



European Commission Consultation on Child Safety and Mobile Phone Services

Response from the UK Children's Charities Coalition on Internet Safety (CHIS)

October 2006

Introduction

The Children's Charities Coalition on Internet Safety (CHIS) brings together the UK's major child welfare and child protection organizations to focus on promoting children's interests in the online environment.

CHIS welcomes this consultation from the European Commission as a useful contribution to protecting children from the risks associated with the use of mobile phones. This is a crucial area for child protection in light of the widespread and increasing use of mobile phones by children across Europe, and fast-developing new technologies in this area which pose new risks as well as creating new opportunities.

CHIS believes the EU can support efforts in this area in particular by coordinating the exchange of experience and best practice, as well as helping to promote approaches which best protect children from identified risks.

The announcement of the EU Strategy on the Rights of the Child, outlined in a Commission Communication of July 2006, as well as the UN Study on Violence Against Children which was launched on 11th October 2006, gives this work particular impetus.

Questionnaire on child safety and mobile phone services

Risks.

1) Can you provide the Commission's services with figures and examples on risks raised by the use of mobile phones by children and young people?

Bullying. There is a range of recent research which demonstrates the risks posed by mobile phone use in the UK and in particular the substantial risks of bullying via mobile phones (NCH, 2006; Livingstone, 2005). Research carried out last year by NCH and Tesco Mobile reported that 14% of children had

been bullied through their mobile phone and that 10 percent had been photographed on their mobile in a way that makes them feel uncomfortable. A recent survey by the Anti Bullying Alliance showed that bullying using phone picture and video clips has more impact on the victim and is more traumatic than traditional forms of bullying.

Exposure to sexual predators. We are also aware from other sources of the risks of children being exposed to sexual predators via adult chat or other online services. For example, calls to the NSPCC's helpline ChildLine demonstrate the ways in which mobile phones have become an additional medium through which children can be abused and made to feel unsafe.

"Jenny gave her mobile to someone she met in chatrooms. The person said they were 15 and she believed them. Now she feels they are much older. She is receiving texts and calls from this person and said she is becoming concerned". Call to ChildLine

Access to inappropriate content and other pressures. There are also concerns about children's access to age-inappropriate content which may cause them distress, as well as children's vulnerability to fraud or unfair commercial pressures.

"Shown an image of someone being beheaded on a mobile phone in February. Can't get it out of her head & frightened she will dream of it happening to her. Fears feeling the pain of having her head cut off. Dreamt of being stabbed & felt the pain then. Mum suggest she look at other images." ChildLine Counsellor

Location services. The Children's Charities Coalition on Internet Safety has also recently become concerned about the emergence of location based services attached to mobile phones on the UK domestic market. These are services which make it possible to track the location of the person carrying a mobile phone.

These are clearly a source of risk, both if they are marketed inappropriately to suggest that they enhance a child safety, and if location data falls into the hands of potential predators. Whilst they may have a superficial attraction – i.e. being marketed to suggest that children can be traced by their parents, the reality is that they may make children less safe, enabling for example abusers to track children. These services in any case only mean that the phone can be tracked – it will not always tell you about the location of the child.

We have recently called for a licensing regime to be introduced for any company that plans to use or promote these services.

Health risks. Although it is outside the scope of this consultation it is important to note that there remains a great deal of public concern about the health risks

to children associated with the use of mobiles, and those associated with the placing of the radio masts necessary to create and maintain a network.

2) Do you see specific risks associated with the use of pre-paid cards, which ones?

Lack of supervision. Where children are very young it would be preferable if there was the opportunity for parents to supervise or guide and influence their children's mobile phone use more closely.

Most children in the UK who own mobile phones use prepayment methods to pay for them. This means that an itemised bill is never produced or sent to the household in which the child is living. As a consequence, there is no scope for parents to monitor the different services that children are using on their mobile phones. The prepayment method used in the UK also makes it possible for third parties to buy credits for a child, perhaps without their parents' knowledge or approval. In some cases this has been done to facilitate secretive contacts between a child and a sexual predator.

Expense. It is also important to note that in the UK, prepayment is a more expensive way of making calls than account-based phones. Given that prepaid phones are used predominantly by children, or by poorer adults who might have difficulty obtaining credit clearance for an account, this can push these families further into debt.

Regulatory framework

Please identify which of the above risks are not covered by the current national regulatory, co- and self-regulatory frameworks.

Bullying is covered by the criminal law, the civil law and by the mobile phone companies' contracts with their customers. The other issues referred to above are covered by other codes, such as the ICSTIS¹ code and the Content Code.

Location services are also governed by a self-regulatory code of practice. However, there is serious doubt about its adequacy as other location technologies become available which are not covered by the code e.g. GPS.

Other technologies, more generally associated with surveillance techniques or practices, are increasingly being integrated into or packaged with mobile phones (such as remote listening or remote viewing, or both). When these are also linked to location services these will gradually change the character of the device itself i.e. the traditional telephone element of the device will be less important than its uses for surveillance.

¹ ICSTIS is the UK's regulator for premium-rate content

The economic aspect of prepayment, including the ability of third parties to buy credits, is not covered by any regulations or code in the UK.

Do you think the current balance between regulation / co-regulation and self-regulation is the right one?

Overall, within the UK the balance of regulation and self-regulation has to date been broadly satisfactory.

The exception to this is, as outlined above, the issues mentioned in relation to location services. This issue must be swiftly and satisfactorily resolved in order to ensure the overall balance remains successful. It may be that as an ever-wider range of surveillance technology becomes available on the mass market, greater Government action is needed.

Technical solutions

5) What measures do you recommend in the different areas described below, and why?

5a) Classification of commercial content

We believe that the material supplied by the networks themselves should be classified in such a way as to allow parents to predetermine whether or not it is suitable for their children. In terms of technical solutions we are broadly satisfied with the progress that has been made in the UK so far.

5b) Opt-in/Opt-out

Should the opt-in (whereby the user has to explicitly request access to adult content rather by accessing it by default) approach be applied in all EU countries?

We favour opt-in as the best approach to protect children. This is the best way of dealing with inertia or ignorance of the risks, as parents have to explicitly request access to adult content.

5c) Age verification

Should Mobile network operators implement face to face identity check to determine the age of the user? Should this process also be applied when a customer buys a pre-paid card?

A crucial element of child protection in the mobile environment is ensuring thorough and consistent age verification to ensure that children cannot access age inappropriate material.

We favour as strong and as effective a system of age verification as it is possible to have. Face to face, with associated documentary evidence, would certainly be one way of doing it but we have no reason to believe the UK's current system is not working satisfactorily. Europe wide more countries have ID cards, some with an online component already built in so it would be a great deal easier to implement an online system of age verification.

In the UK the age verification system allows the networks to determine whether or not a handset user is 18 or above. This works through the use of credit cards or similar financial instruments. Yet under the ICSTIS regulatory code it is possible for some premium rate services to be developed and marketed to persons under the age of 16, and to persons who are aged 16 or 17. There is as yet no reliable way in which either age group could be verified within the UK, and neither does it seem to be possible to exclude persons who do not fit these age categories from using the service anyway.

In our view the age verification system used by the network operators ought to be fully aligned with the system used to market premium rate services. We are not opposed to the networks or other commercial providers developing systems which will allow greater granularity in terms of users' age. However, there needs to be evidence that any alternative systems work reliably and effectively.

5d) Filtering and blocking systems.

Should filtering systems be installed by default when the subscription allows Internet access?

Filtering and blocking systems should be installed by default. If controls are placed on the networks' own content it would be odd and confusing if, as near as possible, a similar standard was not applied to other accessible content and services. We believe that this is the only way to consistently protect children from harmful content. This is especially the case given that there is much less supervision of children's mobile phone by parents compared to children's computer use.

5e) Chat rooms

Should chat rooms accessible by children be moderated (in an automatic way or by a person)?

Wherever possible chat rooms should be moderated by a person. Automated systems have a place but they are better as a support to a human system. On their own automated systems are not yet sophisticated enough to be sufficiently reliable.

According to the UK Government's (Home Office) good practice guidelines on technical moderation, technical moderation on its own can not offer the same level of online child protection as human moderation, to combat the sexual grooming of children. These guidelines explain that technical moderation can be outwitted by the creative use of combinations of numbers, letters and punctuation marks, and that software based solutions find it very difficult to pick up and interpret the context of personal communication, for example, the subtleties of grooming behaviour.

5f) Raising awareness among parents and children.

It is essential that the networks themselves promote safety and awareness messages to parents and children directly, and other relevant actors should also play their part. Members of CHIS are actively involved in promoting safety messages for example using their websites to raise awareness.

It is very important to consult children and young people themselves about safety. Children are often far more skilled and competent users of mobile technology than their parents. Research published a couple of months ago by NCH reveals a substantial gap between what children know and what their parents know. For example, 69% of parents admit that they know less about mobile phones than their children, with 43% of parents not knowing what WAP is and more than half not knowing what 3G is (Get I.T Safe. Children, parents and technology survey 2006).

5g) Dedicated mobile phone packs for children, for which age group?

There may be a case for simpler or restricted function phones which are designed for younger children, but starting at about the age of 10 these will rapidly lose their appeal. At the same time, this may raise public concerns about inappropriate marketing to children.

European solutions

Among the measures listed above which ones would it be useful to elaborate at European level? For which ones would it be useful to discuss/exchange best practices at European level?

We believe that the European Union can play a role in improving child safety in the use of mobile phone services, particularly in relation to the aspects outlined below.

CHIS emphasises that any of these initiatives must be developed with the full participation of all relevant stakeholders, including NGOs specialising in child protection, and children and young people themselves.

- Location Services: Interpretation of Data Protection Rules

CHIS believes that a priority for work at European level relates to the risks emerging from location services, an issue relying heavily on data protection considerations. As noted above, new developments in location services raise significant issues for child safety as these could be used for inappropriate purposes.

The EU's 'ePrivacy' Directive² provides that location data may be used, but only with the consent of the subscriber or user. However, the way this consent is obtained by different companies varies considerably, with some approaches providing better protection for children than others.

² DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

For example, at least one French location service provider operating in the UK interprets the data protection regulations differently from their UK competitors. After *each* location request the French company sends a text to the handset of the “locatee” informing him or her that their location data has just been provided to a locator. We think this approach is far superior and it minimises the risk of misuse in a way the system commonly used in the UK does not.

These differing approaches stem from varying transpositions of EU data protection rules (the so-called ePrivacy Directive) into national law, and different ways in which these rules are interpreted.

In the UK for example, the *Privacy and Electronic Communication (EC Directive) Regulations 2003* which transpose the ePrivacy Directive appear to be clear that “*in respect of each connection to the public electronic communications network in question or each transmission of a communication, be given the opportunity to withdraw such consent, using a simple means and free of charge*”. However in reality there are problems in the way this is being interpreted by location service providers.

We believe the Commission could play a role in promoting best practice in relation to location services for the purposes of child protection. For example, information is needed about how, in different Member States, the relevant articles of the ePrivacy Directive have been transposed into national law, and how in their turn location service providers and the mobile phone networks are interpreting the relevant regulations. This could usefully lead to guidelines for good practice in this area, as well as better mainstreaming of child protection concerns in relevant EU legislation.

A licensing regime for companies using or promoting location services, such as that CHIS is calling for in the UK, could be explored as a possible EU-wide approach.

Furthermore, given the likelihood of these services being marketed EU-wide, we believe that there is an argument for the European Commission to consider a stronger (possibly regulatory) role in ensuring that these are not marketed to parents and children as safety tools.

- Child safety in handset manufacturing standards

One way of protecting children is through building handsets in ways which maximise safety. Up to now, work with private sector companies in this area at European level has been primarily with mobile phone network operators rather than handset manufacturers.

CHIS believes it would be useful for the Commission to bring together the major handset manufacturers to discuss with them ways in which, at the factory, components can be built in to handsets which will help minimise risks and maximise safety. In the context of the internal market there may be some scope for the Commission to assist the development of common standards for mobile-based filtering products and classification systems.

For further information contact:

John Carr, NCH
+44207704 7159

Zoe Hilton, NSPCC
+44207825 2500