Public consultation response

Age Verification, Cross Media Rating and Classification,

Online Social Networking

http://ec.europa.eu/information_society/activities/sip/public_consultati
on/index_en.htm

EU Kids Online

www.eukidsonline.net

July 2008

Questionnaire 1: *Cross Media Rating*

We agree that, given the current trend towards platform and media convergence, the feasibility of cross media rating systems needs urgent discussion.

1. Of which media rating systems are you aware in your country. Has there been an attempt to implement a cross-media rating system? If yes, what are the positive outcomes of it and its success factors? If no, what could be used as a starting point towards a cross media rating system?

For console gaming, Iceland has implemented the PEGI system and this year the same system will be applied to DVD/VIDEO/TV. The system has been promoted by SAFT, the Safer Internet Action node in Iceland, in collaboration with the industry. The system is well known by consumers and used by the industry.

The UK has rejected a uniform content-rating system to date, recognising the different relationships that viewers have with content through various delivery platforms. Ofcom has suggested that the possibility of a cross-media common labelling system should be considered, treating as part of its media literacy remit investigation into the feasibility of a common labelling scheme for content across all broadcast and interactive platforms.

2. What are the main obstacles moving towards a pan-European cross media rating system?

We identify no serious obstacles in principle and, some hold, in practice.

3. What role should the different stakeholders play (industry, public bodies, etc.), towards implementing a pan-European cross media rating system?

Industry should accept and promote the system in collaboration with relevant public and private bodies. The legal environment should be clear and be able to address issues raised quickly.

4. Are you aware of relevant research, pilot projects, or national cross media rating initiatives? If published online, please provide us with the relevant URL.

Millwood Hargrave and Livingstone (in press) note, following an extensive review of the international research literature, that:

> "In a context of converging technologies and media content, we are particularly concerned at the lack of evidence providing a secure basis for making comparisons across media platforms. Audits of the media used by different segments of the population provide cross-media information regarding both use and skills for a range of platforms but there is not sufficient research about attitudes to, or the influences of, cross-media content. We note that comparisons across different media regarding the nature or size of effects are difficult in methodological terms. However, such research could and should be attempted."

Questionnaire 2: *Age Verification*

1. Which age verification systems are you aware of? In which domains are they being used?

Apart from those that make use of Credit Card numbers and CVV codes, we are not aware of any age verification systems.

The Icelandic Safer Internet Action node is currently preparing a pilot project, in collaboration with the Office of Post and Telecommunication and the Ministry of Financial Affairs, on the subject - with main focus on age verification systems for children. The pilot is a part of a bigger EU funded project - where Iceland is in charge of a pilot project concerning children's use and safety online. On the website www.skilriki.is we're developing the first-step platform, with chat rooms for certain age groups. The platform uses Debit cards issued to the user by the government or user's bank. A USB card/slot is connected to the users PC and the PIN code is used for verification. The current pilot was started some two years ago but the current EU project had a kick-off meeting last June.

2. Do you think that these systems are efficient? If yes, please state why. If no, why do you think they are unsatisfactory?

Janet Wolak's survey (NCMEC) has some detailed questions following up with 'victims' of online grooming, questions that be asked in European surveys and have not done thus far. On this basis, she and David Finkelhor have made the much publicised claim that children know they are going to meet adults for sex, in other words, there is no age deception on their part (of course, the groomer knows that the victim is a child). Setting aside the question of whether a legal minor can be held responsible for such knowledge, I would observe that, in addition lacking such data in Europe, if may be that matters in Europe are different. American teens are now long familiar with the internet, but in Europe, for many it is new, and games with identity (age, sexuality, etc) may be going on that mean children here can still be deceived – thinking they are meeting a child when really it is an adult.

Age-verification technology can presumably only be implemented if all parents are required to vouch for their child's internet access (a solution which is too restrictive for children) or (2) if we insist on age verification for all (a solution which is too restrictive for adults). So even if technically feasible, it is not socially feasible. The same is likely to apply to systems (age-related filtering, for example) that rely on parents and children logging onto the same household computer via personally passwords so as to permit age-appropriate activities only - this isn't how families work, for they share passwords and, if blocked using one, will tend to leave the computer on and open-access on whoever's password is the least restrictive. A password system, for all but the most conscientious (and, probably, the youngest children), thus seems as implausible as a system

that relies on children's truthful self-reporting of their age (something that the number of under 13's using social networking services quickly undermines).

3. Are you aware of legal requirements in your country for providers of online services to verify the age of their visitors/customers?

In so far as we have replies from different countries, the answer is generally 'no'.

In the UK, the Home Office Taskforce on Child Protection on the Internet has published guidance for social networking, aimed at parents and children, and the providers of social networking sites.[i] It makes several recommendations including those relating to safety information, editorial responsibility (including appropriate advertising), registration, user profile and associated controls, identity authentication and age verification.

4. Are you aware of relevant research, pilot projects or national initiatives towards age verification on the internet? If published online, please provide us with the relevant URL.

Unfortunately not.

Questionnaire 3: *Online Social Networking*

1. What risks are minors most likely to encounter on SNSs? Are you aware of relevant research or statistics? If published online please provide us with the relevant URL.

Any SNS user in general and youngsters in particular are most likely to encounter the following risks:
- Loss of privacy
- Sexual harassment online
- Sexual harassment offline when youngster arrange a meeting with online friend
- Loss of high security level in physical life, e.g. by giving out information about hometown, high school, home address, phone numbers, personal picture
- Receiving embarrassing content, such as sexual related, violent, xenophobic pictures, videos etc of unknown individuals or even of (close) friends
- Viewing embarrassing content on friends' profiles
- Becoming a victim of bullying
- Being drawn into becoming a perpetrator of bullying
- Online fraud, e.g. reconstruction of users' social security number using information often found in profiles, such as hometown and date of birth
- Collection and storage of personal and private data/information used by corporations for advertisement and consumption reasons, e.g. by revealing information about favourite books, movies, music, TV shows, interests, hence, being bombarded with advertisements and special offers

Research:

As we have already noted in responding to the recent EC consultation on Social Networking Sites, there are only a limited number of European surveys with statistics relating to children's general usage and experience of social networking sites: e.g. Larsen (forthcoming) in Denmark, Anchor Ireland (2007) in Ireland and Ofcom (2008) in the UK. Many surveys do not report the age of the user or survey only adults.

The picture can be supplemented by other quantitative studies focusing on specific aspects e.g. Valkenburg, et al (2005) in the Netherlands (looking at self-esteem) and Taraszow et al (forthcoming) in Cyprus (looking at personal information online). In addition there are the various qualitative studies, such as Livingstone (2008) in the UK (on styles and privacy), Fluckinger (2007) in France (on the emergence of peer networks), Siibak (2008) in Estonia (on content creation) as broader studies that include data on the use of social networking sites, such as Aas-Hansen (2007) in Norway, Mascheroni et al (2007) in Italy and the TIRO project (forthcoming) in Belgium.

To put risks into context, it should be noted that the main activity of young people on social networking sites is building their own profiles (presenting themselves to peers), visiting other young people's profiles (to see how others present themselves) and commenting on profiles, photos etc. (which in the academic literature we often refer to as building social capital and which is a form of gift-giving that is usually reciprocated). To take the positives of social networking sites, studies have shown how this is also important for self-confidence, self-identity and self-esteem (e.g. Valkenburg et al, 2005).

Hence, many of the profiles are authentic, even if young people are presenting themselves in a good light. Because there is an element of trust in this process, Danish research has pointed out young people can be very critical of fake profiles (Larsen, (forthcoming) Denmark). That is quite positive as regards fears about grooming. That said, some young people themselves create fake profiles (Livingstone, 2008; Ofcom, 2008). Expressed in a positive light this has been called 'identity play', but looked at from a different perspective, if it misleads peers and creates peer problems it can be viewed as a risk related to young people's own conduct.

To put concerns about negative online communications of SNSs into context, various national studies stress just how much communication is positive - see Larsen (forthcoming), Fluckinger (2007), Ofcom (2008), Valkenburg, et al (2005), Mascheroni et al (2007), Siibak (2008). Only a minority of actions on SNS were 'negative'. While this may include 'cyberbullying', much of it seems to arise from arguments offline between peers, or between ex-boy/girlfriends, young people teasing each other by posting 'embarrassing' pictures, etc (Haddon and Vincent, 2007). While we have studies of online bullying in general , we do not yet have specific material relating to this phenomenon on SNSs.

As regards 'stranger danger', from the countries where we have research, most social networking sites are used by youth to communicate with known people, usually peers (e.g. Aas-Hansen (2007)in Norway, Larsen (forthcoming)in Denmark, OfCom (2008) in the UK, Siibak (2008)in Estonia and Anchor Ireland (2007) in Irleand). For example, in the UK 92% of young people using SNSs said that they mainly used sites to stay in touch 'with friends and family they see a lot' (OfCom, 2008).

However, it is worth drawing attention to one particular practice, that of youth competing to add friends to the friends list as a signal to others of their own popularity. In their enthusiasm to do this the result is that young people have sometimes added 'friends' to their lists who they have not met offline e.g. (Anchor Ireland (2007), UK OfCom (2008)). Even if the privacy settings are set to private, this can mean that these 'friends', who are in effect strangers, have access to the profiles of young people's networks.

Although not the main goal, some young people did use SNSs to make new friends: e.g. 12% of youth in an Irish survey said this was their main aim (Anchor Ireland, (2007). That Irish study also noted that 20% of 12-14 year olds said this as the main aim vs. 9% of the 15-17 year olds, presumably because the older youth are by now more likely to have established a network of friends and are less likely to try to expand it. But it does mean that if there is an issue of stranger danger it may be for younger teens.

Still on the theme of contact with strangers, in a UK study 17% of youth 'talk to people I don't know' on SNS (Ofcom, 2007). We have no figures for actually meeting strangers but the Ofcom qualitative study noted that some young people at least mitigated risks by meeting people they had contacted online in public places and bringing friends. That report noted that from the young person's perspective, this whole process of moving from online to offline could constitute 'free online dating'.

Turning to privacy issues, it has been noted in US material that young people spend a considerable amount of time in adult supervised spaces (school, many parts of the home, after school activities, etc) and this may be increasing (Boyd, 2006). On the other hand, young people value spaces for unmonitored peer interaction and, indeed, this is part of the appeal of the internet in general and SNS in particular. Hence privacy is valued, but first and foremost it is privacy from adults, especially parents! (e.g. also noted in Norway by Aas-Hansen (2007) and in a study of slightly older young people in relation to the Korean SNS). The implication is that any initiatives that suggest that parents need to intervene more and monitor what their children put on their profiles need to be thought through very carefully!

Despite the adult perception that young people do not seem to care what they reveal to peers, UK research has show that young people do think about what they do or do not put on their profile (Livingstone, 2008). However, what adults think should be private is not necessarily what young people think should be private. In this respect various studies have indicated the types of information that young people give out: e.g. in an Irish study 8% gave out their home address, 12% their mobile phone and 49% their date of birth (Anchor Ireland, 2007).

There are 2 caveats worth mentioning here. First, US research shows that many do take some precautions e.g. putting some fake details on profiles, not giving details that would allow a stranger to locate them. Second, it is important to remember that putting some things in the profile that are personal is also a means to gain intimacy among peers (Livingstone, 2008). In some cases young people may be aware of adults online, but they put up the details anyway (boyd, 2006).

There is a mixed picture in Europe as regards the use of public and private settings, in the UK, 41% of youth had profiles set to public (Ofcom, 2007). In part there is reason to believe that there could be problems understanding how privacy settings work (Ofcom, 2007; Livingstone, 2008. But, as noted above, part of the decision to leave the settings public can be motivated by the desire to be visible to other teenagers (boyd, 2006).

In general, most studies suggest that parents do not know much about SNS. While 65% parents say the set rules about their children's use of SNS, only 53% of children said the parents set rules (Ofcom, 2007, UK). In that study, among the parents setting rules the two main types of rule concerned meeting new people (30%) and giving out personal details (27%) (NB these are the figures from the parents' answers).

Lastly, in the UK 27% of 8-11 year olds claim to have a profile on a SNS (Ofcom, 2007, UK). Admittedly some sites cater for younger children, but most have minimum age that is higher than 11. The Ofcom qualitative study confirmed that a certain amount of 'underage' use was taking place. That same study also notes other research showing that 15% of 6-11 have 'used' Bebo, 4% have 'used' Facebook, and 8% have 'used' MySpace (Nielsen, August 2007, in Ofcom 2007). However, it is not quite clear what counts as 'used' in this study – this was simply the question wording in the survey.

In Italy, a new study has recently been completed by Save the Children Italy, as follows. It represents one of the first attempts in Italy to investigate teenagers' use of social networking websites and instant messaging services, with a special focus on risky experiences. The research was conducted by Doxa, a well known research institution, but was promoted by Save the Children Italy within its involvement in the Safer Internet Programme and the Easy4 activity.

Its origins and the nature of the subjects involved leads to the focus on risky experiences: beside issues of access and use (for example which is the main social networking site used by Italian teenagers) great attention is paid to issues of privacy and risky experiences. This focuses results on questions about their willingness to give out personal information online, the degree of self-disclosure in personal profiles, whether online friendships result in offline face to face meetings or not (and if the person met is significantly older), if they met harmful or unpleasant content on the internet and how they tend to deal with these risky experiences. Especially, they were asked if they wished a major involvement by Internet Service Providers in order to promote a safer online environment for children.

The study was conducted on a national representative sample of 300 children aged 13-17. The questionnaire was administered by telephone using C.A.T.I. The results can be summarised as follows.

- 73% have used instant messaging at least once.
- the most used instant messenger is MSN, and the most social media site is YouTube.
- 48% of the interviewee have a personal profile on MSN or a social networking site (34,3% boys vs 44,9% girls, 34,8% aged 13-14 and 42,3% aged 15-17) 8,2% of boys and 10,5% of girls have more than one profile.
- Social network users admit giving out personal information on their personal pages
  - their true name 73,9%
  - the place/city where they live 69,7%
  - one or more pictures 60,7%
  - email address 57,4%
  - pictures of their friends 54%
  - their surname 48%
  - the name of the school they attend 18,4%
  - their mobile phone 6,6%
- 12% of interviewees (25 of users of social networks and MSN) thinks it's very easy to identify someone from their personal pages, while 18,4% of the sample (34,8% of the users) think it is not so easy but not impossible. By gender and age)
  - 14,9% girls (26,9% girls users):
  - 9,9% boys (23,3% boys users)
  - 6,6 % aged 13-14 (15,4% users)
  - 15,9 % aged 15-17 (30,3% users aged 15-17)
- Thus perception of risks connected to giving out personal information is higher among girls and increases with age.
- Reasons for using instant messengers and social networking: 78% user to stay connected with friends; 19, 8% to meet new friends; 15,1% have fun; 3,1% affairs, relations; 1,5% research and study.
- 46,9% of the users have met friends online. 28,8% of users have met their online friends offline (33,6% boys vs 24,8% girls, 22,4% aged 13-14 vs 32% aged 15-17). 37% of these (48, 3% boys and 24,7% girls) went to the meeting alone, while 63% went with friends or other people.
- 24,8% of the users admit have established a contact with older people (adults? It says in Italian "very older people" so it is supposed to be adults!) The nature of the relationships is examined in the next slide (26) with a warning since the number of answers was too limited (anyway 44,6% describes the relationship as friendship).
- Online risks: 16 % of the sample and 32,8% of users of social networks and MSN have had at least once an "unpleasant" experience online. Among users:
  - 15,2 have met pornographic content on social networking sites
  - 9,8 have received offensive messages
  - 8,6 have been asked for erotic pictures
  - 7,4 have been asked for sex online

- 6,4 have found embarrassing, disconcerting images of people they know
- 5,6 have experienced the diffusion of personal information without their consent
- 2,3 have found embarrassing images of themselves
- 42,2% of the interviewees and 86,6% (81,1% boys, 91,3% girls; 89,2 % aged 13-14, 85,5% 15-17) of the users think ISPs should do something to prevent these situations.

2. What controls, if any, should be available to parents over their children's SNS accounts? Should parents be allowed to cancel accounts or change profiles of their children?

Not without their permission. This is their site and as children of the social networking generation they would never accept that and then there would become a gap between the parents´ and the child's communication and then there would be true danger. If there is no communication then parents don't know what is going on. It would be likely that the child would e.g. get a different site that their parents would not even know about and then they have no control. The best thing is for parents to have access to their sites and comment on the content and have an open communication.

3. Which tools are the most appropriate to protect minors when using SNSs? What further steps should SNS providers take to reduce the risks to minors on their sites?

(i) Education about privacy and online protection. Privacy is something that children (and sometimes adults) tend to forget and look at as non important when it truly is. In International Youth Panels, there has been much discussion about how difficult it is for children to report when something isn't right. They want a more visible "help button" where they can report if someone is bothering them and confidence that any request will be responded to promptly, confidentially and effectively.

(ii) SNS providers could:

- automatically and regularly search for illegal, annoying, disturbing and risky behaviour/activities of its members
- block a user's profile if illegal/inappropriate content is found on their profile or in their activities
- introduce an age verification system to ensure user provides correct age
- ensure default (privacy) settings when a new profile is being created and for all those who reveal themselves in some way to be legal minors, while also providing reminders of the importance of privacy subsequently.

4. What should Members States do in order to improve the safe use of SNSs by minors? (E.g. legislation, co-regulation, awareness activities, introduction of the subject into the educational curricula, etc).

Educational curricula both for children and their parents - parents update

ourselves! When teaching children - use videos that spark conversation, make them write personal information on their t-shirt and walk around school - how does it feel to walk around with all this information about you - how is that different from what you do on SNS?

Codes of conduct among self-regulating industry is also appropriate, as now developed in the UK with the Home Office's code of conduct just agreed and published. It is vital that such codes are independently audited on a regular basis to ensure compliance. This is the proposal of the UK's new Council for Child Safety on the Internet.

Awareness activities, e.g. production of spots, videos to be shown on TV and/or distributed to schools; workshops in schools.

Cooperation with public and private TV channels to incorporate a show about the safe use of the Internet and its risks, SNSs included into the children's programs.

SNSs being one lesson of the safer Internet subject to be introduced into the educational curricula.

Creation of a CyberCrime Unit at the police to deal with illegal internet content.

Bibliography

Aas-Hansen, Sunniva (2007) På nett med barna? Et hefte om barn og unges internettbruk. (On the Net with Children? A Report about Children and Young People's Use of the Internet). Oslo: Redd Barna (Save the Children) http://www.reddbarna.no/default.asp?V_ITEM_ID=9267

Anchor Ireland (2007) *The Anchor Watch_Your_Space Survey: Survey of Irish Teenagers' Use of Social Networking Websites.* Available at www.webwise.ie/GenPDF.aspx?id=1744

Boyd, D. (2006) *Identity Production in a Networked Culture: Why Youth Heart MySpace,* American Association for the Advancement of Science, St Louis, February, 19th, Available http://www.danah.org/papers/ASAS2006.html

Fluckinger, C. (2007) 'L'évolution des formes de sociabilité juvénile reflétée dans la construction d'un réseau de blogs de collégiens' *Doctoriales du GDR "TIC & Société".* Marne-La-Vallée, 15-16 janvier 2007. Available at http://gdrtics.u-paris10.fr/pdf/doctorants/2007/papiers/Fluckiger_C.pdf

Haddon, L. and Kim, S-D. (2007) 'Mobile Phones and Web-based Social Networking - Emerging Practices in Korea with Cyworld', The *Journal of the Communications Networ*k. Vol.6, No.1, January-March. Available at http://members.aol.com/leshaddon/Date.html

Haddon, L. (2007) *More than a Phone: Emerging Practices in Mobile Phone Use amongst Children,* in proceedings of the conference, Communication in the 21st Century: The Mobile Information Society, 27th-29th September, Budapest. Available at http://members.aol.com/leshaddon/Date.html

Larsen, M. (Forthcoming) 'Understanding Social Networking: On Young People's Construction and Co-Construction of Identity Online', *Journal of Computer Assisted Learning*.

Livingstone, S. (2008) 'Taking Risky opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression', *New Media and Society*, Vol.10, No.3, pp.459-77

Mascheroni, G., Pasquali, F., Scifo, B., Sfardini, A., Stefanelli, M. and Vittadini, N, (2007) "Young Italians' Crossmedia Culture*s*", *Observatario*, Vol. 2, No.1 March. Available at http://obs.obercom.pt/index.php/obs/issue/view/10

Millwood Hargrave, A., and Livingstone, S., with others (in press) *Harm and Offence in Media Content: A review of the empirical literature.* Bristol: Intellect Press. Second Edition.

Ofcom (2008) *Social Networking: Quantitative and Qualitative Research Report into Attitudes, Behaviours and Use.* Available at http://www.ofcom.org.uk

Siibak, A. (2008) *"How you doin'" Visual Management of Young Men on a Social Networking Website*, paper presented at the NYRIS 10 conference, Lillehammer, 13th-15th June.

Taraszow, T., Shitta, S. and Laouris, Y. (Forthcoming) "How much Personal and Sensitive Information do Cypriot Teenagers reveal in Facebook?" *International Journal of Media and Cultural Politics.*

TIRO project (forthcoming) Will be available at http://www.belspo.be/belspo/fedra/proj.asp?l=nl&COD=TA/00/08

Valkenburg, P. M., Peter, J. and Schouten, A.P. (2005) 'Friend Networking Sites and their Relationship to Adolescents', *CyberPsychology and Behavior*, No.9, pp.585-590.

See also:
-http://sils.unc.edu/~wildem/Publications/CHI2006-Privacy.pdf
-http://petworkshop.org/2006/preproc/preproc_03.pdf
-http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html
-http://csis.pace.edu/~dwyer/research/DwyerHICSS2007.pdf
-http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf
-http://chimprawk.blogspot.com/2005/10/freshman-facebook-zeitgeist.html
-http://ibiblio.org/fred/pubs/stutzman_pub4.pdf
-http://www.ibiblio.org/fred/facebook/stutzman_fbook.pdf

Further information

This response has been prepared by Sonia Livingstone with contributions from Elena Aristodemou, Gudberg Jónsson, Leslie Haddon, Yiannis Laouris, Giovanna Mascheroni, Maria Francesca Murru and Tatjana Taraszow.

For further information and reports, please see www.eukidsonline.net or contact Sonia Livingstone at s.livingstone@lse.ac.uk.

---

[i] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/social-networking-guidance