



EUROPEAN COMMISSION
Information Society and Media Directorate-General

**PUBLIC CONSULTATION
ON ONLINE SOCIAL NETWORKING
SUMMARY REPORT**

1. Background and structure of the consultation

The public consultation ran throughout July 2008 and it was published on EUROPA at http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm Information was also sent to the subscribers of the mailing list of the safer internet web site on EUROPA.

The consultation was based on 3 questionnaires structured around the following themes: age verification, cross media rating and classification and online social networking.

The purpose of the public consultation was to gather the knowledge and views of all relevant stakeholders (including public bodies, child safety and consumer organisations, industry) in order to feed the 2008 edition of Safer Internet Forum which was dedicated to the above mentioned topics.

This report is a summary of the 54 responses received to the questionnaire on **social networking services**.

2. Summary of contributions

Contributions came from the child welfare and consumer organisations, national youth panels, industry and researchers and some public authorities. A complete list of respondents and their contributions are available on http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm

There was an important degree of consensus between respondents across most questions, with differences related to issues of detail, or suggestions about how policies or principles should be implemented. Most respondents addressed the range of potential risks to minors online, which is a long list ranging from the trivial to the extremely serious, and a smaller number focussed upon the dangers which they actually encounter and report most frequently on a daily basis.

The following matters gave rise to a high degrees of consensus between respondents:

2.1. Bullying and invasion of privacy were most frequently cited as the most likely dangers encountered by minors. Grooming and other inappropriate, sexually motivated contacts were less likely to be encountered, but should nevertheless be taken very seriously. More research in this area is necessary in order to get to know the true levels of wrongful or criminal behaviour.

2.2. Protection of minors is important, but parental control should not extend to a right to cancel or amend accounts without the knowledge or agreement of the account holder. Parents should talk with children and take an active role in overseeing online activity, while respecting their privacy.

2.3. Social networking service providers should continue to pursue a policy of self-regulation to meet public expectations relating to the protection of minors. However,

compliance with self-regulation regimes should be independently monitored, with the possibility of certain minimum levels of protection established by law.

2.4. Education and awareness is the most important factor in increasing the ability of minors to protect themselves online. This might be increased by parents taking a more proactive role, or by social networking providers providing more information on home and sign-on pages, or by governments in making media awareness a compulsory part of school curricula.

2.5. More research on the actual harm befalling minors using social networking services is necessary. However, where comparative figures are available, they reveal significant differences between countries.

3. Replies to individual questions

3.1 Risks minors are most likely to encounter on social networking sites

The two most frequently identified threats which minors would be most likely to encounter were cyber-bullying and risks to privacy associated with supplying personal information online. For example, a Danish survey of 1500 minors reported that bullying and other activities engaged in by minors among themselves are far more likely to be experienced than exploitation by adults.

Under the general heading of **cyber-bullying**, respondents included a broad range of behaviours including more generalised harassment which minors may suffer at the hands of others who are known to them: circulation of photographs, rumours or gossip (true or false), “happy slapping” and other behaviour which would be distressing or hurtful to the subject.

Under **risks to privacy**, respondents included many problems associated with minors supplying personal information online by which they might be identified, identity theft, the wrongful selling on of user databases to third parties, spam, phishing and problems relating to exposure to targeted, viral or otherwise inappropriate marketing. Regarding the supply personal information online, EUKidsonline highlighted that " 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)."

Risks of **exposure to harmful content or inappropriate contact for sexual purposes (grooming)** were also widely discussed. This was considered the most likely risk by a small number of respondents. It was clear that whenever minors are actually confronted with such problems, these were matters of the greatest concern, but the picture is far from clear about the level or likelihood of risk actually confronting minors in this regard.

Some respondents felt that the dangers of interactions with a sexual theme are extremely hard to quantify or evaluate. A number of governmental and NGO respondents quoted submissions to the UK's Byron review, which underlined the difference between risk of harm (which is the focus of much of the current research) and actual harm, which is harder to identify, where relevant statistics are not available and where research findings may not be generalisable from one part of the world to another.

When harm comes to a young person in this way, it is a very serious matter, but respondents' experience suggested that such problems arose less often when compared with other areas of possible risk. On inappropriate contact with adults for example, one national media authority stated that "The risk of meeting unknown adults on social networking sites that might imperil children for sexual or violent harassments is very low." Another reference suggests that meeting an online contact offline is "the least common but arguably most dangerous risk".

A German NGO expanded upon this point in the following way:

"For teenagers, some offers concerned with the representations of violence or sexuality are related to trying out taboos....The suggestional strength and the relevance to reality of such offers are often severely limited due to their poor quality. Moreover, a critical public reflection on this problem can serve to make clear to teenagers that some of the available contents are socially objectionable. We should certainly take this problem seriously, but should not overestimate it."

The second point, as expressed by one respondent was that the reported incidence of unwanted sexual contact aimed at minors and perpetrated by older people, tended to be a function of the amount of resources used to detect them. Therefore the full extent of this problem may not yet be known.

In summary, although some respondents provided input on existing research on use of social networking sites by children and teenagers (see **list on links to research in annex**) they agreed that more research/survey data on the relative likelihood of different risks confronting minors online is necessary.

3.2 Parental control over children's accounts on social networking sites

Respondents were almost unanimous in declaring that parents or other carers should not be able to close accounts or alter profiles of those in their care without, at the very least, informing or involving the young person concerned in the process. One telecoms company "believes that parents or guardians are entitled to have full control of their children's SNS accounts". Other respondents agreed that parents should have such legal rights, but advised that they should only be used as a last resort, and once again, with the full participation of the child. An Internet consulting company suggested that carers might have limited rights to control or cancel accounts of minors during what they describe as a "training period", to help them get started in the right way. More commonly, respondents felt that the rights of minors would be wrongly compromised by allowing such interventions and that they should not be permitted under any circumstances.

Several respondents considered this matter in detail and set out a number of problems associated with giving parents a power to intervene or close an account. The first of these was the difficulty in establishing formally that the person claiming such a right was indeed the user's parent or held a suitable supervisory position in relation to the user. Some respondents, particularly among the social networking service providers, also felt that giving such rights to parents would be ineffective as young users would quickly re-register or find other ways to avoid parental control. A related point was that making such rights available could undermine relationships and create an atmosphere of mistrust between carers and minors. Such barriers might prevent minors accessing the very real benefits of social networking.

One NGO made suggestions for services which social networking providers might offer to help this process. The respondent proposed that carers be given access to a service which would allow them to monitor a minor's online activity at some suitable level of generality, or to receive logs or summaries describing the activity in broad terms. Alerts might be flagged if a minor accesses unsuitable content, or puts him/herself at risk in some way.

One major social networking service provider made the point that, whereas there are many difficulties associated with intervening in a minor's online activity when the minor is the account holder, it is easier when the carer is the primary account holder and permit the minor to share or otherwise "occupy" the space set up and configured by the carer. It was further suggested that parents could, and perhaps should, join sites which their children use in order to understand more fully what is involved.

All respondents to this question stressed however that there is no alternative to discussion and co-operation between parents and children. There is much information available to help carers structure discussion and advice, to be alert to possible risks and to take action when problems arise. Various sources and tools for carers were suggested, including for example WOT – Web Of Trust, which is a free tool for the Mozilla Firefox browser that warns the user about the content of a website through a rating system.

3.3 Appropriate tools to protect minors when using social networking sites

Responses to this question tended to list existing protection tools and techniques. **Age-verification** was mentioned frequently, but always with caveats about its effectiveness (see separate report on Age verification). **Reporting tools** and "**stop buttons**" were mentioned, with the comment that some sites offered much in this area while others did very little. One national media authority felt that **human moderation** and a highly visible "stop" button for users to employ when confronted by offensive content or behaviour should be mandatory for social networking providers. An inter-governmental agency proposed **workshops in "Privacy Enhancing Technologies"** to encourage collaborative progress towards greater online security.

Image filters and language algorithms were also identified as tools which again went some way to block harmful contact or inappropriate behaviour but were far from perfect. All respondents supported calls for further research and development in this area.

Some specific examples of protective measures currently in use were described. One NGO suggests a number of new technologies: anti-grooming and anti-bullying technology, "uses sophisticated tools to monitor, analyse and assess online relationships as they develop over a period of time. It does this by examining live online chat and instant messenger conversations". Children's charities cited tools available for the protection of younger users, such as offline authentication and moderation, pre-moderated services and template environments which are used to restrict comments that can be made.

Many respondents supported the view that service providers should acknowledge the limitations of automatic, technical based protective tools and employ more proactive human moderation. Currently, many sites withdraw or block access to harmful or illegal content in response to reports from users. More should be done to **pre-moderate** uploads and identify known infringers to prevent inappropriate content reaching a site in the first place. A German NGO elaborated a proposed set of minimum standards which could be applied to sites targeting different age groups and which might differ depending on the targeted age group. For example, sites targeting children under 14 would be expected to use high levels of pre-screening of content, full moderation and minimal collection of personal information. Such measures would render age verification unnecessary as everything on the site will have been cleared as unobjectionable. Sites targeting adolescents (14-18) could have greater flexibility, but would be expected to apply appropriate levels of pre-screening of content and proactive checking of content and user behaviour. For sites targeting adults, very rigorous age-verification measures would be expected, which would render further screening and moderation unnecessary. In some matters, these separate approaches for different age groups would be supported by clear rules: for example on acceptable uploads, behaviour in chat rooms and publishing personal information. Requirements for pre-screening, content checking and chat room moderation could be addressed with greater flexibility so long as they were consistent with the service providers' duty of care. The application of more detailed age-dependent safety measures, with controls carefully aligned to the age of the user was also strongly advocated in the response of a major children's charity.

3.4 Member States' role in improving the safe use of social networking sites by minors

The overwhelming response to this question was a focus on education and awareness activity. Numerous national programmes were cited, and the importance of collaboration between governments and other stakeholders was stressed throughout. Several respondents, including felt that IT and media awareness should form compulsory elements of national school curricula.

A national consortium of consumer agencies argued for closer regulatory control over online advertising and publicity, as exposure of minors to inappropriate exploitation was a serious risk.

Industry self-regulation was also strongly supported by all respondents and again various national examples were quoted, including The UK Home Office Guidelines for social networking providers and the "Rome Memorandum"- Report and Guidance on Privacy in Social Network. The need for independent auditing of compliance with

such self-regulatory schemes was invariably stressed by NGOs and child protection agencies.

Notwithstanding their support for industry self-regulation, several respondents felt that national and European laws might play a role “at the extremes” where risks were most serious. Moreover, it was felt by a number of respondents particularly those representing consumer groups, that industry should be held to account legally where the self-regulatory response was inadequate, or where compliance was weak or variable. For example, the Byron Review recommendation in the UK for “clear and mandatory take-down times for abusive and offensive content” was endorsed. Arguments for extending the legal responsibilities of service providers beyond the present “notice and take-down” requirements were also put forward by a German NGO. Reasonable protection measures, (for example use of filtering and screening tools, sanctioning of users who breach terms of use, content checking) should be mandatory. There should also be a legal obligation to provide proof of suitability to operate services targeting minors. One young people’s charity proposed that public subsidies might be made available to social networking providers to incorporate more safety features into their sites. A number of children’s charities thought that a set of uniform minimum standards for the protection of minors was essential, and that enthusiastic compliance with such standards should be seen by social networking providers as an opportunity to add value to their products, and not merely as an expensive overhead cost in providing their services.

4. Conclusion

The detailed responses received to these questions are indicative of the seriousness with which respondents view the issue of the safety of minors using social networking services. The areas of consensus, as set out in the points 1-5 of the introduction to this summary document, cover many of the most important policy aspects of social networking:

- Bullying and other threats which young users inflict upon each other may be more likely to arise than threats from adults.
- Much is known about potential risks, but more research on the nature and extent of harm actually experienced by minors online is needed.
- Parental involvement in their children’s online activity is important, but principles of privacy and trust should dictate how parents help children to stay safe.
- Education and awareness are the most important factors in enabling minors to keep themselves safe.
- Industry self-regulation is the preferred approach for service providers to meet public expectations with regard to the safety of minors. Legislation should not place burdens on service providers which prevent them from providing minors with all the benefits of social networking. However, available safety measures vary greatly from one provider to another and mandatory minimum levels of provision may need to be established.

Annex :

Links to available research

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>

Boyd, D (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, in MacArthur Foundation Series on Digital Learning - Youth, Identity, and Digital Media Volume 119-142 (David Buckingham ed.,2007), available at <http://www.danah.org/papers/WhyYouthHeart.pdf>.

Boyd, D (2007) Social Network Sites: Public, Private, or What?, Knowledge Tree 13 (May 2007), available at <http://kt.flexiblelearning.net.au/tkt2007/edition-13/social-networksites-public-private-or-what/>

Boyd, D (2007) Socializing digitally, Vodafone Receiver Magazine, # 18: The Home (June 2007),available at <http://www.danah.org/papers/VodafoneReceiver.pdf>.

Boyd, D. and Jenkins H., (2006) , Discussion: MySpace and Deleting Online Predators Act (DOPA), MIT Tech Talk (May 26, 2006), at
<http://www.danah.org/papers/MySpaceDOPA.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 Network. 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> EU Kids Online, July 2008 12

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

Lenhart, A., *Teens, Stranger Contact & Cyberbullying*, Pew Internet & American Life Project (April 30, 2008), available at http://pewinternet.org/PPF/r/250/presentation_display.asp.

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 Cultures", *Observatorio*, 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>

Rosen, L., *Adolescents in MySpace: Identity Formation, Friendship and Sexual Predators* (June 2006), available at <http://www.csudh.edu/psych/Adolescents%20in%20MySpace%20-%20Executive%20Summary.pdf>

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.

Taraszew, 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.

Wolak, J., et al., Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment, *American Psychologist*, Vol. 63, No. 2 111-28 (Feb.-Mar. 2008), available at <http://www.apa.org/journals/releases/amp632111.pdf>.

The authors state the social networking sites do not appear to have increased the risk of victimization by online molesters. Id. at 117.

Wolak, J., et al., 1 in 7 Youth: The Statistics about Online Sexual Solicitations, Crimes Against Children Research Center (Dec. 2007), available at <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/1in7Youth.pdf>.

Ybarra, M. & Mitchell, K., How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs, Pediatrics (Jan. 28, 2008), available at <http://www.pediatrics.org/cgi/content/full/peds.2007-0693v1>

Childnet report commissioned by Becta Young People and Social Networking Services <http://www.digizen.org/socialnetworking/>

“The experiences of Danish children and young people at online meeting sites on the internet”, February 2008. Aalborg university and the Danish Media Council, excerpt in EN in the Insafe virtual library:
<http://resources.eun.org/insafe/SurveyEnglish1.doc>
<http://malenel.wordpress.com/2008/02/12/new-survey-young-peoples-experiences-onsocial-network-sites/>

“What do kids have to say about internet, IT and cell phones?”, June 2007, a study by BRIS (Children’s rights in the society), Report in Swedish in the Insafe virtual library:
http://medieradet.se/upload/Rapporter_pdf/BRIS_rapport.pdf

Save the Children Italy survey on SNS use by young Italian people:
http://www.easy4.it/dmdocuments/profili_da_sballo_instantmessaging_STC.pdf

Save the Children Norway survey:
http://www.reddbarna.no/default.asp?V_ITEM_ID=4435 (to be published in September 2008)

Save the Children Finland surveys: Children’s Voice 2008:
http://www.pelastakaaapset.fi/nettivistijje/english/Childrens_voice_2008.pdf (to be published August 2008)

Mannerheim League for Child Welfare
http://www.mll.fi/in_english/projects/tunne/

A Report to the Anti-Bullying Alliance by Peter Smith, Jess Mahdavi, Manuel Carvalho and Neil Tippett Unit for School and Family Studies, Goldsmiths College, University of London An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying

<http://www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf>

JIM Studie 2007 <http://www.mpfs.de/fileadmin/JIM-pdf07/JIM-Studie2007.pdf>
In 2008 the JIM study will concentrate on youngsters using social communities.

ARD/ZDF Online-Studie 2007: <http://www.daserste.de/service/studie.asp>

Institute for Public Policy Research: Behind the Screen, April 2008 (www.ippr.org)

“Privacy Topics - Social Network Sites and Virtual Communities”, December 2007, Privacy International:

[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559084&als\[theme\]=Privacy%20and%20Human%20Rights](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559084&als[theme]=Privacy%20and%20Human%20Rights)

“CA/NCSA survey on social networking”, September 2008:

<http://staysafeonline.org/features/SocialNetworkingReport.ppt#484,1,Slide 1>

Internet Caucus Advisory Committee, Panel Discussion, Just the Facts About Online Youth Victimization: Researchers Present the Facts and Debunk Myths (May 2007), available at <http://www.netcaucus.org/events/2007/youth/20070503transcript.pdf>.

“Social Networking Websites and Teens: An Overview”, July 2007, Pew Internet:

http://www.pewinternet.org/ppf/r/198/report_display.asp

http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf

http://www.pewinternet.org/pdfs/PIP_Stranger_Contact_Data_Memo.pdf

<http://www.pewinternet.org/pdfs/PIP%20Cyberbullying%20Memo.pdf>

http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf

S. Gürses, B. Berendt, T. Santen, 2006, “Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments”. Workshop on Ubiquitous Knowledge Discovery for users (UKDU'06). Proceedings.

S. Preibusch, B. Hoser, S. Gürses, B. Berendt, June 2007 “Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling” in Proc. of the Data Mining for User Modelling Workshop (DM.UM'07) at UM 2007.

S. Gürses, forthcoming. Multilateral Privacy Requirements in Social Networks. Ph.D. Thesis.

Rosenblum, D. May/June 2007, “What Anyone Can Know - The Privacy Risks of Social Networking Sites” in IEEE SECURITY & PRIVACY

Solove, D. J., January 2006. A taxonomy of privacy. University of Pennsylvania Law Review 154 (3).

“Security Issues and Recommendations for Online Social Networks Editor: ENISA Position Paper No.1”, October 2007. ENISA

See also:

- <http://sils.unc.edu/~wildem/Publications/CHI2006-Privacy.pdf>

- http://petorkshop.org/2006/preproc/preproc_03.pdf

- <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>

- <http://csis.pace.edu/~dwyer/research/DwyerHICSS2007.pdf>

- <http://csis.pace.edu/~dwyer/research/DwyerHICSS2008.pdf>

- <http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.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
- http://firstmonday.org/issues/issue11_9/barnes/index.html
- <http://www.informationweek.com/story/showArticle.jhtml?articleID=202200395>
- <http://internetducttape.com/2007/03/08/how-to-use-facebook-withoutlosing-your-job-over-it/>
- http://lessig.org/content/articles/works/architecture_priv.pdf
- <http://www.sophos.com/pressoffice/news/articles/2007/10/facebooknetwork.html>
- http://www.truste.org/pdf/Q4_2004_Consumer_Privacy_Study.pdf
- <http://sils.unc.edu/~wildem/Publications/CHI2006-Privacy.pdf>
- <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>
- <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>
- <http://jcmc.indiana.edu/vol13/issue1/donath.html>
- <http://jcmc.indiana.edu/vol13/issue1/liu.html>
- <http://jcmc.indiana.edu/vol13/issue1/hargittai.html>
- <http://jcmc.indiana.edu/vol13/issue1/kim.yun.html>
- <http://jcmc.indiana.edu/vol13/issue1/byrne.html>
- <http://jcmc.indiana.edu/vol13/issue1/humphreys.html>
- <http://jcmc.indiana.edu/vol13/issue1/lange.html>