Understanding Online Social Network Services and Risks to Youth

STAKEHOLDER PERSPECTIVES

A PRELIMINARY REPORT ON THE FINDINGS OF THE CEOP CENTRE'S SOCIAL NETWORK SEMINAR SERIES

Child Exploitation and Online Protection Centre

First Published: November 2006

Author: Margaret Brennan

Publishing Agency: Child Exploitation and Online Protection Centre, London.

Please address any requests for further copies of this report or any other queries concerning this publication to:

Margaret Brennan,
Child Exploitation and Online Protection Centre,
33 Vauxhall Bridge Road,
London
SW1V 2WG

Electronic version available for download at:
www.ceop.gov.uk/corporate_literature.html

CONTENTS

Executive Summary

Since the advent of the Internet and the emergence of the online community, few Internet forums have triggered such expressions of public concern for the welfare of younger members as social network services (SNS). Notwithstanding the fact that online social networks have utterly revolutionised social interaction, this new environment can facilitate new forms of social deviance and criminality. Its ability to collapse the conventional social barriers that govern sexual behaviour has compounded this situation, presenting new opportunities for sexual expression and deviance both to young people and to adults with a sexual interest in this group. This has resulted in a very real series of risks to the welfare of young people that socialise in this environment.

To date, the safeguards we have set in place have not had a meaningful impact on the array of risks faced by young social network users. The recent confusion of reports of abuse of young social network users, reactionary interventions, media hype, and resulting moral panic has generated much fear and made the safeguarding challenges presented by this new environment seem almost insurmountable. This situation is not helped by the fact that our understanding of these problems is largely anecdotal and under-researched.

In keeping with it's Safer by Design ethos (Child Exploitation and Online Protection Centre, 2006) the CEOP Centre recognises that interventions aimed at keeping young people safe in this environment will only be effective if they are informed by a reliable, first-hand understanding of the nature and scale of the problems faced by young SNS users. Building an evidenced knowledge base of the effects of social networking sites on youth was the principal aim of the CEOP Centre's Social Networking Seminar series.

The following report details the key outcomes of this seminar series. The aim of these seminars was to:

- Explore usage patterns among youth and adult populations
- Determine the positive and negative aspects of social networking
- Identify risks to the welfare of youth users
- Identify the respective responsibilities of safeguarding stakeholders
- Establish ways in which youth can be better safeguarded in this online environment.

CEOP invited a range of stakeholders to participate, principally young Internet users, parents, teachers, SNS and other media providers, law enforcement, local and national child protection agencies, educational authorities and members of the Home Office Task Force on Social Networking Services. Sixteen workshops were held over a four-day period in July of this year. In the course of these workshops, adult and youth participants were invited to discuss their own experiences of social networking for a and share their perspectives on this online environment.

Broadly speaking, adult groups perceived that they did not completely understand the phenomenon of online social networking or what the actual safeguarding risks are for young people in this environment. They were however, aware of the challenges these fora pose to law enforcement, SNS providers and other agencies seeking to mitigate these risks. This group felt that these challenges have stemmed from a historical lack of awareness of the risks to young people associated with these services, few visible facilities that could allow the public to report abusive behaviour to these authorities and consequently, low levels of detection and intervention. Moreover, they expressed concern that they did not know how or where to access learning resources that would allow them to become effective safeguarding agents. The youth user group echoed many of these concerns and asserted that they should be used as a resource to build knowledge around risks and possible countermeasures in the social networking environment. Both groups reaffirmed the need for further education on online safety and the capacity to report to safeguarding authorities should they encounter risks or harmful behaviour online.

Ultimately, we need to continue to enhance our understanding of new and emerging risks to the welfare of young social network users and share these insights with every stakeholder group. This will rely heavily on further research, enhancing the ability of the public to report abusive behaviours to safeguarding authorities and the provision of further opportunities to young people to share their understanding and experiences of abusive behaviour mediated through social networking environments.

The following report comprises the key findings of the seminars, a series of recommended action points for safeguarding youth and the CEOP Centre's initial responses to this call to action. The combined perspectives of workshop participants will advance a more rigorous, multi-faceted understanding of the phenomenon of social networking; an understanding that can be used to meaningfully progress the safeguarding initiatives of all stakeholders, at national and international level.

1. Introduction

Online Social Networks: Social Opportunity, Deviance and Risks to Youth

"Just as the computer has begun to revolutionise social life, it will revolutionise crime and deviancy; especially the parameters of deviant sexual behaviour…in fact, it is doing so already."

(Durkin and Bryant, 1995)

A social network is a social software that enables people to rendezvous, connect or collaborate through computer-mediated communication (CMC) and to form online communities. On social network services (SNS) people create a self-descriptive profile and then make links to other people they know on the site, creating a network of personal connections (Donath and Boyd, 2004). These services allow people to come together online around shared interests or causes. Although penned over a decade ago, Durkin and Bryant's prediction of the social impact of computer-mediated communication is more relevant in today's online environment than ever before; particularly in the context of the social networking debate. Since the advent of the Internet and the subsequent emergence of the online community, few social softwares have triggered expressions of public concern for the safety of younger users to this degree. So great is the public attention they have received that a bespoke task force on SNS has been established by the Home Office to develop good practice guidelines aimed at safeguarding youth users of social networking services.

Durkin and Bryant make three key observations about the impact of computer mediated communication on social interaction. While CMC has revolutionised social behaviour (particularly that of younger users), the enhanced communicative capability afforded by increasingly interactive forms of CMC also facilitates social deviance and criminality. In particular, it has revolutionised the parameters of deviant and criminal sexual behaviour. When applied to the social networking context, these observations advance a basic understanding of the issues particular to this phenomenon.

1.1 Social networks and social behaviour

The emergence of online SNS has radically challenged our understanding of traditional, territorial social networks. Hill and Dunbar (2003) estimated that an average Westerner's social network comprises about 150 individuals, sometimes known as "Dunbar's number." Once a physical social network is established, this number of members tends to change little over time. In contrast, the great exhortation of social networking sites is to "grow your network now!" meet new people and form new connections. The goal is an ever-increasing girth of one's social network. (Donath and Boyd, 2004). The many social advantages provided by online SNS can be evidenced in the great popularity they have enjoyed since their introduction in early 2003. By July of 2006, MySpace had become America's second-most popular virtual environment, comprising eighty-seven million users and expanding at a rate of about two hundred and seventy thousand new users a day. Approximately one quarter of its users are minors (Granneman, 2006). This September, it was estimated that this service comprised over one hundred and six million members, with little change in the rate of users signing up to the service (Faultline, 2006).

Young people engage with others through a variety of associations, forming many different types of networks. These social networks are not only important in terms of emotional support but are also crucial in giving them more opportunities, choice and power (Boeck, Fleming and Kemshall, 2006). Online social networks allow young people to meet and interact in ways that comfortably approximate real-world social exchanges and provide many social opportunities far superior to those that can be achieved within traditional social forums. Anderson (2006) enumerates some of the many advantages of online social networking over other forms of social interaction:

- Social networking services encourage people to create web content rather than consume it
- Changes web exploration from solo journey to a social outing
- Discover any type of experience (e.g. new music, a book etc)
- Choices and opinions can be informed by preferences of peers
- Discuss matters that are hard to handle face to face
- Find and participate in groups of like interest (sport, school)
- Lots of fun!
- Act as a platform for self expression - and the network is your audience

Children and young people, having a heightened need to communicate and be included in social networks willingly exploit these online facilities and push the boundaries of use to create virtual social networks. Young SNS users perceive these areas as private and free from parental control, while allowing opportunities for regular and instant communication with their peers (Morrissey, 2006). In the UK, as many as six in ten 13-17 year olds have personal profiles on social networking sites (Goodchild and Owen, 2006).

1.2 Social networks, crime and deviancy

Innovation in technology also has the potential to revolutionise crime and deviancy. We now know that this can, and does, provide new, ever-changing opportunities for the pursuit of deviant interests. Online social networks, more usable now than ever before, have also become increasingly "abusable." The increasing user-friendliness of these services has afforded some users new opportunities to abuse their networking capabilities to facilitate criminal or other deviant behaviours. Social networking sites remove the privacy barriers we use to keep incompatible contexts of our lives separate in the physical world (Donath and Boyd, 2004). The absence of conventional social barriers to abuse in this forum (e.g. physical and geographical constraints, parental supervision, peer protection, a law enforcement presence etc.) means that vulnerable groups like children and young people who require safeguarding and protection become more vulnerable still in the online social networking environment. Many principles and processes have been established to promote effective safeguarding and the welfare of children in the offline context (e.g. Children Act, 1989; Working together to Safeguard Children, 2006). These have yet to be translated in a way that affords young people due protection in the online world.

1.3 Social networks and deviant sexual behaviour

Before the advent of social networking forums, the principal effect of social software on sexual deviancy was that it allowed computer users with special or deviant sexual predilections to communicate with persons who share similar interests throughout the world (Durkin and Bryant, 1995). Historically, individuals with a sexual interest in children have exploited this capacity to communicate with like-minded individuals, nurture their shared interests and even facilitate deviant and criminal behaviours in the offline environment.

The emergence of superior communicative technologies, particularly social networking forums, has exacerbated this situation. Quite apart from their ability to interact with like-minded others, individuals with a sexual interest in children can now access and engage directly with a pool of potential victims on an unprecedented scale. The types of interaction now possible present new opportunities to deviants to nurture and advance their sexual interests by observing and interacting with youth online, accessing erotic paraphernalia (text, images, video, live-time communication, etc.) and more ominously, soliciting direct engagement with children offline.

The concerns have been reflected in a steady increase in the number of reports to law enforcement in the UK that relate to the sexual abuse of children and young people in social networking environments (The CEOP Centre, 2006).

Concerning as this is, those with a stake in safeguarding youth users of SNS need to recognise that the propensity to engage in risky, sexually deviant behaviour is not just limited to predatory adults with a sexual interest in children. The accessibility of social networking forums to youth users combined with unparalleled levels of media literacy within this population mean that young people can readily use online social networking environments as an alternative social medium. Moreover, traditional social theory dictates that young adolescents engage in an exceptional level of socially disapproved behaviours that pose risks to their long-term well-being (Arnett, 1999). It follows that young people can and will exploit social networks to socialise, express themselves and experiment sexually; to behave and misbehave just as they would in real-world social environments.

This situation presents new risks to youth users of social networks and consequent challenges to those tasked with safeguarding them in this environment. Technology changes the fabric of the material world, which in turn changes the social world (Smith, 1992). Because it is mediated online, sexual interaction and other risk-taking behaviours among youth find new forms of expression in the social networking context (e.g. through self-production of erotic material such as images/video, participating in sexually-themed chat, engaging in sex acts using webcams, etc.). Though little understood by participants, these virtual interactions can have harmful real-world effects. For example:

- These behaviours can be witnessed by an unfamiliar audience, particularly by adults with a sexual interest in children
- These behaviours render youth prone to unwanted sexual advances (exposure to sexual paraphernalia, harassment, solicitation etc.)
- Youth may upload visual representations of themselves that are sexual in tone without completely understanding the perpetual quality of any image, video etc. that is distributed online, or the ways in which these can be subsequently accessed and exploited by adult audiences for the purposes of sexual gratification
- This behaviour may have a negative social influence on younger, lesser developed children that share these online spaces

To date, many of the interventions set in place to tackle the abuse of young social network users have been overbroad and under-specific, based on a less-than-complete understanding of the complexities of this phenomenon. Consequently, these interventions have not had a visible impact on the risks faced by young social network users, perceptions of the prevalence of these risks, or dissuaded youth from engaging in online behaviours that can put them at risk of harm. Social networking services have planned to balance the continuing expansion of their networking capabilities by "beefing up" security and safety options (Granneman, 2006). This cannot and should not be the complete solution. It is not sufficient to abdicate major safeguarding responsibility to technological industry and law enforcement agencies without the benefit of broader consultation; resulting interventions will always be limited in scope and reactive in nature. More worryingly, quick-fix, reactive interventions could themselves have harmful unintended consequences for young people.

This July, the US House of Representatives voted by an overwhelming majority to ban, with few exemptions, commercial SNS in schools, libraries and other facilities receiving federal aid (Roush, 2006). The Deleting Online Predators Act (DOPA) forbids publicly funded organisations from allowing young people to access sites that have chat rooms or "social networking" elements where they might encounter adults seeking sexual contact. Broad proscriptive interventions like DOPA may have negative residual effects on young people. Opponents of this legislation claim it will restrict children's access to vital online learning and social resources and widen the digital divide by limiting access for people who use library and school computers as their primary conduits to the Internet (American Library Association, 2006). Furthermore, restricting access to SNS in this way may compel young people to use social networking services in other settings where they are less supervised than at school (e.g. in their bedroom, friends houses, Internet cafes, etc.).

Introduction

It is also becoming apparent that the measures SNS providers put in place to protect users of their services (e.g. site monitoring, profile protection for under 18s and age verification systems based on credit card use) afford limited protection to children and young people. Some younger users have become adept at circumventing these monitoring systems or tend to frequent sites that offer free services. Moreover, these measures may not be useful from a harm reduction perspective; sometimes leading simply to the impersonation of identity among those seeking access to younger users "New rules - based on the ages the users report themselves to be - are in place that control who can view profiles, and the amount of information that can be viewed by other users…so we're right back to the spectre of a predator claiming to be 14 so that he can more easily target other teens," (Granneman, 2006).

The recent confusion of reports of harm to young social network users, reactionary interventions, media hype and resulting public and parental concern have generated fear and made the safeguarding challenges presented by this new environment seem almost insurmountable. Moreover, our understanding of the effects of online social networking on young people is largely anecdotal and under-researched. In keeping with it's Safer by Design ethos, the CEOP Centre recognises that interventions aimed at keeping young people safe in this environment will only be effective if they are informed by a reliable, first-hand understanding of the nature and scale of the problems faced by young social network users. Building an evidenced knowledge base on the effects of social networking sites on youth was the principal aim of the CEOP Centre's Social Networking Seminar series.

The key findings of the seminars and a series of safeguarding action points are detailed in the sections that follow. It is hoped that these findings will act as a conceptual platform for the design of future safeguarding interventions that will ultimately reduce harm to young members of online social networks.

Alex Nagle
Head of Harm Reduction

2. Structure and Conduct of Social Network Seminars

Structure and conduct of Social Network Seminars

The following sections detail the key outcomes of series of seminars hosted by the Child Exploitation and Online Protection centre on the phenomenon of social networking. The outcomes reported here constitute a preliminary exploration of the key themes of concern explored with workshop participants. It is anticipated that the data collected in the course of these seminars will inform and support parallel safeguarding programmes in this area headed by the Home Office Task Force on Social Network Services. The combined perspectives of workshop participants will contribute to a more rigorous, multi-faceted understanding of the phenomenon of social networking; an understanding that can be used to meaningfully advance the safeguarding initiatives of these stakeholder groups, at national and international level.

CEOP invited a range of stakeholders to take part in these seminars, principally young Internet users, parents, teachers, SNS and other media providers, law enforcement, local and national child protection agencies, educational authorities and members of the Home Office Task Force. Each day-long seminar began with a series of introductory presentations on the topic of social networking. In the afternoon, participants broke out into four workshop groups followed by a summary presentation of workshop outcomes. The aim of these seminars was to explore usage patterns, positive and negative aspects of social networking, identify risks to the safety of youth users, the respective responsibilities of safeguarding stakeholders and establish ways in which youth can be better safeguarded in this online environment.

Sixteen workshops were held over a four-day period in July 2006. Adult and youth contributors were invited to offer their own experiences of social networking fora and share their perspectives on this online environment. Four daily workshops were broken down by group as follows:

Youth Stakeholder Group

One youth workshop was held per day. Youth workshop contributors ranged in age from ten to sixteen years and comprised a cross-section of pupils from a number of schools in South East Britain. The average number of participants per youth group was fifteen. Young people's workshop participants engaged in focus group discussions about their experiences and perceptions of the online social networking environment. They were also invited to take part in group project work where participants created charts and diagrams describing these views and experiences. It was important that measures were instituted to maximise young peoples' capacity to contribute freely to the workshops without embarrassment, and in doing so, allow for the emergence of extra information that could otherwise have been withheld from the group. To this end, the workshops were semi-structured in format; facilitators did not adhere to a strict schedule of questions in the workshops and allowed in-group conversation to develop independent of facilitation, although it was ensured that a series of predetermined discussion themes were addressed in the course of each of the workshops. These groups were facilitated by an independent workshop co-ordinator.

Adult Stakeholder Group

Three adult workshops were held each day; each involved group work and focus group discussion. Groups were facilitated by an independent co-ordinator. Participants represented a broad range of stakeholder groups (detailed above) and were principally derived from statutory authorities and the private sector. To facilitate the ability of group members to contribute freely to the workshops, programme of each workshop was designed generate in-group conversation. Like the youth workshops, the discussion schedule was semi-structured in format while adhering to a series of key themes of concern.

3. Key Findings*

3.1 Youth Stakeholder Group: Experiences and Perceptions of Online Social Networks

3.1.1 Understanding youth usage of social networks

How were these sites discovered?

Users reported that they mostly heard about these sites through their friends. It was not clear whether, or to what extent, this was through word of mouth or through some form of online notification.

Why are these sites used?

All users reported that the reason they used the sites was because they provided some social or entertainment value, especially:

- Meeting/chatting with friends
- Gaming activities
- Accessing photos
- Relieving boredom

What do young people like best about social networking?

Youth users reported they most enjoyed five particular benefits of social networking:

- Facilitates social relationships - e.g. ability to keep in contact, meet new people, maintain long-distance relationships etc.
- Economical (social networking is free on sites frequented by young users) - young people reported that social networking is a cost-effective alternative to the mobile phone, allows them to download music freely etc.
- Entertaining (e.g. humour, gaming, learning, etc.)
- User friendly - sites are easy to use; meet their need to block unwanted contacts etc.
- Facilitates self-expression - users reported that sites allow them to express their views in a way that they cannot do offline

What do young people like least about social networking?

Youth users reported that they least liked the following aspects of SNS:

- Insecurity of information - younger users feel that information they post on sites (particularly "private" images and personal information) is not secure, not confidential and "gets put on the web." Equally, many voiced concerns that they often felt pressurised by other group members to hand out "personal information", especially email addresses, when they did not feel comfortable in doing so
- SNS can be an unsafe social environment (youth reported feeling exposed to unwanted information or individuals)
- Exposure to unwanted audience of individuals - youth feel visible to a large audience who are not known to them. Many reported their webcam "turning on with people they don't know"
- Difficult to foster trusting relationships with those they do not know offline - young people expressed that they cannot authenticate the identity of those they are talking to
- Exposure to unwanted information (e.g. pop-ups, banners, etc.)

It is worth noting that many reported they had direct experiences that supported these negative concerns.

What were the worst or most outrageous things witnessed on social networking services?

Broadly speaking, the worst experiences reported by youth users of social networking services fell into the following categories:

- Verbal abuse - these experiences ranged from reports of "seeing rude words" and witnessing or being the subject of inappropriate comments to reports of targeted, consistent "nasty personal messages"

The findings detailed in this section represent the perspectives of CEOP Social Network Seminar participants. All quotations are directly attributable to the stakeholder group participants.

- Unwanted sexual advances - these ranged from requests for sex to reports of webcam-mediated indecent exposure, approaches from older men and offline meetings between youth and adults
- Exposure to unwanted information - youth users reported being sent viruses, being spammed, seeing rude pop-ups, "obscene images of girls and boys", etc.
- Impersonation of identity - "pretending to be a girl when you're a boy."

3.1.2 The impact of abuse

Who do young people feel are most at risk of abuse in online social networking fora?

Only one group of youth users suggested that they themselves could be at risk of abuse on social networking sites. Users mostly reported that those at risk of victimisation were "weak", "vulnerable" youth; primarily younger, inexperienced users. In particular, youth users reported that girls were at greater risk of victimisation in these fora.

Who else do young people feel can be harmed by misuse of social networking fora?

Youth groups also recognised that the family and friends (online and offline) of those abused on social networking fora, law enforcement and network administrators, can be adversely affected by abuse of social networking fora.

How do youth perceive this abuse happens?

Youth reported that most abuse is facilitated in the following ways:

- Potential abusers reading their profiles
- Abusers hacking into their accounts
- Through text messages, in chat rooms and via email
- Exploitation and blackmail using pictures
- Youth being careless with personal details (e.g. giving email addresses to strangers etc.)

What is the emotional impact of abuse in social networking fora?

The nature of the reported emotional impact depended on the type of abuse experienced by youth users. Specifically, feelings of hurt, shame, anxiety and depression were associated with sexual victimisation, annoyance with spamming, anger and powerlessness with hacking.

Would youth continue to use a site that did nothing to tackle reported problems?

Interestingly, most users reported that they would continue to use a social networking forum even if it did not deal with reports of abuse, unless the problem affected them personally and was of a very serious nature. Respondents attributed this condition to the many benefits of using these fora, the feelings of need and social dependency associated with interacting in social networking environments, the inconvenience of creating new profiles etc. Most users felt that they were sufficiently in control of their online environment to manage the situation themselves, e.g. that they could block the aggressor from contacting them, that they could discourage their friends from further using the site if need arose but expressed concerns about other young users.

3.1.3 Safety and reporting: What do young people feel can be done?

Where would youth users go if they needed help?

All respondent groups reported that they would turn to a friend (either online or offline) for help. Popular choices were also teachers and parents but some youth specifically reported that would not seek help from these groups if needed. These respondents felt that because "their knowledge is less than ours", teachers and parents would not be in a position to help if required. Many respondents also reported that they would tell the police (if offline and serious) and utilise online reporting facilities to seek help, namely CEOP, ThinkuKnow and report abuse links from other websites.

How do youth users think they can be helped? What do they think is being done to help them stay safe online?

The youth group were aware of the following online safety supports:

- Report abuse functions
- Moderation and surveillance (youth reported that police have unlimited access to all sites)
- Because parents have a better understanding of the best way to manage problem situations they can check how to report and to whom (e.g. hotlines, help-sites, police or social services, etc.).
- Use of online pop-ups and videos with safety messages to pre-empt abusive scenarios
- Block lists and banning or removing troublesome users
- Advertising and awareness-raising (posters, notices, ad campaigns, police talks, training programmes like ThinkuKnow, etc.)

What do youth think can be done to keep themselves and others safe?

Youth users perceive they can keep themselves safe by only talking to people they know and being careful to stay in "safe" Internet areas where they will not be targeted.

Notably, young users produced a greater series of recommendations for promoting the online safety of their peers than themselves. In particular, they made the following suggestions:

- Stay on the look out for "bad" or risky behaviour among online friends
- Explain to parents how SNS work
- Tell others of bad experiences on these services
- Inform friends about what it is to put themselves at risk online (e.g. giving out personal details like email and telephone numbers)

What measures do youth feel should be online to protect them?

The youth user group felt that the following online safety supports should be made available:

- Better presented terms and conditions of use on sites that will grab young people's attention and help minimise the risk of abuse
- A comprehensive system for identifying troublesome users and abusers
- Filtering for abusive language, images and other content
- Better detection, blocking and removal systems to identify and block abusers and "dangerous" social networking services
- Service requests and sign-up should be made more rigorous. More minimum required information should be sought by service providers to support these actions
- Parents should be educated
- PCs should be licensed
- A recognisable logo (like CEOP) should be placed on safe sites
- Better moderation and surveillance. Youth users want to feel that there is someone watching over them 24/7
- All complaints to social networking services should be dealt with
- Troublesome users or abusers should be identifiable to youth users who can then block them

3.2 Adult Stakeholder Group: Social networks - Understanding the Reality, Risks and Safeguarding Needs for Children

3.2.1 Understanding social networks

What did adult stakeholders know about social networking before the event?

Most reported that they knew very little, if anything, about these fora prior to attending the event; many had become aware of the phenomenon of social networking though the media attention it had received in preceding months. Adult knowledge of social networks was principally anecdotal; based on media reports and/or their children's use of social networks rather than on direct user experiences of these services. However, several contributors did report that they used them regularly for work and social reasons. Contributors who had user experience of social networking forums tended to endorse their value as educational support tools for children and specified that they had huge potential in this regard.

Many adult group participants shared the following perceptions:

- Online social networking is a "generational thing", a form of social interaction that many adults do not understand
- Real-time social interaction (e.g. going for a coffee) is more valuable than online social networking
- Social networking is a consequence of the fact that children are being socialised differently to their parent's generation (e.g. they now spend more time indoors and online)
- Social networks facilitate creative expression
- Parents do not know enough about social networking services
- Social networking services carry a lot of information that is inappropriate for children and aren't very secure

How did adults hear about social networking services?

Contributors reported that they had mainly heard about the sites through:

- Word of mouth
- Friends and colleagues
- The media
- Special interest or hobby groups

What did they find positive about social networking?

Adult stakeholders reported that social networking services have the following benefits:

- Social value - notably an ability to allow users to transcend traditional social barriers. Social networking services allow users to access large network of individuals, meet like-minded people easily and project themselves and experiment on a new social platform. They can also help individuals to overcome traditional social barriers (e.g. those living with a physical disability, etc.) and find old or lost friends
- Educational and informational value - social networking sites facilitate expedient access to information resources, allowing children and young people to share information, collaborate on school work, etc.
- Emotional value - adult groups reported that they enjoyed the affirmation they received from other social network users, feeling that "you are never an outcast"

What did they find negative about the social networking?

Contributors perceived the major negative aspects of social networking were as follows:

- Insufficient surveillance on sites
- Little guidance on social networking forums to assist those who are not conversant with these services
- Users can be exposed to unwanted information, e.g. banner ads, pop ups, very personal information
- Permanency of content once posted online. Theoretically this information is out there forever
- Authenticity - there is no way to verify information or identities on these sites
- Facilitate online bullying
- Has generated fear among users and non-users alike
- Stunts the real-time social development of youth; spending time online means that they are not being traditionally socialised

What did they believe online social networking services are all about?

Contributors attributed the following qualities to SNS:

- Fun - SNS are like a second "kids' bedroom" where they can invite friends in without parents knowing what they are doing
- Platform for self-expression; these services give children the opportunity to express themselves in traditional and new ways (e.g. impersonation)
- A place for children to meet: Many children are no longer as free to socialise as and where they would like to in the offline environment - this gives them an alternative social outlet
- Children are using this new environment to do the same things their parents used to do
- Important tool for rendering young people IT-literate

3.2.2 Identifying risk

What are the issues facing young people on social networking sites?

Generic:

- Lack of boundaries
- Lack of control
- Reduction in inhibitions
- Trickery
- Peer pressure
- Vulnerability; young people don't understand how personal information can be used against them
- Easier for offenders to make direct contact with children
- Differing levels of moral, sexual and physical development are not accounted for when interacting in this environment

Specific:

- Bullying (e.g. happy slapping, etc.)
- Racial abuse
- Viruses and malware (e.g. downloading Trojans)
- Underage distribution offences (underage sex and images - young users may be distributing indecent images of themselves to an older audience with deviant interests)
- Money scams
- I.D theft (through impostors, hackers etc.)
- Harassment
- Gaming addiction
- Compromises traditional literacy in young people (e.g. the use of SNS may have a negative impact on children's spelling)
- Access to inappropriate or illegal content
- Grooming (easier access to children)
- Sexual abuse

What are the biggest safeguarding concerns for adults regarding children's use of social networks?

- Hacking leading to grooming
- Teaching children to keep safe and be proactive
- Impersonation making grooming easier

3.2.3 Safeguarding youth users of social networks

Whose responsibility is it to safeguard children and overcome these issues?
Who are the stakeholders?

Respondents felt that everyone has a role to play; that there exists a "chain of combined responsibility" when safeguarding young social network users. This group expressed that the nature and scale of this responsibility varies according to the nature of the safeguarding issue.

Specifically, adult respondents felt that the following groups hold a stake with regard to the issue of safeguarding young social network users online:

- Parents
- Industry (especially product or service providers)
- Schools and educational authorities
- Children and young people (when they come of age)
- Community
- Government (e.g. Home Office Task Force)

- Friends or peers of young SNS users
- Commercial sponsors or advertisers
- Local authorities
- Children's services
- NGOs
- Law enforcement (CEOP and the VGT)
- International community

According to adult stakeholders, what were the biggest improvements that need to be made to safeguard children?

- Creation of a safe area or clean zone ("a defended area") where parents know it is safe for their children to engage in social networking activity
- Finding a happy medium between free speech and safeguarding children.
- Effective network regulation and moderation. This would help build more secure communities; it could also be used to build knowledge about abusive behaviour and possible safeguarding interventions
- Sustained media awareness and responsible media reporting to deliver accurate information to the public about SNS
- Education (for children and parents): This would be both preventative and empowering. These groups felt that parents need to know more about social networking and the role they can play in safeguarding young SNS users. Similarly, this group advocated that children and young people should be helped to better understand the problems that may arise with use of SNS, the potential implications of risky online behaviour, in addition to any positive steps they can take should they encounter any problems on these services.
- Creation of national and international policy and legislation that will tackle the abuse of children and young people in these forums and render service providers accountable for implementing counter-measures (e.g. through penalties for non-compliance).
- Improved communication between safeguarding stakeholder agencies (service providers, law enforcement, schools, etc.)

According to adult stakeholder groups, what measures currently exist to ensure a safe on-line environment for young people?

- Systems for reporting abuse or concerns
- Education and awareness raising
- Industry partnership - e.g. sharing IP addresses, security tools
- Cross-sector partnerships
- Moderation - e.g. content filtering and surveillance activity
- Authentication of user identities
- Acceptable use policies
- Industry standards - e.g. code of practice for users, service and content providers
- Legislation and consequence for industry
- Law enforcement presence (e.g. covert Internet investigators)

How should stakeholders work together to safeguard children?
What more could be done to promote working together?

Several key actions were suggested across adult stakeholder groups. These are as follows:

- E-safety groups like the Home Office Task Force on Social Network Services should be convened. These groups should represent all stakeholders. This is an invaluable forum for the development and exchange of best safeguarding practice and should be used to facilitate broader engagement with parents and children.
- A partnership of stakeholders (like that suggested above) should develop a code of conduct for users and providers of social networking sites
- This group felt that service providers are critically placed in terms of safeguarding both young users and their own commercial reputation and consequently, have a moral and corporate social responsibility to intervene. Many of the groups advocated that social network service providers should sign up to a code of conduct that is

externally moderated by another safeguarding stakeholder (e.g. government or law enforcement). However, they stressed that this could not be another self-regulatory scenario with generic, inconsequential standards.

- Compliance with these codes of conduct should be compulsory for service providers. Penalties like fines and "naming and shaming" exercises if contravened.
- E-safety should be a part of the national curriculum (ideally on the PSHE programme) with a view to making this a compulsory subject
- Educate parents - children should teach parents about social networking
- Government-sponsored media campaign to educate on the positives as well as the negatives of social networking
- Identify and co-ordinate best practice across agencies. However, participants felt that leadership is essential here; one figurehead agency should lead and co-ordinate across agencies
- Government should provide funding for the issue and oversee the development of a ten year plan with short-term, medium term and long-term interventions
- Measuring the success of these interventions; a reduction in the incidence of abuse of young people in social networking forums should be the key performance indicator

The sections that follow set out a series of initial proposals for safeguarding youth on social network services and target government departments, law enforcement, SNS and other media providers as well as CEOP. In accordance with its partnership ethos, CEOP will continue to work closely with the various sectors to action these recommendations. These have been informed by the major findings of the seminars.

CEOP's education and awareness initiative - ThinkUKnow

This initiative should be used as a vehicle to:

- *Educate* children in schools about safety in online social networking environments and share knowledge of new and emerging threats to young social network users as this is made available to CEOP (through analysis of public reports, force referrals etc., liaison with SNS and other media providers about new products or services etc.)
- *Collect data* from children about new patterns of social software usage, social networking trends, risk factors and harmful behaviours, suggested interventions etc.

Developing "online social responsibility" among youth social network users

One of the key findings of the social networking seminars was that children perceived more risks to others than they did to themselves in social networking environments. Notwithstanding the need to highlight to young people the ways in which they themselves may become personally vulnerable when using social networks, we can harness this knowledge and use it to serve another safeguarding function.

This finding indicates a natural propensity among youth users to look out for the safety of members of their online peer group. Youth should be encouraged to be on the lookout for the safety of their online peers and report on their behalf where they perceive a peer has become a target of abuse *or* is engaging in behaviour that puts them at risk in the online environment. To achieve this, we need to look at ways of fostering a sense of "Online social responsibility" among young users of social networks. Some suggested ways of generating this social responsibility are as follows:

Education:
One potential way of promoting this is to incorporate a programme of study on the topic of "Online citizenship and social responsibility," into the schools curriculum. As a minimum interim measure this topic should be introduced as a discussion theme in the ThinkUKnow education and awareness programme.

By Design:
SNS providers already custom-design certain social network functionalities to promote social engagement within online social networks and establish "community feeling" among members (Wildbit, 2005). This design process should be tailored to promote feelings of concern and responsibility among younger social network members for the safety and welfare for other users and expedite reporting processes as appropriate.

Engage children more directly with the development of safeguarding initiatives for social networks

This could be achieved by using CEOP's Young People's Panel and feedback captured from children and young people through the ThinkUKnow programme as a vehicle to inform the development good practice guidance for SNS providers and measure the effectiveness of these practices as they are developed and instituted going forward.

"Informed Choice" - keeping young SNS users in the know

Youth participants expressed concern that they did not know enough about specific types of behaviour and other risk factors that can be harmful to themselves and/or others in the social networking environment. Moreover, they affirmed that they wanted to be further educated about the nature of any threat to their online safety, the consequences of their online actions, and the pitfalls of engaging in risky behaviour. Older youth stipulated that they should be afforded the opportunity to make informed decisions should they select to engage in risky behaviour; but equally that they had the right to know what harm could potentially come about as a consequence of online "misconduct." To effect this they suggested that terms and conditions section and advice pages on social networking services should contain more information on this topic, presented in a "child-friendly" manner, or links to same, especially on sites with high proportions of children and young people registered as users.

Utilise CEOP's safer by design function

Industry and CEOP should work together to identify new social networking functionalities and other technologies that that could facilitate or co-facilitate harm to children in the social networking environment (e.g. live blogging software, Voice Over IP technologies, webcams, new chat or messaging services etc.).

Equally, CEOP should feedback to industry on points of design and security within social networking forums that are:

- Being exploited by offenders to target children
- Used by children to engage in risky or harmful behaviours.

Keep sight of new online forums and other technologies that facilitate abuse

Social networking forums are but one of a series of tools that can place children at risk of sexual exploitation and other forms of online abuse. Safeguarding agents should not limit the focus of safeguarding interventions to one forum. With increasing popularity of new forms of ICT and converging media (e.g. live blogging services; voice over IP, live messenger, SNS via mobile etc.), an over-emphasis on the pitfalls of social networking services themselves (especially in the delivery of education programmes etc.) could place children at risk in other forums by blind-sighting them to the potential threats of new and emerging technologies.

Further research

At present, much of our knowledge on the topic of safeguarding children in social networks is anecdotal rather than empirically-based. Safeguarding interventions will only be effective if they are grounded in a real and evidenced knowledge base - this requires further research to fill existing knowledge gaps on risk factors and possible interventions in social networking environments.

Strategic threat assessment of social networking trends

CEOP should conduct a strategic threat assessment of online forums to establish where children are experiencing the most problems and interventions would be best targeted. This assessment should be informed by online reports, feedback from CEOP's ThinkUKnow initiative, intelligence from forces on Internet-related offending patterns, industry input, further research etc. to generate concrete information on the *incidence, location and nature* of online episodes (e.g. bullying, harassment, solicitations etc.) particularly in the social networking environment.

The outcomes of this assessment should be shared with stakeholders to support the development of targeted safeguarding interventions in a way that optimises available resources.

Victim profiling

Youth participants reported that those young people most at risk of abuse in social networking environments are "vulnerable" individuals whose online identities and behaviour make them appear "weak," and of "low self-esteem." We also know that the content of user profiles dramatically affects the social behaviours, norms and cultures of online environments, most notably at the expense of less privileged groups, like younger users (Boyd, 2001). This provides a rationale for further research in the area of "victim profiling." This would allow safeguarding agents to determine whether there are particular online profiles (i.e. online profiles that are more attractive targets to adults with a sexual interest in children) or specific categories of behaviour that place young people at risk in social networking environments. This would afford industry, child protection agencies, educational authorities etc. the opportunity to focus safeguarding interventions more effectively (e.g. targeting tailored safety messages at particular groups of "at risk" social network users).

Link to social network safeguarding initiatives in other jurisdictions

There should be consistent liaison on an international level between social networking task force initiatives to share and develop good practice, identify trends of social network usage country-to-country, and detect new and emerging problematic online behaviours in particular countries which may ultimately become more widespread. This reciprocal liaison would facilitate the design and institution of pre-emptive harm reducing interventions within the UK and other participating countries.

Mobilise parents and educators as safeguarding agents

Participants reported that extensive media coverage of the threats to child safety posed by social networking forums have generated uncertainty and confusion among parents and caregivers unfamiliar with SNS or the use of the Internet more generally. The effect of this is that these groups feel overexposed to dangers of social networking, badly-versed on the finer points of safeguarding their children in the online environment and frequently powerless to intervene.

Clearly, there is a need for a broader programme of education and awareness-raising among this population. "As with all other Internet safety issues, the single biggest positive impact on children's online behaviour is brought about by active engagement by parents in the online activities of their children," (Morrisey, 2006). In particular, many participants (being parents themselves) suggested it would be helpful if, as an interim measure, there was a parental advice file visibly placed on all social networking services to inform them about steps they can take to safeguard their children online, the risks they may face, how and where to report a problem, links to further learning resources etc.

5. CEOP and SNS: Next Steps

In accordance with the recommendations for safeguarding action that emerged from the stakeholder groups, CEOP has undertaken to:

Conduct further research

Notwithstanding the value of the initial insights provided by CEOP's Social Networking Seminar participants, the stakeholder sample surveyed was small. For this reason, it is difficult to ascertain whether, and to what extent, these outcomes are reflective of the experiences of the broader population of SNS users. Further research is needed to build upon these insights and develop a reliable understanding of the safeguarding challenges posed by social networking forums, nationally and internationally. Consequently, CEOP is collaborating on a number of research initiatives to progress this agenda. This will help fill the knowledge gaps that exist around risk factors and possible interventions on SNS and ultimately, make these online environments safer by design.

Advance the activity of ThinkuKnow: CEOP's education initiative

Under the auspices of its education and awareness initiative ThinkuKnow, CEOP will continue to educate children and young people about safety in online social networking environments and share knowledge of new and emerging threats to young social network users. This initiative will also facilitate the collection of data from young people about their online activities on an unprecedented scale. It is envisaged that this feedback will inform future programmes of research on the social networking phenomenon.

Progress CEOP's safer by design initiative

CEOP will continue to work closely with SNS and other media providers to make their online social networking environments safer by design for children and young people (e.g. by placing its "Report Abuse" mechanism in a prominent area on their sites to enhance public reporting capability). This programme of work will also be heavily informed by feedback about social network usage from the ThinkuKnow programme, reports of abuse received by CEOP from the public and the input of CEOP's Young People's panel.

Develop good practice guidance for social network service providers

CEOP will continue to play an active role in the development of good practice guidance for social network service providers nationally and internationally.

Continue monitoring SNS forums

CEOP will continue to monitor and feedback to SNS and relevant media providers on the nature, scale and location of the reports it receives from children about problems they experience on social networking forums.

Develop future education and awareness raising initiatives

CEOP will continue to expand its programme of work around education and public awareness. This will include the development a series of educational resources for parents and primary age children that will promote safety in SNS and other online environments and enhance their capacity to report abuse and child welfare issues to safeguarding authorities.

American Library Association, (2006) cited in Out-law.com, (2006). *US Social Networking ban could unfairly block some sites.* The Register, [Online]. Available from: http://www.theregister.co.uk/2006/08/01/social_networking_ban/ [Accessed 12 August 2006]

Anderson, G. (2006). The CEOP Social Networking Seminar Series. *Using Social Networks.* 17 July 2006. Child Exploitation and Online Protection Centre, London.

Arnett, J.J. (1999). Adolescent storm and stress. *American Psychologist*, 54(5), pp.317-326.

Boeck, T., Fleming, J. and Kemshall, H. (2006). *Young People and Social Capital.* [Online]. Available from: http://www.pcrrd.group.shef.ac.uk/reports/project_4.pdf [Accessed 5 November 2006]

Boyd, D. (2001). Sexualities, Medias, Technologies. *Sexing the Internet: Reflections on the role of identification in online communities.* 21-22 June 2001. University of Surrey. [Online]. Available from: http://www.danah.org/papers/SexingTheInternet.conference.pdf [Accessed 14 November 2006]

CEOP, (2006). *How we do it.* Child Exploitation and Online Protection Centre. [Online]. Available from: http://www.ceop.gov.uk/how_we_do_it.html/ [Accessed 15 October 2006]

Children Act 1989. London: HMSO

Donath, J. and Boyd, D. (2004). Public displays of connection. *BT technology journal* 22(4), pp.71-82.

Durkin, K.F. and Bryant, C.D., (1995). Log on to sex: Some notes on the carnal computer and erotic cyberspace as an emerging research frontier. *Deviant Behaviour: An Interdisciplinary Journal*, 16, pp.179-200.

Faultline, (2006). *MySpace music deal poses multiple threats.* The Register, [Online]. Available from: http://www.theregister.co.uk/2006/09/08/myspace_threatens_record_labels/ [Accessed 20 November 2006]

Goodchild, S. and Owen, J., (2006). Children and the Net: An IoS Special Investigation. *The Independent on Sunday*, 6 August. pp.1-2, 6-9.

Granneman, S. (2006). *MySpace, a place without MyParents.* The Register, [Online]. Available from: http://www.theregister.co.uk/2006/07/03/myspace_parenting/ [Accessed 12 August 2006]

Hill, R.A. and Dunbar, R.I.M., (2003). Social Network size in humans. *Human Nature*, 14(1), pp.53-72.

Morrisey, J. (2006). E-society - Young people social networking online. *The Irish Independent*, 18 April. [Online]. Available from: http://www.ncte.ie/AbouttheNCTE/Publications/Articles/esociety/ [Accessed 15 November 2006]

Out-law.com, (2006). *US Social Networking ban could unfairly block some sites.* The Register, [Online].

References

Available from: http://www.theregister.co.uk/2006/08/01/social_networking_ban/ [Accessed 12 August 2006]

Roush, W. (2006). *The moral panic over social networking sites.* Technology Review, [Online]. Available from: http://www.technologyreview.com/read_article.aspx?id=17266&ch=infotech [Accessed 19 November 2006]

Smith. M. (1992). *"Voices from the WELL: The Logic of the Virtual Commons"* [Online]. Available from: http://www.sscnet.ucla.edu/soc/csoc/papers/voices/Voices.htm/ [Accessed September 12 2006]

Wildbit, (2005). *Social Networks Research Report.* [Online]. Available from: http://tidbit.wildbit.com [Accessed 3 August 2006]

Working Together to Safeguard Children 2006. London: HMSO

Yoke, B. (2006). *Testimony before the subcommittee on telecommunications and the Internet of the committee on energy and commerce.* [Online]. Available from :http://www.ala.org/ala/washoff/WOissues/techinttele/DOPA_testimony.pdf [Accessed November 1 2006]