up to the age of 12. However, as seen in paragraph 55 above, risk assessment studies, particularly in the United States[50], have identified the most likely targets and victims of 'online enticement' (children

[49] http://www.crb.gov.uk/index.htm

[50] "Online Victimisation: A Report on the Nation's Youth"- National Center for Missing and Exploited Children (June 2000)

being approached and groomed by paedophiles on the Internet) as being teenagers, mainly girls, between the ages of 13 and 17. It is therefore important that such provision is extended to cover this age range. Particular thought needs to be given to moderating chat rooms geared specifically to teenagers. There may be resistance on the part of some young people to the idea of adults, known or unknown, 'eavesdropping' on their conversations, many of which may have some sexual content. The idea of using teenagers themselves to moderate some teen chat areas should be explored.

Supervision - client end (parent/carer)

126. Server end supervision cannot be relied on to safeguard all chat activity by children, particularly since some children may seek out and participate in adult discussions on a whole range of topics rather than limiting their chat activity to chat rooms designed for their own age group and therefore more likely to be moderated. Data about adult/child friendships which have been formed online can inform our knowledge of the kind of chat areas likely to cater to shared adult and teen interests – primarily those concerned with computer role-playing games (see MUD and MUSH in paragraphs 18 to 20 above), but also typically on subjects such as music, dance and sport.[51]

127. As for offline aspects of childcare, there is a clear responsibility on parents and carers to supervise the Internet use of children in their care. Where possible the family/child's computer should be in a shared space, although it is recognised that this may not always be feasible, especially in households with more than one Internet connection

128. In seeking to supervise the relationships being made by children through the Internet it is also important for parents to bear in mind that contact initiated in chat rooms may well be developed through other media, such as email and (mobile) phone.

129. The tools outlined in paragraph 106 above can be useful to parents in filtering and monitoring their child's activity, but the best way for parents to know what their children are doing online is to take an interest in their children's online experience and activity, and encourage children to discuss any problems they may encounter. In this context education and awareness are the key to equipping parents to support their children.

130. In allowing their children to go online, parents and other carers should be satisfied that their charges are aware of the nature of the risks and how to avoid them, and how to deal with problems should they nonetheless encounter them. It is essential that other 'gatekeepers' such as teachers and librarians should also be aware of online safety issues.

Education and awareness

[51] ibid

131. Education and awareness are key elements in empowering users to get the maximum benefit from the Internet and to protect themselves and children in their care against inappropriate content or contact online. The European Union has recognised the importance of education and awareness in its Safer Internet Action Plan[52], and is funding a number of initiatives across Europe, many of them in the not-for-profit sector.

132. Awareness materials should be provided from a variety of sources and in a range of different contexts. Such resources should be made available in offline formats as well as via the Internet itself. This is particularly important for informing less ‘net-literate’ parents and teachers.

133. Clear concise safety messages need to be aimed at several distinct age ranges and, where appropriate, to take into account the different approaches needed in communicating to boys and girls. Considerable research has been done on the most effective way to communicate these issues to children – the European Union funded the Netaware project[53] in 1999 which conducted research in 6 EU member states to identify best practice – their findings are available online and can be used to inform awareness programmes. In particular, since many teenagers often have (and demand) a degree of independence and privacy not relevant to a younger age group, careful thought must be given to the best way of communicating both the dangers and the possible solutions to them. Internet portals aimed at teenagers should be engaged in the process of developing and disseminating relevant safety messages.

134. It has been suggested that the effective communication of online safety advice may have a positive spin-off back into the ‘real world’ in raising children’s awareness of personal security and ‘stranger danger’ issues generally and thereby making them more ‘streetwise’ as well as more ‘chatwise’.

Government

135. The government has consulted widely on the issue of Internet awareness, and has launched a number of different initiatives. The Department for Education and Employment has made a Superhighway Safety Pack[54] available to all schools on request. Originally published in October 1999, this was updated and relaunched along with the Parents Online website on 18 September 2000.[55] The Clickthinking initiative by the Scottish Executive has made similar resources available to teachers in Scotland.

136. In a recent Parliamentary written answer Education Minister Michael Wills confirmed that no reports had been received of indecent approaches to children at school, through Internet chat rooms or by email, and that open chat

[52] http://europa.eu.int/ISPO/iap/index.html and http://www.saferinternet.org

[53] http://www.netaware.org/gb/website.html

[54] http://safety.ngfl.gov.uk/

[55] http://www.parentsonline.gov.uk/surfing/index.html

lines are rarely used in schools, specifically to avoid any possible compromise to pupil safety.[56]

137. It is essential that online safety messages are made available to as well as through schools. Internet policy guidelines for teaching and ICT staff, and contained within home/school agreements, must be consistent with best practice in these areas.

138. The Department of Trade and Industry launched the UK Online[57] programme on 11 September 2000. This is designed to enable everyone in the UK to gain access to the Internet by 2005 and to make the UK one of the world's leading knowledge economies. The UK Online website contains safe surfing information including child safety guidance.

139. The government has recognised the importance of co-ordinating these initiatives both between the various government departments and with external agencies. Meetings between a range of agencies have led to the adoption of the NetSMART rules[58]as a standard set of safety messages.

Industry

140. The Internet industry has a responsibility for educating consumers about the risks associated with the use of their products as well as the benefits. In this context ‘industry’ requires broad definition, since ISPs, virtual ISPs, hardware and software manufacturers and retailers, telcos and even television and mobile telephone companies can form part of the chain of Internet access provision.

141. A number of Internet Service Providers do already offer awareness material for their users, either on their websites and/or through mailing offline resources to their subscribers. All ISPs, particularly those aiming at a consumer rather than a business market, should provide such material, either on their own sites or by providing a prominent link to a central source. Customer helpdesk staff should be trained in either offering safety advice themselves or in advising subscribers where such information can be obtained.

142. Hardware manufacturers and retailers are uniquely placed to provide safety advice at the point of sale, either as an integral part of the literature provided with the product, or at the very least in the form of a separate leaflet which can be included with technical handbooks, brochures etc.

143. An additional suggestion raised in the course of the group’s discussion, but not considered in detail, was the possibility of home PCs being sold with pre-installed filter software with a high level of protection set as the default. This could then be reduced or removed by users for whom it was inappropriate or undesirable, but would ensure a degree of security even for new users.

[56] http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmhansrd/cm001107/text/01107w23.htm#01107w23.html_sbhd3

[57] http://www.ukonline.gov.uk/

[58] http://www.childnet-int.org/tips/index.html#3

144. Providers of chat software could readily incorporate regular banners or warning messages into their scripts, reminding users of the key safety messages (see Section C below). Similarly, website providers can include such messages in the HTML code. An example is that made available[59] by Childnet International through their ChatDanger site[60], which represents the first dedicated resource specifically providing safety advice about chat rooms.

Other

145. A number of other channels could be used very effectively to promulgate Internet awareness material. A variety of organisations have experience in communicating safety messages to young people on a range of different subjects, including sex education, road safety and the dangers of drug abuse. This experience should be drawn upon to inform the development of education programmes for young people on Internet safety.

146. In particular, 'stranger danger' education should be expanded to cover Internet issues. The evidence in paragraph 39 above indicating that less than 1% of child abuse incidents involve a stranger demonstrates the importance of teaching children that no matter how much they have chatted with someone online, that person remains a stranger until they have met in the real world. In this way the child's vigilance may be maintained and any possible risk reduced.

147. Suitable channels for safety messages include, but are not restricted to, the following:

Schools and colleges

148. Educational establishments need to be both recipients of and channels for Internet safety messages. It may be appropriate to include Internet Safety in the PHSE curriculum at secondary school level. For example, role play has been used successfully in encouraging children to think through and 'own' btheir personal responses to dangerous situations, and the same technique could be applied to identifying and dealing with online risks.

149. In Scotland, the brand new 5 – 14 curriculum guidelines for Information and Communication Technology are already exploring ways for safety topics to be included within this subject area as well as within the PHSE syllabus.

Children's charities

150. Various of the children's charities and youth organisations have their own programme of activities which bring them into regular contact with children either in schools or elsewhere. They might consider including Internet safety and awareness activities as part of their standard presentations to children.

[59] http://www.chatdanger.com/banner/banner.htm
[60] http://www.chatdanger.com

The UK children's charity NCH Action for Children already incorporates an Internet safety message in its School Presenters' programme.

Young people's organisations

151. Organisations such as the Scout and Guide movements are another possible channel for such awareness programmes – Internet safety should feature regularly alongside stranger danger, drug awareness and road safety sessions.

Media

152. The broadcast and print media are uniquely placed to spread messages about Internet safety. Recent media coverage of risks to children have highlighted some of the issues and have created a timely opportunity to respond with guidance on keeping safe online. Every media opportunity for educating Internet users should be exploited in a balanced and constructive way, avoiding the sensationalist and potentially counter-productive approach too often associated with much treatment of Internet safety issues over recent months.

Web resources

153. A number of different sites already provide excellent safety information. Examples are available from the Internet Watch Foundation[61], NCH Action for Children[62] and Childnet International[63].

Kitemarking

154. Kitemarks are a recognised and effective tool for increasing consumer confidence in the offline world, and are being used increasingly in the context of e-commerce, for example through the TrustUK scheme[64]. Particularly if online schemes use logos which are familiar in the offline environment, such as the Consumers Association Which? Symbol, they can be an important factor in empowering users to make informed choices about their Internet access and that of children in their care.

155. An acceptable set of minimum standards should be agreed for 'safe' chat rooms for children, and the use of some kind of kitemark would enable parents and carers to identify chat services which met these standards and where they could allow their children to go online with a greater degree of confidence. Some concern has been expressed that site providers who subscribed to such a scheme would be more liable than those who didn't, and that therefore they would be reluctant to display the kitemark. However, a disclaimer could make it clear that no absolute guarantees can be given, and that the mark demonstrates due diligence rather than a watertight scheme for ensuring online

[61] http://www.iwf.org.uk/safe/index.htm
[62] http://www.nchafc.org.uk/internet/index.html
[63] http://www.childnet-int.org
[64] http://www.trustuk.org.uk/

safety. Many schemes include similar disclaimers without necessarily diminishing their effectiveness or credibility.

156. A number of questions arise with regard to this issue:
- Who should own the kitemark?
- How should it be allocated and distributed?
- What enforcement mechanisms should be in place to prevent kitemark abuse?
- Who should be eligible to display the kitemark, ie should it be restricted to providers of online chat services, or could it also be displayed and 'sold on' as an added value benefit by providers of chat software, chat room moderators, etc?

157. It is recommended that the experience of existing kitemark schemes should be used to inform discussion and resolution of these issues, and that providers of children's chat services should be involved in establishing the appropriate standards.

Reporting

158. If incidents do occur in chat rooms which appear to constitute an inappropriate sexual approach to a child or an offline risk to a child's safety, it is crucial that appropriate reporting mechanisms can be readily found and are easy to use.

159. Research from the United States[65] into online enticement of children found that just half of such incidents were reported. Of those reported, only 10% were referred to the user's ISP, a hotline or law enforcement, with the rest being reported to friends, siblings or parents. This reluctance to report incidents, even to parents or other carers, means that it is imperative to provide 'child-friendly' reporting mechanisms which use accessible language and ensure the confidentiality of the reporter. The expertise and experience of existing child-focused schemes such as ChildLine[66] and the NSPCC [67] could be useful in establishing best practice in this area.

160. Providers of web-based chat services should provide a prominent link – a so-called 'trouble button' - to their own abuse department and/or to an external agency who can take swift and effective action. Regular banners or warning screens should also include similar links.

161. Internet content hotlines, such as the Internet Watch Foundation in the UK, have become established as an effective mechanism for dealing with complaints about content on the World Wide Web and in Usenet newsgroups. However, the realtime nature of chat has meant until now that (with the exception of the US CyberTipline) hotlines have not undertaken to deal with reports of IRC or chat room activity. The IWF has received 111 reports about chat since the launch of its hotline in December 1996, of which 36 have been

[65] "Online Victimisation: A Report on the Nation's Youth"- National Center for Missing and Exploited Children (June 2000)
[66] http://www.childline.org.uk/
[67] http://www.nspcc.org.uk/help/

referred on a non-verifiable basis to law enforcement. If the remit of the Internet Watch Foundation were extended to deal with realtime reports of risks to children in chat rooms, this would have significant resource implications, and IWF funding levels and sources would need to be re-assessed in order to support this increase.

162. Realtime handling of reports also requires 24/7 responses from both law enforcement and Internet service providers so that urgent threats can be investigated immediately. It is expected that the establishment of the National Hi-Tech Crime Unit and of the Internet Crime Forum network of 24/7 contact points will contribute significantly to achieving timely responses.

Law enforcement responses

Capability

163. The growing popularity and penetration of the Internet means that many kinds of criminal activity are increasingly migrating to the electronic world. The National Criminal Intelligence Service has recognised the facility presented by computer networks for criminal, in particular paedophile, activity[68], and the need for law enforcement to develop appropriate responses and resources.

164. In the UK there are currently only a small number of specialist police officers and even fewer dedicated units equipped to deal with Internet investigations. The dedicated units are often connected with or have evolved from fraud squads and are now applying the same investigatory techniques to a wide range of activities, including crimes against children. Others are part of obscenity or paedophilia units. These dedicated units are frequently operating with minimal resources and because of their specialist knowledge are often called upon to deal with cases outside their own geographical area, which can create difficulties for them in justifying their continued funding.

165. Knowledge of Internet issues among non-specialist personnel varies greatly, and many local officers receiving reports of Internet-related crimes do not know how to respond, with the result that initial handling of such complaints can be inconsistent and piecemeal.

166. There are particular difficulties in retaining experienced personnel, for both internal and external reasons. Firstly the system of tenure within forces, which was introduced to enhance equal opportunities by ensuring that individual officers only remain in a particular post for a fixed period, means that specialist knowledge and expertise are lost within the police structures. In addition, the competitive salaries offered by the private sector to specialists in computer security and investigation has also led to a significant migration of experience and available resources.

167. There is a clear need for more training of police officers in the area of Internet crime. Non-specialist officers should have knowledge of whom to contact

[68] NCIS Project Trawler: crime on the information superhighways report (1999) and 2000 UK Threat Assessment reports

about reports of criminal activity on the Net, and in particular in chat rooms. Training is also required to ensure that police are familiar with the provisions and procedures for requesting information from the relevant private sector organisations. Considerable progress is being made on these issues through the work of the Internet Crime Forum.

168. A best practice paper[69] prepared by the INHOPE Forum for the European Union in July 1999 found that most law enforcement agencies across Europe lack the training and the resources to address computer–related crimes, especially when they are occurring in IRC. The paper recommends that European governments should follow the example of the United States where government has been proactive in supporting federal and local law enforcement in tackling computer and Internet related crime. For example, the FBI has an online task force with the specific remit of interacting with individuals who use computers to lure children into illicit sexual relationships and investigating individuals who produce and distribute child pornography.

169. One aspect of police activity in the US, which cannot readily be replicated in the UK, is the extent to which law enforcement personnel are able to engage directly with suspects in order to gain evidence. The FBI Internet Crimes Against Children Task Forces can go into chat rooms where illegal activity is believed to be taking place, and can pose as children, make contact with suspected offenders, and even arrange to meet offline. A significant proportion of the convictions gained in the United States, including at least one transjurisdictional case involving the UK police[70], has been initiated through such sting operations.

170. UK law enforcement officers have much stricter restrictions on any activity which could be perceived as entrapment, and are therefore more limited than their American counterparts in proactive investigation of suspect chat room activity. Indeed, in the DTI/Home Office review of the Internet Watch Foundation it was concluded that there may be a case for revisiting the laws of entrapment[71], which have developed through cumulative case law rather than statute, and is therefore not enshrined in any specific legal instrument.

171. However, it would be inaccurate to suggest that UK police possess no such powers. The only instances where police become involved in undercover operations are invariably serious cases. With the approval of an authorising officer, within the context of an authorised operation, an undercover officer can infiltrate existing criminal activity, or become a party to the commission of criminal offences. Any such operations have to be sanctioned at an extremely high level, are extremely closely monitored and supervised on a daily basis, and only allow the participation of specially trained officers. These must be supported by a full back-up team. (An exception to the 'full back up team' scenario would be where an officer posed as a child on the Internet, but if that officer then took part in a physical meeting with a suspect the 'full back

[69] Handling Illegal IRC Content: a best practice paper prepared for the INHOPE Association by Louis Alexander and Jim Reynolds, former head of the Metropolitan Police Paedophilia Unit.
[70] See paragraph 46 above
[71] DTI and Home Office Review of the Internet Watch Foundation, section 8.2.1.1

up team' scenario would have to be implemented.) All details of police participation must be meticulously recorded at all times. It is clear from this that undercover work has significant resource implications, particularly for local forces.

172. The introduction of the Regulation of Investigatory Powers Act, which came into force in September 2000, provides a statutory basis for the use of surveillance and covert human intelligence sources. The authorisation procedure is set out in Part II of the Act, and is outlined in the draft codes of practice[72].

173. Whilst ‘entrapment’ is not a defence against liability under English law, it can be a mitigating factor for sentence under section 78 of the Police and Criminal Evidence Act 1984 if a trial judge concludes that the defendant was induced to commit a crime which he or she might otherwise not have committed. A recent case brought before the European Court of Human Rights[73] concluded that where undercover officers did not confine themselves to investigating suspected criminal activity in an essentially passive way, but incited an offence which would otherwise not have been committed, the subsequent trial of the individual so incited contravened Article 6(1) of the European Convention on Human Rights, namely the right to a fair trial.

174. It therefore seems that the current position in the UK does allow for police undercover operations to be used to deal with chat room activity. However, there are likely to be problems in obtaining convictions if the actions of the police go beyond merely giving an offender an opportunity to commit an offence which he would have done had any other opportunity presented itself.

Co-ordination

National

175. There are 43 police forces in England and Wales, which operate with a high degree of autonomy and with limited access to shared information and intelligence. Since the structure of the Internet and therefore the nature of much Internet crime does not respect even national boundaries, it is imperative that separate forces within the UK have prompt and effective mechanisms for exchanging information and responding to real-time risk. One of the concerns raised in the Patrick Green case was the length of time taken to transfer the necessary documentation between the two forces, that of the victim and that of the perpetrator.

176. On 13th November 2000, the Home secretary announced £25 million funding over the following three years, for the new National Hi-Tech Crime Unit, which would begin work in April 2001. The Unit is being developed by a joint project team from the National Criminal Intelligence Service

[72] http://www.homeoffice.gov.uk/ripa/ripact.htm

[73] Texera de Castro v Portugal (1998)

(NCIS), the National Crime Squad (NCS) and HM Customs and Excise (HMCE).The unit will be managed by the NCS on behalf of those agencies and wider law enforcement. More than 120 specialised and dedicated personnel, one third of whom will be centrally based, will be deployed by the Unit and local Forces. The unit will have a number of remit areas, including the following:

i. Investigate, or support the investigation of, serious and organised crime usually operating on a national or international scale, that wholly or partly involve computers or computer networks such as the Internet
ii. Investigate attacks on the United Kingdom Critical National Infrastructure
iii. Undertake forensic retrieval and examination of computer-based evidence gathered in its investigations
iv. Provide the national point of contact for overseas investigators of international offences involving computer networks
v. Provide technical support and advice to investigators in the police service and other law enforcement agencies across the United Kingdom
vi. Work in partnership with local police and other agencies taking forward to promote information security and other hi-tech crime reduction strategies
vii. Liaise with industry on behalf of the police service to support co-operation between law enforcement and industry in the detection, investigation and reduction of hi-tech crime.

177. The establishment of this national unit will be a major step forward in tackling criminal activity on the Internet, in terms both of providing specialist technical support and expertise and of co-ordinating investigations both within this country and internationally. The government funding will also help to establish a 24/7 point of contact system with overseas police forces in accordance with the UK's commitments within the G8.

178. In finalising the precise role and priorities of the unit, it is important to ensure that child safety on the Internet is considered of paramount importance, and that sufficient resources are available through the unit to tackle criminal activity against children in chat rooms. In November 2000 the Home Office minister Charles Clarke stated that the unit would deal with criminal use of chat services in cases where this fell within its remit. In addition, local police computer crime units would investigate crimes with a local impact. The Hi-Tech Crime Unit would also work with police and industry to develop best practice for proactively policing the Internet to identify and prosecute criminals using newsgroups and chat rooms to facilitate illegal activity[74].

179. Communication and co-operation within the UK are also being improved through the work of the Internet Crime Forum. As well as facilitating discussions between a range of law enforcement agencies, government and industry, the ICF is also working on the establishment of 24/7 contact points on a national level.

International

[74] Written answer to Parliamentary Question, 22 November 2000

180. The Internet offers unprecedented opportunities for communicating on a global basis. This facility is open to abuse by criminals in a number of ways, including illegal activity targeted at sexual exploitation of children, as follows:

- Using the Internet to make contact with other adults with sexual interest in children elsewhere in the world to exchange child pornography or to procure a child for sexual purposes
- Exploiting the borderless nature of the Internet to host illegal content or commit criminal acts in a less hostile jurisdiction
- Having access to potentially millions of children worldwide from whom to select an appropriate target.

181. The paramount importance of having prompt and effective international responses to the threats posed by cyber-crime has been recognised by a range of high-level international organisations. The G8 countries held a high-level meeting of government and industry representatives in Paris in June 2000, and this was followed up with a practical workshop session in Berlin in October. The Berlin meeting considered a range of issues, including the following:

- The establishment of 24/7 contact points
- Retention and preservation of data
- Computer security
- Law enforcement training needs
- Education and awareness programmes.

182. In addition, Europol and Interpol have both been exploring both the policies and the operational procedures for enhanced international co-operation on computer related and aided crime. The Council of Europe is currently debating a draft Cyber-Crime Convention[75]. This covers a range of issues concerning both national and international measures to combat illegal activity using computers and computer networks. Specifically on the issue of international co-operation[76], it makes the following recommendations:

- Mutual assistance between national police forces on expedited preservation of stored computer data and disclosure of preserved traffic data;
- Provision of trained and equipped 24/7 points of contact for the purposes of
  (1) providing technical advice;
  (2) preservation of data pursuant to Articles 24 and 25; and
  (3) the collection of evidence, giving of legal information, and locating of suspects.

183. As demonstrated above, there is clear commitment by a wide range of high-level bodies to establishing mechanisms which will improve international communication and co-operation in the detection and investigation of computer crime. As in the case of the UK National Hi-Tech Crime Unit, it is imperative that the design and implementation of such mechanisms are appropriate for protecting children against sexual solicitation and abuse, as well as for other kinds of threat such as attacks on the Critical Infrastructure, fraud or money laundering.

[75] Draft Cyber-Crime Convention (Draft No 22, 2.10.00)

[76] ibid., Chapter III

Conclusions

184. This consideration of the potential risks to children using online chat services inevitably reflects the complex nature of the issues involved. This is perhaps not surprising given the complexity of the various contributory factors: the technology, the legal framework, and the psychology and behaviour of potential offenders. Nevertheless, in building on the results of this work it is essential that all the relevant stakeholders, including government, the computing and Internet industries, law enforcement agencies, child welfare organisations, the education sector, self-regulatory bodies and the wider online community, demonstrate a genuine commitment to seeking, identifying and implementing effective solutions which will enable children to enjoy the benefits of the Internet without compromising their safety.

In response to the issues specified and discussed above, a number of recommendations were agreed, and the key safety messages for children's chat room activity were identified.

Section B:

Recommendations[77]

a) Children should use chat services specifically targeted at their own age range which have adequate levels of care and protection as outlined in (d) below.

b) Relevant UK legislation should be kept under constant and comprehensive review to ensure that it can meet changing circumstances, both online and offline, to protect children from abuse.

c) The various sectors of the IT industry should continue to research better, cheaper and more user-friendly technical solutions to the potential dangers of chat, including the identification and investigation of improved measures to ensure an appropriate level of traceability.

d) Providers of chat services specifically aimed at children should provide a responsible standard of care to protect their users. The nature and extent of protective measures should be transparent to all users.

e) A focussed education and awareness programme should be aimed at parents and other carers to advise them of the potential risks to children using chat services and appropriate steps they can take to protect them.

f) All Internet Service Providers should provide clear advice to their subscribers about the potential hazards of chat and the simple safety messages (see below) to help avoid them.

[77] The order of these recommendations reflects the sequence in which the supporting issues are considered in the paper.

g) Industry, user groups and children’s organisations should jointly explore the possibility of introducing a kitemarking scheme which would offer a simple way for parents to identify chat services committed to providing an enhanced standard of care for young users.

h) A user-friendly reporting mechanism should be available to facilitate the prompt reporting and investigation of incidents in chat rooms.

i) Law enforcement officers should have specialised training and increased resources to ensure a prompt and effective response to reports of incidents in chat rooms. The new National High-Tech Crime Unit should ensure that online protection of children is and remains a high priority.

Section C:

Safety messages - 'Chat Wise, Street Wise'

1) Don't give out personal details, photographs, or any other information that could be used to identify you, such as information about your family, where you live or the school you go to.

2) Don't take other people at face value – they may not be what they seem.

3) Never arrange to meet someone you've only ever previously met on the Internet without first telling your parents, getting their permission and taking a responsible adult with you. The first meeting should always be in a public place.

4) Always stay in the public areas of chat where there are other people around.

5) Don't open an attachment or downloaded file unless you know and trust the person who has sent it.

6) Never respond directly to anything you find disturbing – save or print it, log off, and tell an adult.

.

APPENDIX 1

Members of the Internet Crime Forum sub-group on chat

John Carr	NCH Action for Children
Camille de Stempel	AOL Europe
Ruth Dixon (Chair)	Internet Watch Foundation (IWF)
Cathy Gerosa	Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS)
Stephanie Harris	Internet Services Providers Association (ISPA)
Phil Hills / Norman Trew	National Criminal Intelligence Service (NCIS)
Steve Quick	Metropolitan Police Paedophilia Unit
Jim Reynolds	International Paedophilia Consultant
Birol Mehmet / Steve Ruddell	Home Office
Roland Perry	London Internet Exchange (LINX)
Pete Uglow	(formerly) West Midlands Police

The group would also like to acknowledge the additional input and opinion provided by Malcolm Hutty from the Campaign against Censorship of the Internet in Britain (CACIB).