Opinion of the European Economic and Social Committee on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies

COM(2008) 106 final — 2008/0047 (COD)

(2008/C 224/13)

On 7 April 2008 the Council decided to consult the European Economic and Social Committee, under Article 153 of the Treaty establishing the European Community, on the

Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies.

On 11 March 2008 the Committee Bureau instructed the Section for Transport, Energy, Infrastructure and the Information Society to prepare the Committee's work on the subject.

Given the urgent nature of the work, the European Economic and Social Committee appointed Ms Sharma as rapporteur-general at its 445th plenary session, held on 28 and 29 May 2008 (meeting of 29 May 2008), and adopted the following opinion unanimously. votes

1. **Conclusions and recommendations**

1.1 The European Economic and Social Committee praises the Commission for its work already done towards addressing the issues of child protection in regards to 'online technologies' ([1]), specifically noting that the average awareness level in the population has been increasing thanks to campaigns by social partners, in particular NGOs and the Commission's annual Safer Internet Days.

1.2 The EESC itself has drafted many opinions to highlight the issues ([2]). Additionally it recommends an international partnership approach which encourages:

1.2.1 International sharing of data and pooling of ideas across governments, law enforcement, Hotlines, banking/financial/credit card institutions, child abuse counselling centres and child welfare organisations and the internet industry.

1.2.2 EU and/or international 'taskforce' which meets quarterly to facilitate the sharing of data, expertise and good practice between stakeholders, including Hotlines, law enforcement, governments and, particularly, the international internet industry.

1.2.3 Definition and promotion of an International and European good practice model as regards the combating child sexual abuse content on the internet by Hotlines.

1.2.4 A review of all existing and future Hotlines in light of currently accepted good practice and the evaluation of Hotlines' performance against new good practice models.

1.2.5 A streamlining of Programme resources and funding allocation in the future as a result of Hotline review.

1.2.6 Participation by Hotlines in the European database project.

1.2.7 Encouragement of Hotline, and other relevant organisations, partnerships with national domain name registries to de-register domain names advocating the sexual abuse of children or providing access to this content.

1.2.8 United efforts in raising awareness of the problems of 'grooming' and 'cyber-bullying' ([3]) and sign-posting to the relevant law enforcement agency and children's charities where appropriate.

1.2.9 Introduction of support procedures for analysts and those viewing the images working within the Hotline environment.

1.2.10 Work to ascertain and ensure the harmonisation of legal frameworks in this area across member states.

1.2.11 Establishment of a Networking Office at Commission level to act as independent assessor, coordinate research, review Programme implementation and achievement of recommendations.

1.2.12 Establishment of an annual 'Experts' panel to intensify the transfer of knowledge.

([1]) For the purposes of this document, 'online technologies' refers to technologies that are used for accessing the Internet and to other communication technologies. In addition, in certain cases such as video games, there are both 'online' and 'offline' uses of content and services and both may be relevant to child safety.

([2]) 'Illegal content — Internet' OJ C 61, 14.3.2003 p.32 and 'Safer use of the Internet' OJ C 157, 28.6.2005 p.136.

([3]) 'Grooming': Direct contact by predators who will befriend children in order to commit sexual abuse; 'cyber-bullying': bullying in the online environment.

1.2.13 Establishment of Youth Forum to ensure the inclusion of children and young people's views and experiences in research and future Programme implementation.

1.2.14 Proactive and collaborative use of funding streams, such as Daphne and Safer Internet Programmes.

1.2.15 Establish liaison with relevant US authorities to encourage reduction in the hosting of child sexual abuse content in the US and establish active trans-Atlantic data exchange.

1.3 Working with a partnership approach ensures maximisation of expertise, knowledge dissemination and funding. Most importantly it guarantees the involvement of stakeholders and social partners in overall EU efforts to minimise illegal online content and reduce access to it.

2. **General Comments on the Commission's Proposal:**

2.1 The internet and communication technologies (hereafter referred to as 'online technologies') ([4]) were envisaged and designed as communications tools for academics and researchers; however, they are now used in homes, schools, businesses and public administrations in most parts of the world.

2.2 Children are active users of online technologies, and increasingly so. But, beyond the benefits of interactivity and participation in the online environment, they also face some serious risks:

a) Direct harm, as victims of sexual abuse documented through photographs, films or audio files and distributed online (child abuse material).

b) A perpetuation of victims' sexual abuse by the repeated viewing of the records of their abuse due to widespread online distribution and global availability.

c) Direct contact by predators who will befriend them in order to commit sexual abuse ('grooming').

d) Victims of bullying in the online environment ('cyber-bullying').

2.3 Further trends (see Appendix 1) ([5]) include:

a) The fast and dynamic evolution of new technological landscapes, increasingly shaped by the digital convergence, faster distribution channels, mobile internet, Web 2.0, Wi-Fi access and other new content formats and online technological services.

b) Recognition of the very young age of child victims and the extreme severity of the sexual abuse they are suffering.

c) Clarification of the scale of the problem as regards publicly available websites depicting the sexual abuse of children, that is, a concrete 'manageable' target of around 3 000 websites per year hosted around the world facilitating access to many hundreds of thousands of child sexual abuse images.

d) Recent data regarding the regional hosting of child sexual abuse networks suggests the majority of this content is hosted in the US.

e) Recent data suggests that online child sexual abuse content regularly hops host company and host country in order to avoid detection and removal, thereby complicating law enforcement investigation at a solely national level.

f) Lack of international efforts by domain name registries to de-register domains advocating the sexual abuse of children or providing access to such content.

g) The remaining and potentially, widening 'generation gap' between young people's use of online technologies and their perception of risks verses the adults' understanding of its use.

h) Public exposure to child sexual abuse material may be reduced by voluntary industry blocking of individual URLs by service providers.

i) The benefit of national recommendations regarding online tools, such as filtering products, search engine security preferences and the like.

2.4 Protecting internet users, particularly children, from exposure to illegal and 'harmful' content and conduct online, and curbing the distribution of illegal content is a continuing concern for policy and law-makers, industry, end-users and particularly parents, carers and educators.

2.5 From a legal point of view an essential distinction has to be made between what is illegal on the one hand and 'harmful' on the other, since they require different methods, strategies and tools. What is considered to be illegal may vary from country to country, is defined by the applicable national law and is dealt with by law enforcement, other government bodies and those Hotlines with the appropriate authority.

2.6 The EESC requests that the legislative harmonisation across Member States is implemented and enforced at National level and includes the following as minimum as set out in the Council of Europe Cybercrime Convention ([6]):

a) What constitutes child sexual abuse material.

b) That the age of a child for the purposes of the victims of child sexual abuse material is 18.

c) That the possession and viewing/downloading of online child sexual abuse material is an offence and warrants severe custodial penalties.

([4]) As 1.

([5]) This appendix is available only in EN and can be found attached to the electronic version of this Opinion on the Web.

([6]) Council of Europe ETS 185 Convention on CyberCrime 23 XI 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

2.7 Although certain Europe-wide standards have been established, clarifying legal issues through various recommendations and directives, it should be established whether this data has been converted into practice throughout member states.

2.8 'Harmful' content refers to content that parents, teachers and other adults consider to be potentially harmful for children. Definitions of such content vary across countries and cultures, and can range from pornography and violence to racism, xenophobia, hate speech and music, self-mutilation, anorexia and suicide sites. As such, the EESC acknowledges it is difficult to establish international partnerships regarding such material but that national efforts could be made to raise awareness of tools, methods and technologies to protect children from exposure to it.

2.9 The EU has been a forerunner in the protection of children online since 1996, and the successive Safer Internet programmes (Safer Internet Action Plan 1999-2004, Safer Internet plus 2004-2008) have been major features in this field. The Commission adopted a Communication on the implementation of the Safer Internet plus programme in 2005-2006 ([7]). Additionally, an impact assessment between April and July 2007 ([8]) confirmed that the actions carried out have been effective, while stressing the need to adapt them to emerging internet technologies and dynamic criminality in this area.

2.10 The objective of the new programme will be to promote safer use of the Internet and other communication technologies, particularly for children, and to fight against illegal content and illegal and 'harmful' conduct online facilitating cooperation, exchange of experiences and best practice at all levels on issues relating to child safety online, thus ensuring European added value.

2.11 The programme will have four actions encouraging international cooperation as an integral part of each of them

a) reducing illegal content and tackling harmful conducts online,

b) promoting a safer online environment,

c) ensuring public awareness,

d) establishing a knowledge base.

([7]) COM(2006) 661. Communication from the Commission on the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet plus).

([8]) http://ec.europa.eu/saferinternet.

2.12 However the EESC would ask for definitions and legal clarifications in respect of the words 'harmful' and 'conduct', particularly considering transposition into national law. Further clarification is also required on the role of Hotlines, which do not investigate suspects and do not have the necessary powers to do so (See Appendix 2) ([9]).

3. **An International Model**

3.1 The internet is not owned or managed by huge multinationals which control the content. It is made up of hundreds of millions of pages posted by a multitude of publishers, making it difficult to monitor or control illegal content. However, action is possible from local (the home) to national and international level (including cyber space) to reduce the availability of illegal content if all stakeholders work together.

3.2 The Internet Watch Foundation identified a core of 2 755 child sexual abuse websites hosted internationally during 2007; 80 % of these websites are commercial operations, which frequently hop host company and region to avoid detection ([10]). These tactics, coupled with the complex multi-national nature of the crimes, mean that only a united global response involving law enforcement authorities, governments and the international online sector will enable effective investigation of these websites, their content and the organisations behind them.

3.3 The EESC recognises that 'A partnership approach' is required to ensure child protection. The Social partners, including Government, the online industry, law enforcement agencies, child protection charities, businesses, employee representatives, NGOs including consumer organisations, and the public must work together to highlight the dangers and risks, whilst at the same time allowing young people to gain from the benefits of this revolutionary tool of socialising, learning and innovation.

3.4 The internet can be accredited with improving the quality of life for many but especially for young people, the elderly and many disabled people. It is a unique communication tool, and more and more these days a 'social network'. Changing dynamics in lifestyles, families and employment patterns have led to more independent or isolated periods of time. Therefore protecting the user, in particular the vulnerable, especially children, is a priority which cannot be left solely as a responsibility of their guardians.

([9]) This appendix is available only in EN and can be found attached to the electronic version of this Opinion on the Web.

([10]) The UK Hotline for reporting illegal content specifically: Child sexual abuse content hosted worldwide and criminally obscene and incitement to racial hatred content hosted in the UK * See Appendix 1 and 2 (available only in EN, can be found attached to the electronic version of this Opinion on the Web).

3.5 The emergence of new technologies and services is key to innovation and growth of business globally. Young people are often the first to understand the capabilities and take up these innovations. However, along with development comes abuse and this is a mounting concern. Self regulatory bodies of both industry and stakeholders, have the in depth knowledge of these technologies, with the possibility to develop counter measures to combat this abuse. The sharing of knowledge, raising of awareness and signposting consumers as to how to report sites, together with a distribution of funds where possible to eradicate such abuse, but especially in the context of child abuse, is an essential duty and part of the internet industry's corporate social responsibility.

3.6 The scale and scope of the online problem of the distribution of child sexual abuse content is the subject of much speculation. However, as recognised in the Commission's report, there is a lack of statistical information across the EU member states. Efforts should be directed at tracking the movements and activities of websites associated with the distribution of child sexual abuse content in order to provide information to authorised bodies and international law enforcement to effect the removal of such content and the investigation of its distributors.

3.7 Such organisations must be established at national levels and meet regularly with the EU Commission to formulate strategies. A Platform at EU level, with industry, government, banking/financial/credit card institutions, NGOs, education, employer and employee representation, could be a valuable tool for rapid analysis and action across the Union, with dissemination of information beyond EU borders to facilitate international law enforcement cooperation.

3.8 An EU 'expert meeting' every year regarding the developments surrounding technology, psychosocial factors and law enforcement should be encouraged in order to intensify the transfer of knowledge. Conclusions from these meetings would be disseminated to all European Member States, and platform members, in order to be adapted, integrated or used at National and local level.

3.9 The establishment of a 'Networking Office' in Brussels which researches projects not only from Europe but globally, would support the Platform to ensure knowledge is up to date and relevant, including statistics, with the dissemination of effective processes which combat the issues and can be quickly transferred to active partners. Visits and monitoring would also be the role of the network office. Additionally, the Office could act as an independent Hotline assessor, and review applications for new projects to ensure the prevention of duplication of work already done, and effective and efficient usage of funds. Partnerships could also be proposed by the Office. The role of the network office would be to react to new challenges at the same speed as their developments.

3.10 The establishment of a 'youth forum' may be valuable in the involvement of young people and the dissemination of information to social networks utilised by those most vulnerable. Youth have their own language and are often reluctant to listen to authority but welcome advice from their peers within their social environment. The 'Rights of the Child' must be taken into account and therefore young people must be involved in the process.

3.11 An effective model is required with commitment from stakeholders to sharing information for adaptation to new and emerging forms of internet criminality around the world and the exchange of knowledge.

4. **Guidelines for Hotline Implementation**

4.1 A good practice model for Hotlines:

4.1.1 Hotline analysts trained and recognised in the assessment of illegal online content.

4.1.2 Hotline analysts with expertise in the tracing of potentially illegal online content.

4.1.3 An evidenced partnership approach with all key national stakeholders including government, banking/financial/credit card institutions, law enforcement, organisations working with families, children's charities and, particularly, the internet industry.

4.1.4 Co- and self-regulatory Hotline, showing evidenced effective partnership with the national internet industry and adherence by them to a Code of Practice.

4.1.5 Universal 'notice and take-down' of illegal online content hosted by any national company.

4.1.6 Participation in the centralised European database project of child sexual abuse URLs.

4.1.7 Commitment to achieving blocking at network level by national internet companies of a dynamic list of child sexual abuse websites to protect users from accidental exposure.

4.1.8 Hotlines to have comprehensive websites in their national language providing a simple, anonymous reporting mechanism with clear sign-posting to Helplines and other relevant organisations regarding off-remit issues such as grooming and cyber-bullying.

4.1.9 Awareness-raising of the Hotline function and related issues.

4.1.10 Evidence of European and international data, intelligence and expertise sharing.

4.1.11 Participation in European and international partnerships with stakeholders to share data, intelligence and pool ideas in order to combat the cross-border nature of these crimes.

4.1.12 Action at a European and international level to enable the removal of child sexual abuse content on the internet and investigation of its distributors, wherever that content is hosted around the world.

4.1.13 Contribution to any national or international bodies set up to take international ownership of combating these websites and facilitate the collaboration of multi-national law enforcement agencies.

4.1.14 Dissemination of guidelines to employers, teachers, organisations, parents and children such as the 'ThinkuKnow' education programme by the CEOP — The Child Exploitation and Online Protection Centre (UK police).

4.1.15 Awareness raising focus on internet users, particularly in partnership with or with sponsorship from national online companies.

4.1.16 Organisations to be a member of INHOPE, the International Association of Internet Hotlines, ensuring that international good practice sharing between Hotlines and industry can be used to remove content ([11]).

4.1.17 Reporting procedures must be simple, upholding individual anonymity for reporters and with rapid processing.

4.1.18 Hotline operators must provide processes that ensure a level of support and counselling for analysts working within the viewing and data processing environment.

4.2 In addition, Hotlines should:

a) Develop partnerships with their national domain name registry companies to ensure that domains regularly providing access to child sexual abuse content, or with names advocating sexual activity with children, are investigated and de-registered.

b) Seek to obtain voluntary funding on a self-regulatory basis from national internet companies who benefit from the Hotline's operation of a reporting mechanism, a 'notice and take-down' service and the provision of dynamic block lists.

c) Encourage or facilitate the blocking of child sexual abuse websites by the internet industry in that country.

d) Encourage the fostering of positive relations between Hotlines and Helplines offering signposting facilities with victim support organisations, in order to promote complementary awareness raising of relevant and up-to-date issues.

5. **Specific Comments: Commission Proposal**

5.1 The Proposal of the Commission leaves several issues unanswered:

a) Who will coordinate the proposed measures, and with what qualification?

b) How are the criteria for the single areas being formulated? Many programmes already established would fit more than one criteria of the proposed Knowledge Database ([12]).

c) Who chooses the appropriate candidates?

d) Who is responsible for a continuing evaluation and networking of these projects?

5.2 Addressing the above questions would prevent reinvention of the wheel, duplication of work already done, and ensure effective and efficient usage of funds. Most importantly it must be guaranteed that experts from the field will be actively involved in the initiative in close co-operation with consultants or civil servants. This would also hold true of the proposal above for a 'Networking Office' at Commission level which researches such projects, gets to know them, visits them and keeps in contact.

5.3 Consideration must be given by the Commission in towards more proactive and collaborative use of funding streams, such as Daphne and Safer Internet Programmes.

5.4 Finally the Committee requests the Commission to stress the importance and impact of:

— Adoption throughout member states of the 'notice and take-down' by Hotlines and the internet industry of child sexual abuse content.

— Wider adoption of the initiative to protect internet users by blocking access to child sexual abuse URLs.

— International effort by domain name registries and relevant authorities to de-register domains associated with child sexual abuse.

([11]) Sept 2004-Dec2006 INHOPE processed 1.9 million reports, 900 000 from the general public, 160 000 forwarded to law enforcement agencies for action.

([12]) For example: Innocence in Danger 'Prevention Project' would fit more than one of the criteria. There are many other such examples.

5.5 The above measures would reduce the occasions when innocent internet users might be exposed to traumatic and unlawful images, diminish the re-victimisation of children by restricting opportunities to view their sexual abuse, disrupt the accessibility and supply of such content to those who may seek out such images and disrupt the dissemination of images to internet users for commercial gain by criminal organisations.

5.6 Importantly, the implementation of the activities would make operations increasingly difficult for those behind the distribution of child sexual abuse content. Whilst the dynamic nature of the crime and the technological sophistication of the offenders make it difficult to wipe out entirely, the more costly, risky and transient operations are made, the less likely this appears to be an easy route for gain, whether financial or otherwise.

5.7 Recent data regarding the scope and scale of child sexual abuse websites (not individual images or URLs) provide further encouragement in the fight towards total eradication. Concrete targets can now be set to demonstrate the benefits of data sharing and 'ownership' at the highest international level and the impact of a positive and successful united international partnership in substantially reducing the numbers of child sexual abuse websites.

Brussels, 29 May 2008.

The Chairman
of the European Economic and Social Committee
Dimitris DIMITRIADIS

Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on roadworthiness tests for motor vehicles and their trailers

COM(2008) 100 final — 2008/0044 (COD)

(2008/C 224/14)

On 16 April 2008, the Council of the European Union decided to consult the European Economic and Social Committee, under Article 80(2) of the Treaty establishing the European Community, on the

Proposal for a Directive of the European Parliament and of the Council on roadworthiness tests for motor vehicles and their trailers.

Since the Committee unreservedly endorses the content of the proposal and feels that it requires no comment on its part, it decided, at its 445th plenary session of 28 and 29 May 2008 (meeting of 29 May 2008), with 85 votes in favour and two abstentions, to issue an opinion endorsing the proposed text.

Brussels, 29 May 2008.

The President
of the European Economic and Social Committee
Dimitris DIMITRIADIS