COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 27.2.2008
SEC(2008) 242

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to 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

IMPACT ASSESSMENT

{COM(2008) 106 final}
{SEC(2008) 243}

TABLE OF CONTENTS

1. Background 4
1.1. State of play: Commission action 4
1.2. State of play: Legislation 6
1.3. Lessons learnt from the past 8
2. Procedural issues and consultation of interested parties 10
3. Problem definition 12
3.1. Problem analysis 12
3.2. Specific risks for children and young people 16
3.3. Who is affected? Target groups 23
4. Objectives 23
4.1. General objective and Specific objectives 23
4.2. Illegal content and harmful conduct/content 24
4.3. Promoting a safer environment online 24
4.4. Awareness-raising 24
4.5. Establishing a knowledge-base 24
4.6. All actions 24
5. Strategic Policy options 25
5.1. Formulation of policy options 25
5.2. Analysis of the impact of the policy options 27
5.3. General policy option 1: Make no change 27
5.4. General policy option 2: Modify 32
5.5. General policy option 3: Slow down 37
5.6. General policy option 4: Stop 41
6. Comparison of the Strategic Policy optio 43
6.1. Comparison 43
6.2. Ranking of options and preferred option 46
7. Risks and Assumptions 47
8. A proposal for a new programme 49
8.1. European Added Value and the principle of subsidiarity 49
9. Cost-effectiveness 51
9.1. Justification of the cost of the proposed intervention 51
9.2. Cost-effectiveness of the funding mechanism 52
10. Monitoring and evaluation 53
10.1. Programme level data sources 54

10.2. Ex-post assessment of the results on programme level 54
10.3. Project level data sources 54

Legislative instruments 57

The structure of the new programme 60

Summary of the results of the public consultation (Online public consultation and Safer Internet Forum 20-21 June 2007) 62

Information sources and documentation used 67

1. BACKGROUND

The envisaged new programme has the overall aim to promote safer use of Internet and other communication technologies (hereafter referred to as "online technologies"), especially by children.

1.1. State of play: Commission action

At the policy level, the Commission has been successful in placing the issues of developing a safer Internet firmly on the agenda of the EU and the Member States via policy work which started in 1996 with the Communication on illegal and harmful content on the Internet. This was followed by two successive programmes, the Safer Internet Action Plan (1999-2004) and the Safer Internet plus programme (2005 – 2008). The foresight of the European Commission in identifying issues related to risks to children in the online environment early on in the development of the Internet has been widely recognised.

These programmes constitute the only pan-European initiative relating to child protection online and have several actions that have proved effective.

The Safer Internet plus Programme has had four action lines:

- Fighting illegal content
- Tackling harmful content
- Promoting a safer environment
- Awareness-raising

The launching of **national hotlines** is seen as one of the main achievements of the two programmes. Under the Safer Internet Action Plan a widespread system of hotlines all over Europe in nearly all Member States had been developed, coordinated by INHOPE, the International Association of Internet Hotlines. Hotlines are contact points where end-users can report illegal content on the Internet. All hotlines are working together, *inter alia*, with police, law enforcement and awareness nodes as well as with ISPs, industry organisations and other institutions. Through providing funding for hotlines[1], the Commission "has made a significant contribution to combating illegal content"[2]. According to INHOPE[3], hotlines have been sending a steadily increasing number of reports on illegal content to the police. In the second half of 2005, the number of reports increased by 16% compared to the first 6 months. In 2006 the European hotlines received 96.497 web based reports of which 29.550 (31%) were transferred to the police (according to INHOPE)[4]. Some spectacular international law enforcement operations were initiated by reports received by Hotlines, such as in 2003 the “Marcy" operation, which led to investigations against 26,500 persons in 166 countries.

---

1 Annex 1 to the Safer Internet Plus programme decision list up 4 actions.

2 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 23

3 Source: INHOPE website: http://www.inhope.org/fr/news/press_release.php?id=20060426. The INHOPE Association is a network organisation for Internet Hotline providers. Its mission is to eliminate child abuse material from the Internet and protect young people from harmful and illegal uses of the Internet.

4 These figures refer to EU Member State Hotlines only. They furthermore exclude reports relating to newsgroups and e-mails, i.e. reports not taken from the public. For the period September 2004 to December 2006 the global INHOPE network received, according to the *2007 Global Internet Trend Report,* on average 35,000 reports per month from the public and forwarded in this period a total of 162,000 reports to law enforcement (INHOPE, September 2007, p. 23 and 67, unpublished).

The evaluations of the existing hotlines produced evidence that they are offering a useful, relevant, and effective service.

The development of **awareness nodes** (national contact points) in nearly all EU Member States is considered to be another major achievement. Awareness raising is regarded as a crucial need. It must address itself to different target groups such as local and national media, children, parents' organisations, schools or policy-makers[5]. Under the Safer Internet plus programme the system of awareness nodes is being complemented by Helplines which allow children to receive one-to-one advice on online-related experiences and issues. The evaluation reports underline the key importance of awareness-raising. They highlight the role of the Commission in initiating and launching awareness-raising initiatives across Europe.

Even if the awareness nodes often did "not get the appropriate support from national authorities and the media and are not given a high enough priority on the public policy agenda of national governments"[6], "awareness levels have significantly improved in all Member States"[7]. According to the 2005 Eurobarometer survey, the 41% average **awareness level** of the EU15 countries in 2003 has increased to 54% in 2005 in the 15 "old" Member States[8]. "Member States with relatively lower awareness levels (below average in 2003) made 22.2% progress during this period"[9].

Both the hotline and awareness network have ties with actions in other countries around the world, and have strong visibility in relevant forums. The most visible events in this context are the **Safer Internet Days,** which since 2004 have been celebrated annually at the beginning of February and since 2005 have been organised under the patronage of Commissioner Viviane Reding. The participation rates demonstrate well how the visibility of and the interest in the Community actions have been increasing over the years:

In 2005 65 organizations from 30 countries took part, and the activities included the launch of a storytelling competition for children including personalities such as Princess Alexandra of Denmark and President Grimssson of Iceland.

In 2006 a total of 37 countries and around 100 organizations participated in the Safer Internet Day. In addition to the many national, regional and local events, there was a worldwide "blogathon" for safer Internet: a wide range of organizations active in promoting Internet made postings on the blog and invited comments from visitors, children, schools and parents. The blog, which included content in several languages, had a geographical focus that moved west through the global time zones, from New Zealand to Argentina.

In 2007, more than 200 organisations from 43 countries participated in activities around the world, and far-reaching "extremely high"[10] media coverage could be noted: the EU awareness nodes alone (the national awareness points co-funded by the Community and networked under INSAFE) reported a total of 1,256 media items[11], including a TV spot[12] shown various

---

5 Final evaluation of the implementation of the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks - COM(2006) 663, p. 5.

6 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 42.

7 Final evaluation of the implementation of the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks - COM(2006) 663, p. 5.

8 Eurobarometer study 2005: Safer Internet, p. 41 http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf

9 Ibid. p. 41.

10 Safer Internet Day 2006. Activity Report, Insafe/European Schoolnet February 2006, p. 3.

11 Ibid.

12 Called in its original German version "Wo ist Klaus"?

times on 7 countries[13], the reports however being incomplete and not covering the whole of 43 countries worldwide.

Following the evaluation reports, self-regulatory initiatives instigated by the Commission were successful and "according to the Internet Watch Foundation extremely successful in developing self-regulation in the UK. The SIAP enabled a monumental shift towards widespread awareness amongst service providers"[14]. A further successful example is the agreement with leading European mobile operators on protecting minors using mobile phones, initiated by the Commission and signed on Safer Internet Day 6 February .2007. To implement the European Framework, signatory operators and content providers committed themselves to developing national self-regulatory codes by February 2008[15].

After having selected 4 projects for preparatory actions in 1998, 37 projects were selected for funding under the first phase of the **Safer Internet Action Plan** between 1999 and 2002 (12 hotline, 12 awareness raising projects, 13 projects on rating and filtering systems, 2 service contracts on self-regulation and awareness exchange). Around 13.37 million € were spent. During the extension period of the Safer Internet Action Plan (2003 - 2004) 22 hotline, 25 awareness raising and 5 thematic projects were supported. The Community funding was of around 14.4 Million €. Following the call for proposals 2005 33 contracts were signed under **Safer Internet plus** for a total EC funding of around 10.87 million € (14 hotlines, 16 awareness projects including 10 helplines, 2 thematic networks). The Call 2006 allowed selecting 15 projects (total budget around 4.45 million €), including 6 Hotline, 8 Awareness and 2 Helpline projects, 4 pilot/thematic and user empowerment projects[16].

A further call for proposals has been published in 2007, and a final call will take place in 2008. This Impact Assessment is drawn up to see whether further action is required after the end of the current programme on 31 December 2008.

1.2. State of play: Legislation

Risks for and negative impacts on the child can result from being exposed to illegal content and conduct or to legal, but harmful, content and conduct. Although the issues and the international context are complex, the EU (and the Council of Europe) has set certain Europe-wide standards, clarifying legal issues through various recommendations and directives concerning the protection of minors and human dignity, electronic commerce, privacy and electronic communications and child sexual abuse images.

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 to deal with.

The conceptions of what is to be considered to be illegal vary from country to country. What is regarded as "illegal content" and "illegal conduct" is defined by the applicable national law. Despite many common features, there are also significant differences of details between the laws of Member States (and of third countries where content may be produced or hosted).

The primary method of **dealing with illegal content and conduct** is for the law enforcement bodies to prosecute the offenders and bring them before the courts. There may also be regulatory bodies responsible for taking action to enforce certain rules (such as consumer protection) or there may be parallel civil remedies (as with copyright infringements).

---

13 Germany, Belgium, Denmark, Iceland, Slovenia, Spain, Czech Republic.

14 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 26.

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

16 Some projects combine the functions of Hotlines and awareness nodes and in 2 cases of Helplines.

When considering online technologies, this process is complicated by the fact that the elements of the offence may be spread out over different countries; a child abuse image produced in one place, but hosted in a second and downloaded from all over the word; abusers have been known to travel over country barriers to meet up with children for abuse after having met them online. It may therefore be difficult to exercise jurisdiction over the prime culprits. International co-operation is therefore vital.

Harmful content and conduct is content / behaviour which parents, teachers and other adults consider to be harmful to children. Definitions of what is considered harmful to children again vary across countries and cultures; it can range from pornography and violence to racism, xenophobia, hate speech and music, self-mutilation, anorexia, and suicide sites. There may also be legal provisions restricting distribution of harmful content to adults only (legal pornography, for instance). Also here differences in details between the laws of Member States and of third countries are noticeable.

A variety of means exist **to deal with harmful content**, all of which need to be used in combination in order to increase their effectiveness: enforcement of legal provisions, self-regulation, and technical means such as filtering. Awareness-raising and education play a fundamental role as they help to empower children for a better and safer use of these media, enable parents and educators to better protect children and lead to a better visibility of child safety issues on the agendas of the decision-makers.

In the area of illegal content and in the regulation of distribution of harmful content, the primary liability of content providers is still largely a matter of national law. Member States also differ in the sensitivity, as for example to public exposure of nudity and sexual activity and to how serious it is seen that children are exposed to nudity, violence and other potential harmful content.

Instruments exist which lay down rules that Member States are required to implement. The list of legislative measures attached as Annex 1 covers well the field of online child protection. The impact assessment therefore **does not examine the need for new legislative measures**. It does examine ways of complementing and **not duplicating** what has already been decided through the legislative instruments.

The envisaged new programme will also take into account the actions launched under other programmes and initiatives, namely "Prevention of and Fight against Crime", "Daphne III" and Media Literacy"; it will build on and complement them so as to avoid duplication and to maximise impact. It finally considers the tasks of ENISA which carries out risk assessment and risk management methods to enhance the users' capability to deal with information security threats, security being deemed as vital for the functioning of computers, mobile phones, banking, the Internet etc. A common interest exists where awareness of children and young people is promoted for this type of security issues (e.g. phishing, identity theft). For this reason cooperation is envisaged when it leads to the mutual reinforcement of activities.[17]

The **legal basis** will be **art. 153** of the Treaty Establishing the European Community on protection of the consumer, which was the article used for the legal basis agreed by the European Parliament and Council for the original Safer Internet Action Plan in 1999, for the 2 year extension of the Action Plan in 2003 and for the Safer Internet plus programme.

---

[17] The INSAFE network co-ordinator chaired a working party which produced an awareness-raising handbook for ENISA and ENISA took part in the 2007 Safer Internet Day blogathon. The 2007 theme was “Crossing Borders” and examined user rights and responsibilities on the internet.

1.3. Lessons learnt from the past

The most recent programme evaluation, published in 2006[18] and carried out by independent experts, gave – after the evaluations dating from 2001 and 2003 – again a positive assessment of the achievements of the preceding programmes, underlining their significant contribution in dealing with the risks to children in the online environment. The evaluators recognised the Community action as a relevant and effective programme and recommended that it "should continue". The European Union is seen as a "pioneer which identified at an early stage the issue of illegal and harmful content on the Internet as a serious and important political question of a global dimension"[19].

More specifically, it was concluded that the network of national hotlines and of awareness nodes in nearly all EU Member States are a major achievement of the programme. The "Safer Internet Day" is recognized as a valuable opportunity to improve communication among stakeholders and to reach out to the broader public. At the policy level the programme has been successful in putting online child safety firmly on the agenda of the EU and the Member States. Stakeholders agree that the programme's original objectives, priorities and means of implementation still apply, and that the action lines are appropriate mechanisms for the fulfilment of the objectives. A particular feature is the bringing together of disparate organisations such as child protection NGOs and software development houses and ISPs – organisations with very different aims and cultures.

A series of specific recommendations were formulated in the evaluation reports and in the Eurobarometer:

- To enhance the Hotlines' cooperation with the police
    - The cooperation between hotlines and other stakeholders, in particular with police and law enforcement, is recommended to be strengthened. Collaboration and co-ordination procedures between hotlines and the police should be reviewed and further developed in order to make the fight against illegal content as effective as possible. Hotlines should receive feedback from the police as in some cases a better follow-up of reports is required.
- To increase the visibility of hotlines in public
    - The launching of national hotlines is seen as one of the main achievements of the action. However, the majority of Internet end-users still have little or no knowledge about the existence of hotlines. In most of the countries, the awareness of the existence of hotlines does not reach 10 % of the totality of Internet end-users. It is inter alia recommended to exploit better the potential of synergies between the awareness and the hotline networks.
- To devote a higher proportion of the programme budget to awareness raising
    - Awareness-raising is considered as a crucial need. Numerous techniques, tools and materials, according to local needs, have been developed and should be spread throughout the networks and stakeholders. A higher budget would allow financing additional efforts.

---

[18] Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006.

[19] Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 4.

- To focus awareness-raising more on specific target groups, especially to pursue tailored strategies to address children, parents or teachers
- To focus more on children under 10 who are already heavy users of Internet and mobile phones
    - Awareness-raising should focus more on specific target groups. In many cases, activities are considered to reach only limited numbers of target groups, due to their heterogeneous nature (stakeholders such as local and national media, parents' organisations or schools). As particularly children under 10 have been catching up in the level of use of online technologies the awareness network should pursue tailored strategies to address them.
- To provide information through channels to suit the needs of the parents and the age of the children (schools, ISPs, media)
    - To reach the target groups better and to maximise the effectiveness of awareness raising the evaluators recommend to exploit all possible information channels in a broader way.
- To promote more active involvement by the media in awareness campaigns
    - The better involvement of media in awareness campaigns is regarded as a key tool for reaching a large number of children, stakeholders and citizens. According to the evaluations there is room for intensifying the media's engagement.
- To facilitate discussion among national administrations (e.g. education ministries) on school education concerning safer use of online technologies. To involve children and young people in identifying problems and designing solutions

Children and young people need to be reached at a very early stage, but "Internet Education" is currently insufficiently integrated into the regular curricula of schools in most Member States. Discussion among national administrations (e.g. education ministries) should therefore be facilitated to examine how safer use of the Internet can be brought into the schools.

- To encourage wider involvement of ISPs and other relevant industry players
    - It is recommended to involve the industry more systematically and to exploit their potential to contribute better to make the Internet environment safer for children.
- To encourage industry self-regulatory solutions at European level; to foster the exchange of best practices, *inter alia*, of codes of conduct, content labelling and rating systems
    - The establishment of self-regulation standards should be promoted. This includes also content labelling and rating systems which continue to be an important element in making the Internet a safer place for minors. Even if some encouraging developments in industry self-regulation, codes of conduct and best practices, inter alia in the field of video games and mobile content, were noted, this leaves still room for actuation and improvement.
- To promote the adoption of age verification systems
    - Age verification is regarded to be a promising tool for protecting children from inappropriate content viewing. Existing systems and technologies need, however, to be further developed.
- To develop actions taking account of changing risk situations (e.g. chat-rooms, Instant Messaging Services, peer-to-peer technologies)

- The evaluators point out that new risk situations arise for children with the further diffusion of new Internet enabled end-user devices like "3G" mobile phones and new practices such as social networking (including chat linked to the use of webcams), Internet Blogging or File Sharing. They recommend to map possible future technological developments and user options, to analyse the implication of convergent services and new modes of communication on the safety of children and on user behaviour and to disseminate the results of such analysis largely.

- To continue to engage with actors external to the European Union
    - In view of the global nature of the Internet safety problem the evaluators recommend to reinforce engagement with actors external to the European Union. Specific focus should be given to the cooperation with Candidate countries, Russia and the Ukraine.

The lessons learnt during the years of running the Safer Internet Action Plan and the Safer Internet plus Programme surveys have been taken into consideration when defining the objectives below.

2. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

The Commission launched a consultation of interested parties consisting of an online Public Consultation which ran from 12 April 2007 until 7 June 2007 and of the "Safer Internet Forum 2007" (Luxembourg, 20-21 June 2007). The "core principles" as defined in the Communication on the Collection and Use of Expertise by the Commission: Principles and Guidelines; COM(2002) 713 final, i.e. seeking high quality of advise, ensure openness and effectiveness were rigorously respected.

The **online public consultation**[20] was structured around three topics:

- Fighting illegal content
- Fighting harmful content
- User- generated content and online communication

The questionnaires focused on specific risk situations for children and dealt with a broad variety of possible measures which could make the Internet a safer place. The public consultation gathered 92 contributions, from a range of stakeholders: Industry actors and associations, associations (children's rights organisations, consumer organisations, trade unions and political movements), hotlines and awareness nodes, public administration bodies (law enforcement, regulators, governments etc), researchers and universities and a number of individuals. The individual responses are published on the web[21].

The **Safer Internet Forum** is a European discussion forum for representatives of industry, law enforcement authorities, child welfare organisations and policy makers to exchange experience and knowledge. It provides a platform for national co-regulatory or self-regulatory bodies to discuss ways in which industry can contribute to creating a safer online environment for children and fight against distribution of illegal content, such as child abuse material.

---

[20] Published on:
http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm
http://ec.europa.eu/yourvoice/consultations/index_en.htm
http://ec.europa.eu/information_society/activities/consultations/index_en.htm

[21] http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm

The Forum 2007 focused on specific risks for children related to the use of the Internet and online technologies. It was composed of three workshops and a plenary session for discussing relevant issues with stakeholders, who had the opportunity to give input to the public consultation in advance to the possible follow-up programme from 2009 to 2013 and it gathered 125 participants and more than 20 keynote speakers from 29 countries, from the same group of stakeholders as the public consultation.

The three workshops dealt with:

1. Online-related sexual abuse of children, in particular grooming
2. Assessing the need for awareness-raising for creating a safe online environment for children
3. The impact and consequences of convergence of online technologies for online safety.

Ample documentation on the results of the public consultation are published on the web, i.e. the minutes of the workshops, speakers' presentations, and a Summary Report on the results of the public consultation.[22]

During the Impact Assessment process the lead DG was supported by a **Steering Group** which was composed of members of those Commission services which deal with related areas or which have tasks to Impact Assessment, legal, procedural and budgetary issues.[23]

Opinion of the Impact Assessment Board

The draft Impact Assessment was presented to the Impact Assessment Board on the 7th November 2007. The Board examined it and delivered its final opinion on the 3rd December 2007. The following main recommendations for improvements were suggested by the Board:

– the rationale of the options should be better explained or the set of options reconsidered
– the lessons learnt from current and previous programmes should be explicitly reflected in the policy options.
– links with other Community initiatives in the field of internet security should be clarified
– the report should explicitly discuss the possible social and economic impacts on third countries.
– the report should include summary of the view of the respondents, specify which services participated in the inter-service steering group, strictly separate the problem definition and objective setting and the distinction between option description and impact analysis.

In response the recommendations of the Board, a number of changes were introduced into the draft Impact Assessment. Explanation of the rationale for the choice of options was introduced in chapter 5.1. The options differ essentially in the intensity with which they tackle the risks identified in the problem definition and in which they respond to the given objectives, to "lessons learned" and in the costs of the proposed measures. Actions under each option are described more concretely and the reasons for a relatively modest financial difference between Option 1 and 2 are clarified.

Lessons learned from the previous programmes and evaluations are explained in chapter 1.3. The new section in chapter 4.6 provides explanation as to how the experience was reflected

---

22 http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm#results

23 SG D.01, SG C.01, BUDG B.05, EAC A.04, JLS D.02, MARKT E.02, SANCO B.01, SJ.

when formulating the objectives and options. Links with other Community initiatives in the field of internet security are further explored in section 1.2, particularly with regard to ENISA.

Impact on third countries is discussed in the analysis of impacts for each option and is taken up also as a criterion of comparison of options in section 7.1.

The newly added Annex 3 provides a summary of the view of respondents to the public consultation; internal steering group participants are mentioned in this section (footnote). Description of problems is clearly separated from objectives. Due to the wide variety of issues treated in the IA and due to additional requirements for explanation and input, it was not possible to stick strictly to the recommended limit of 30 pages.

3. PROBLEM DEFINITION

3.1. Problem analysis

The rapid development of Internet and other information and communication technologies has given rise to a completely new economic sector and to new rapid flows of information, products and services across the internal and external borders of the EU. Although this contributes considerably to economic growth in Europe, it also has a negative side which manifests itself in the distribution of illegal and harmful content and in behaviours which are specifically harmful for the most vulnerable citizens - the children. New problems arise with the further diffusion of new Internet enabled end-user devices like next generation mobile phones and new practices such as social networking (including chat linked to the use of webcams), Internet Blogging and File Sharing.

The rapid development and uptake of online technologies in Europe gives children and young people great opportunities for being creative, for cultural and technological understanding, for communication and for learning. Internet penetration in the home stands at more than 42% for citizens and exceeds 90% for businesses and schools. According to the 2005 Eurobarometer survey internet use by children aged 17 or younger has increased from 45% in 2004 to 48%. In the 15 'old' Member States, the proportion of children using the Internet now stands at 51%, with highest recent growth rates in Belgium, Greece and France[24]. New Member States are catching up. In Lithuania, for example, the use of the Internet has augmented between 2005 and 2007 from 42 % of the population to 54 %. Amongst children the percentage increased from 63 % to 74%[25] (this takes into account that children who do not have access at home, may have access at school or other places). Significant growth was also recorded in Slovakia, Malta and Estonia[26].

In the last Eurobarometer survey (2007), which covered 29 European countries (27 MS and Norway and Iceland), 9-10 year old children typically said that they connect several times per week, the minimum connection time being half an hour to one hour. 12-14 year old children generally use the Internet daily, often for one to three hours[27]. This survey also confirms that most European children use mobile phones: The vast majority of the interviewed children

---

24 Special Eurobarometer Safer Internet, May 2006, p. 26.

25 Human Resources Research Department, TNS Gallup, Safer Internet Report, April 2007.

26 Special Eurobarometer Safer Internet, May 2006, p. 26.

27 Safer Internet for Children. Qualitative Study in 29 European Countries. Summary Report, May 2007, p. 6.

have a mobile phone - overall three out of four of the 9-10 year old, and nine out of ten of the 12-14 year old[28].

Most of the risks that children and young people encounter are not specific to them – the risks are the same for adults – and neither are they confined to their use of online technologies; they encounter the same risks in other (real life) arenas as well. However, children are more vulnerable than adults. The **scope of the programme** is aimed at children and the adults responsible for them. The risks for adults in general and for companies are addressed by other Commission initiatives. The approach of the programme is to look at the **child-specific dimension of risks** related to the use of online technologies.

At the same time, risks in the online and offline environment are converging, and although most children and young people are aware of potential risks and of precautions, they do not necessarily take the necessary precautions or act in the safest way when they communicate in the online environment. For example, the possible harm to children playing (video) games (for instance concerning games of a violent or sexual nature) will be the same whether they are played online or on game consoles at home.

As users of online technologies, children and young people can be seen as recipients, participants and actors in the online environment. As **recipients** they may be exposed to content that might be considered harmful to them, and that might cause considerably trauma or incite them to inflict harm on themselves or others. As **participants**, they participate in the communication with others in the online environment, including potential abusers who use online technologies to target children and befriend them (grooming). As **actors**, children generate content in a creative manner, and might inflict pain on others through bullying and abuse.

Both as users of online technologies and as victims of abuse, children are potentially the most vulnerable, and become the victims of grooming for sexual abuse or of abuse which is documented and circulated online (child sexual abuse material). For abusers, they are easy to target, since they are open to deception and exploitation and may have not yet developed defence mechanisms when being confronted to inappropriate content.

Technologies, communication networks, media, content, services and devices will increasingly undergo **digital convergence**. Devices and platforms are already "talking to one another", content is becoming available in new, diverse formats and can increasingly be delivered independent of location or time, and personalized to individual citizens' preferences or requirements. Improvements in networks, faster broadband, combined with new compression techniques, create new and faster distribution channels and trigger new content formats and services as well as new forms of communication. In the public consultation it was pointed out that the increased accessibility to the Internet from various devices will make **children vulnerable** through more access points. New technologies have for example created ways of "round the clock bullying". Whereas previously bullying was confined to times and places where children are in groups, such as at school, technology provides 24 hour communication access.

New technologies include ever-increasing processing power and storage capacity of computers, broadband allowing distribution of rich content such as video which requires high bandwidth, and the increased capacity of the latest "3G" generation of mobile telephones. This new generation of mobile phones allows distributing video content and to access the

[28] Safer Internet for Children. Qualitative Study in 29 European Countries. Summary Report, May 2007, p. 7.

Internet and for example online chat rooms. The technological changes allow an increase in the volume as well as in the types of content distributed. The use of high speed Internet connections is increasing dramatically. In the twelve months before October 2004, the number of people in Europe surfing the Internet at high speed from home increased from 34.1 million people to 54.5 million people – an increase of 60%. The largest increases occurred in Italy (120%), and in the UK (93%)[29]. **Broadband** users are spending significantly more time online, using the web more often, and visiting more websites than their slower, dial-up counterparts. This increase in connectivity by children will see a corresponding increase in benefits for them but also risks of "collateral damage".

Children are often the first to take up and use new technologies. However, currently we are not prepared to understand these changes in time and to develop strategies to deal with the emerging risks. The challenge is to understand these changes in time and to develop counter-strategies as new risks materialize.

Technical tools cannot solve the problems of Internet safety alone, but they are a necessary element within a multi-faceted Internet safety policy. Age recognition systems can restrict access to inappropriate content for minors of age, filtering technologies can support parents in regulating better what their children have access to, and victim identification (face recognition) is an important requirement within the investigations of law enforcement bodies. However, the **existing technologies suffer** of many shortcomings and need to be better adapted to practical needs and requirements.

According to the 2005 Eurobarometer survey[30], 48% of the parents in the EU-25 claim to use filtering or blocking tools to keep their children away from illegal or harmful content in Internet. However, a study carried out by the London School of Economics[31] comes to the conclusion that only 15% of parents in the UK say they install filtering software. This might indicate that many parents think or said they have blocking software installed on their children's PC when in fact they did not. A continued focus on promoting the uptake of **parental control tools** is needed.

The industry is an important actor in the field of online child safety; **self-regulation systems** are a promising way to reduce illegal content and the access to it. The framework agreement between the Commission and mobile phone operators is a promising step, nevertheless the involvement of the industry has a good potential for additional actions, but it **leaves scope for progress**. Interaction and cooperation should furthermore be sought between multiple stakeholders, including the industry and also NGOs, educational organizations, the media, public authorities etc. The current "Youth Protection Roundtable" project encourages for example a cross-sector dialogue between technology-developers and education specialists aiming at developing strategies for a safer use of the Internet applicable on the level of technology development. More can be done in this respect.

The idea of creating a risk free Internet for children and young people is an illusion; it is a fight which cannot be won. A key element of any policy in this field must inevitably be to empower children, i.e. to equip them with the knowledge to avoid hazards and to deal with

---

29 Research data from Nielsen/NetRatings (http://www.nielsen-netratings.com/pr/pr_041202_uk.pdf)

30 European Commission, Special Eurobarometer "Safer Internet" , published in May 2006, http://europa.eu.int/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf

31 In the framework of the "UK Children Go Online (UKCGO)" project: Livingstone S. & Magdalena Bober, UK Children Go Online: Emerging Opportunities and Dangers, Final Report, London School of Economics, April 2005, http://www.lseac.uk/collections/children-go-online

risks. Currently, public **awareness** is **not sufficiently developed** on all levels to recognize the need of children to be better prepared; the subject of Internet security has neither been introduced sufficiently into the curricula of the Member State school systems. Awareness campaigns on the Member State level could become more effective if the actors involved had better knowledge about successful awareness raising methods and tools concerning online safety in the EU. Awareness raising must become more effective and more systematic.

There is a noticeable **lack of** European comparative **facts and figures**, of robust **statistics** (nationally and Europe-wide). For example, hardly any figures exist on the extent and the forms of online sexual abuse and grooming. As far as knowledge exists it is not pooled at European level; this makes it difficult to access the existing resources and hampers the identification of current knowledge gaps. Ongoing investigations on Member State level are not coordinated within the EU which makes it difficult to find comparable results. A number of issues have not been investigated at all and would need to be better analysed on national and EU level, as for example the ways children act when using communication technologies or the ways offenders use new technologies in view of sexual abuses (how they find and target children, the changing nature of grooming behaviour, the link between consumption of child abuse images and contact sexual abuse etc).

Many of the risks that children encounter when using online technologies are not specific to them – the risks are the same for adults – and they are not confined to their use of online technologies. They encounter the same risks in other (real life) arenas as well. However, they are more vulnerable and can be manipulated more easily. **Children's specific views** on the way the "live with" online technologies and on the way they perceive and deal with risks must be better understood when developing policy strategies. Their direct involvement in such reflection processes can bring added value to it. Up to now, this has not been done.

The answers for dealing with the challenges described above and for fighting risk situations which can cause considerable harm to children (illustrated in the preceding chapter) **cannot** be expected to be provided by **market forces alone**. On the one side the market, i.e. the industries, must play their role wherever they are in the position of doing so. Self-regulation, rating and labelling systems, the use of certain technological solutions (e.g. mobile phone handsets specifically designed for children)[32] are promising ways to protect children better. On the other side market interests, i.e. the profit-making, do not always coincide with child protection issues. MMS services[33] for mobile phones and providing access to the internet via mobile phones[34] are examples for innovative services with promising revenues – the industry does therefore not have a "natural interest" in blocking such functions for children. Or, to give another example, labelling video games or rating content will have the effect of decreasing sales to the age groups addressed. Past experience has shown that **public intervention** is **necessary** to enhance the industry's sense of responsibility[35]. Furthermore, due to their cross-cutting nature, actions to enhance internet safety are not limited to the competences of

---

32 Such a mobile phone can allow parents to block the child's access to the internet or to MMS services, thus avoiding them to view harmful content.

33 Multimedia Messaging Service (MMS) is a standard for telephony messaging systems that allows sending messages that include multimedia objects (images, audio, video, rich text) and not just text as in SMS.

34 The majority of children already own a Web-enabled mobile phone. Due to the high costs MMS and connecting to the Internet by mobile phone is a still a marginal use by children, decreasing rates can however change their behaviours rapidly (see findings in Safer Internet For Children, Eurobarometer Qualitative Study in 29 European Countries, Summary Report, May 2007).

35 Again, the example of the framework agreement concluded between the Commission and mobile phone operators shows that public intervention is needed for enhancing industry action.

industries, they also address to specific functions which can only be taken by the appropriate organisations, such as law enforcement or child welfare organisations (see "target group" definition below).

The **legislative framework** as such offers the legal basis and the justifications *de iure* for interventions. However, in order to be effective real-life interventions are needed. To give an example: To abuse a child, to sell such images via the Internet and to consume them are criminal acts in the Member States, but the criminalisation as such does not prevent a certain number of persons from taking such images and hosting them on servers. In order to fight such pictures reporting is necessary (supported by awareness campaigns), police action is needed (which may be required to work smoothly across national borders), blocking of such content on the side of the ISPs is asked for. All these elements and actors have to be brought together in a way that actions are efficient and effective. The Commission has a coordinating and enabling role in this.

3.2. Specific risks for children and young people

The risks children can encounter when they go online or use mobile phones depend on the kind of activities which they deploy. Children use online technologies for a variety of activities: Finding information for school work, read news, searching for information about hobbies/interests, playing games, participating in competitions and quizzes, downloading, listening and watching music and films, communicating with friends and getting new friends through own home pages, social networking sites, chats, instant messaging services, e-mail and mobile phones. In many cases they also create their own web sites posting personal information, images and opinions of themselves and others.

3.2.1. Exposure to harmful content

Exposure to harmful content can cause psychological trauma to children and lead to physical harm if a child is motivated to inflict harm on other children or on him/herself.

The 2007 Eurobarometer study states that "children often cited this risk... It is confirmed here that a good number of them are disturbed, bothered and in some cases sometimes traumatised by it"[36]. The content most frequently mentioned refers to pornographic images. According to the study "almost all the children questioned seem to have been exposed to them." Furthermore "scenes of extreme violence or torture" are "very often cited… Some children say they are upset by them on a long-term basis." Furthermore, to a lesser extent, “racist” or “Nazi” sites are cited in the context of the study.

In 2003, 44 % of the children who used the Internet had visited a pornographic Web site by accident or on purpose. 25 % has received pornographic material through the Internet. 30 % of the children had seen websites with violent material, while only 15 % of the parents thought their children had seen this[37].

According to the 2005 Eurobarometer survey, 18% of European parents of children aged 17 and younger said that their child had encountered harmful or illegal content on the Internet. Although in the 15 “old” Member States, awareness levels increased significantly since the

---

[36] Safer Internet For Children, Eurobarometer Qualitative Study in 29 European Countries, Summary Report, May 2007, p. 43.

[37] Research data from the SAFT (Safety, Awareness, Facts and Tools) project which has been supported under the Safer Internet Action Plan.

previous survey, 44% of parents stated that they would like more information about how to protect their child from illegal and harmful content and contact[38].

3.2.2. Disclosure of personal information

Children are often interacting with other users in the online environment and generating content. When generating content, such as creating their own web site, they tend to post **personal information**, images and opinions of themselves and others, as well as phone numbers and e-mail addresses. This material is in some cases used by offenders for identifying and locating a child offline or it may cause financial and security risks.

3.2.3. Bullying and cyber-bullying

Bullying can start in the school yard, but it can rapidly move into the sphere of online technology: both the exclusion of peers from online networks and the active harassment takes place on the Internet and through mobile phones.

Cyber-bullying is a severe form of harmful conduct, it "can be particularly distressing, as often there is no escape for the victim; the bullying has a potentially enormous audience, thus extending the humiliation and embarrassment of the victim. It is difficult to stop abusive content spreading and reappearing, which may make it difficult for the victim to move on from the incident, particularly if they do not know who the aggressor is"[39]. It is particularly insidious as it can follow young people wherever they go. "In some cases the degree of bullying or psychological ill-treatment may lead to genuine and, in some cases, dramatic disorders"[40]. The harm caused by cyber-bullying may be even greater than traditional bullying as online communications can be extremely vicious, as it can be done anonymously so that the victim may not know anymore whom to trust. In the school context there are reports of cyber-bullying leading to suicide, school violence, school failure, and school avoidance (overall in the UK).

Children also take photos and films with their mobile phones, sometimes without a peer knowing about it, and post it online or send to other mobile phones. There are known examples of people, not only children, being beaten up for the sake of filming, which can be posted online or sent through mobile phones, a phenomenon called "happy slapping".

A recent study in the UK showed that up to 34% of 12-15 year old children and young people had experienced some form of cyber-bullying. "There is also growing concern from teaching unions that school staff is increasingly becoming the victims of cyber-bullying"[41].

It appears that the actions taken up to now in fighting cyber-bullying need to be more effective.

3.2.4. Advertising and high expenditure

Children are easy targets for **advertising** and for people with commercial interests. They sometimes give away too much personal information, and may as a result receive vast amounts of spam or enter into agreements where the terms are not clear, this again might cause them to get a high expenditure.

---

38 Eurobarometer survey (2005), p. 22 to 24.

39 Home Office Task Force on Child Protection on the Internet: Good Practice Guidance for the Providers of Social Networking and User Interactive Services 2007, p. 9 (unpublished).

40 Safer Internet For Children, Eurobarometer Qualitative Study in 29 European Countries, Summary Report, May 2007, p.9. A recent study in the US states that "'Cyberbullying' hits one third of teens" (http://news.com.com/2100-1038_3-6193723.html).

41 direct.gov.uk/en/Nl1/Newsroom/DG_070668, published 21 September 2007

3.2.5. Security risks

Security risks may cause harm to the computer or to the programmes on the computer, and might even allow somebody to steal your identity and money. Security risks are often caused by viruses entering the computer through a downloaded file, online games, spam mails or hacking (people breaking into your security system). Security risks are as important for adult users of online technologies as for children, and users thus risk breaching security. Even though the effect can be serious for the owner of the computer, the effect/consequence on the child is limited.

3.2.6. Evaluation of information sources

Many children use Internet as a tool for searching information concerning school tasks. Online content may be produced by anybody, even children themselves. Research has shown that even though many parents trust that their children know how to value information they find online, many children do not know this. Again, a critical sense regarding trustworthy information online is something that has to be learned and trained at.

3.2.7. Downloading and copyright infringement

Downloading films, music and games from Internet sources is a popular activity for children as well as for adults. In many cases, this happens through sites providing possibilities for exchange of files between individual users of the Internet, so called file sharing. Games and competitions, ring tones for mobile phones and images can be downloaded from a variety of Internet sites. "Downloading music, films, videos, games or other files is especially widespread in the older groups (12-14 years) of both sexes but with a predominance among boys"[42].

In some cases, the downloaded files contain viruses and worms and in this way impose security risks to the computer and the network. In some cases, the downloaded files **disguise harmful and/or illegal content**.

Sharing music and films online is in many cases associated with **infringement of copyright laws**. The recent Eurobarometer study concludes that "in the vast majority of cases, across all countries, children know that most of the downloads are illegal, but they minimise, deny or justify the practice. Whether it is “illegal” or not is not always clear"[43].

3.2.8. Grooming

In 2003, in a report covering 4 European countries, 4 out of 10 children who had chatted on the Internet said that people they had only met on the net had asked to meet them in person. 14% of the children had met someone offline that they first met on the Internet, while only 4 % of the parents thought the children had done so[44].

Adults of all ages who target children for sexual abuse are active online, and take advantage of the fact that children easily trust other people and that they are relatively willing to disclose personal information. The process by which a person befriends a child with the intent to abuse him/her is called **"grooming"**, and the term is used in particular for online activities. Abusers sometimes target children through the relative privacy of the Internet and mobile phones by

---

42 Safer Internet For Children, Eurobarometer Qualitative Study in 29 European Countries, Summary Report, May 2007, p. 23.

43 Ibid., p.53.

44 Research data from the SAFT (Safety, Awareness, Facts and Tools) project which has been supported under the Safer Internet Action Plan.

pretending to be children themselves, or by befriending vulnerable children in the online environment; on chats, through social networking sites and dating sites.

There is noticeable lack of statistics and hard data on the numbers of children ensnared through grooming, be it on national or EU levels[45]. A recent study in the UK speaks of "one third of 9-19 year olds daily and weekly users have received unwanted sexual… comments online or by text message"[46]. This does, however, not describe the specific situation of a grooming process.

Grooming has severe consequences on children. Research shows that children seldom disclose to their parents or other adults about such contact and even in the cases where the contact is stopped before the abuse has taken place, sexual encounters/conversations online can be very disturbing for the child. In some cases, the abuser does not target the child with sexual conversation, but tries to get close to the child by responding to his/ her personality and interests, being the child's best friend. If abuse takes place, the effect on the child is very serious and deeply traumatizing. Since grooming implies befriending the child, the child experiences a severe breach of trust and sometimes great disappointment that a person they trust actually has hurt them.

There is also a noticeable lack of awareness in Member State authorities and the public about the severity and frequency of this severe form of harmful conduct.

3.2.9. Child sexual abuse material

Internet has also become one of the main distribution channels for **material** (images, films, audio files etc) **depicting sexual abuse of children**. Despite increased efforts in the international community aimed at reducing the production and online dissemination of sexual abuse material, the amount of material distributed does not seem to decrease. This material can be produced in a variety of ways and in a variety of circumstances, in some cases involving online grooming techniques, in other involving domestic abuse.

New figures from the UK-based Internet Watch Foundation (IWF) 2006 Annual Report, launched 17 April 2007, show the severity of online child abuse content is increasing, with a four-fold rise in images depicting the most severe abuse, such as penetrative and sadistic sexual activity. Domestic images are replacing commercially made ones. This trend reflects an apparent growing demand for purchasing more severe images with nearly 60 per cent of commercial child abuse websites selling child rape images. 29 per cent of all potentially illegal child abuse URLs known to the IWF contains the most severe abuse[47]. "The trend is frightening and requires concerted action"[48]. There is also a decrease in the age of abused children and an increase in the number of new abused children[49]. Even babies (rape) are presented.

The Internet Watch Foundation has estimated that the number of sites with this type of illegal material has increased with 1500 percent in the period 1997-2005.

---

45 See Safer Internet Forum 2007, workshop 1: 'Online-related sexual abuse of children, in particular grooming', Final report.

46 Home Office Task Force on Child Protection on the Internet: Good Practice Guidance for the Providers of Social Networking and User Interactive Services 2007, p. 25 (unpublished).

47 http://www.iwf.org.uk/media/news.196.htm

48 Safer Internet Forum 2007, workshop 1: 'Online-related sexual abuse of children, in particular grooming', Final report, p. 15.

49 Safer Internet Forum 2007, workshop 1: 'Online-related sexual abuse of children, in particular grooming', Final report, p. 15.

The ways of online *dissemination* seem to *diversify*. It seems furthermore that there is a trend to host child abuse images more and more outside the EU, for example such pictures are hardly found any more on German servers[50]; such material is furthermore increasingly disseminated through the web 2.0, but there is little knowledge and no reliable figures on the size of this problem.

The consequences for the children abused and depicted in the material are severe, and only a percentage of the children have been identified and rescued from the abusive situation. Interpol's Child Abuse Image Database contains 550.000 images of 20.000 individual children. Of these, only around 500 of these children have been identified and rescued in the time since the establishment of the database in 2001[51].

The public consultation called therefore for a more robust programme, with more resources deployed.

3.2.10. Video games

Playing games is one of the most popular online activities for European children[52]. Games may be played offline with one or more children present in the same place, but online gaming using game consoles or personal computers connected to the Internet is increasing.[53] The discussions about the effects on children of playing video games (encompassing both online and offline games) are diverse. The risks to children include health risks, like addiction and loss of physical health due to time spent in inaction, an augmented and unrealistic view of the world around them and anti-social behaviour. However, the most pronounced worry is the risk that children become more aggressive and start engaging in aggressive behaviour as a consequence of playing games.

Although there are cases where a link has been found between playing violent video games and violent and aggressive behaviour, a consensus does not exist in this area. A recent survey[54] showed that although parents are worried about the risk of the harmful effects of potentially harmful content in games, the players of games themselves and the games industry do not perceive violence in games to make game players less sensitive to real-world violence, and they claim not to loose touch with the real world. In many cases, violence in games is seen as no worse than the violence experienced through TV or films. However, the study also shows that many of the young users (below 15) are disturbed by the violence, in particular the bloody deaths, as well as the fact that the characters that kill the most people win.

The gaming industry operating offline has adopted a rating system (PEGI) which rates games according to content (appropriate age, bad language, violence, sexual content etc). This system has also been adapted to the online gaming world and some new game consoles include blocking devices. However, since parents are not always aware of the risks and possibilities for reducing the risks concerning children's use of online games, information to parents (awareness-raising) is important.

---

50 DER SPIEGEL, 23.7.2007 (http://p2p.p2.ohost.de/artikel/virtuelle_front.htm) which mentions servers in Asia. The IWF 2006 Annual Report speaks of "62% of commercial child abuse domains hosted in US" and "28% commercial child abuse domains hosted in Russia".

51 http://www.interpol.int/Public/News/2007/ChildConf20070606.asp

52 2007 Eurobarometer survey: http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

53 The comScore World Metrix study July 2007: http://www.comscore.com/press/release.asp?press=1521

54 The British Board of Film Classification report on Video Games, 2007: http://www.bbfc.co.uk/downloads/pub/Policy%20and%20Research/BBFC%20Video%20Games%20Report.pdf

Another risk associated to online video games is related to contact with potential abusers. Already, many games combined features of social networking and gaming, and there are likely to be more in the future. For more on this issue, see section 3.2.8.

In order to assess possible actions to deal with the potential harmfulness of online and offline games to children, more knowledge is needed about this issue.

3.2.11. Risks related to new technologies and new forms of communication

The World Wide Web has evolved over the last two years to become an increasingly dynamic and interactive platform. **Social networking** (the term cover also the so-called chatrooms) is one of the new phenomena in the online world."Social networking and user interactive services are now a hugely popular and a compelling activity for many Internet users. These services are considered to be part of a paradigm shift in the evolution of the Internet, which is now frequently referred to as Web 2.0. Web 2.0 represents a fundamental shift away from this model, towards a more dynamic and interactive Internet where the creation of content is decentralised and more controlled by individuals or communities of users"[55].

For example, the number of visitors to a popular site "MySpace" increased from 4.9 million in 2005 to over 67 million in 2006[56].

Social networking sites brought together on a single site diverse "interactive technologies that previously had to be accessed separately or independently: chat, search, email, messaging, blogs, videos and so on. Together they have created a new type of social space where the risks to children and young people are manifested in new and different ways"[57], even if the risks which children are confronted to are largely identical with those already identified in the previous sections. "Potential risks to children and young people using social networking services can include but are not limited to:

- bullying by peers and 'friends';
- exposure to inappropriate and/or harmful content;
- posting illegal or inappropriate content;
- posting personal information that can identify and locate a child offline;
- sexual grooming, exploitation and abuse through contact with strangers;
- exposure to information about self–harm techniques or encouraging anorexia and suicide;
- race hatred;
- glorifying activities such as drug taking or excessive drinking;
- encouragement of violent behaviour such as 'Happy Slapping'[58];
- physical harm to young people in making video content, such as enacting and imitating stunts and risk taking activities such as playing 'Chicken' on railways; and
- leaving and running away from home as a result of contacts made online"[59].

---

55 Home Office Task Force on Child Protection on the Intenet: Good Practice Guidance for the Providers of Social Networking and User Interactive Services 2007, p. 4 (unpublished).

56 Ibd. p. 5.

57 Ibd. p. 5.

58 Happy Slapping is a term which typically describes the filming of violent attacks on mobile phones. Happy Slapping has been called a youth craze which began in school playgrounds in which groups of teenagers slap or mug unsuspecting children or passers-by while capturing the attacks on camera or videophones. http://journalism.bournemouth.ac.uk/lnolan/whatis.html

Another new phenomenon is the young people's use of **webcams** - a new and growing concern. Webcams raise challenges for the safety of young internet users. In a number of cases young people have been intimidated or manipulated into recording images of themselves using webcams and sending them to individuals they meet online. Children and young people may use the Internet to engage in cyber-flirting or cyber-sex with their online 'friends'.

Both behaviours can cause various **threats**. Recent investigations conducted on young persons between the ages of 13 and 19, reveals that a high percentage of girls have been requested "to do something sexual in front of a webcam"[60]. A possible consequence can be that this may lead to real-life meetings for sexual abuse (e.g. images used for coercion).

3.2.12. Risks related to mobile phone use

More and more children are using **mobile phones**. In some European countries, the use of mobile phones by children is greater than their use of Internet. The mobile phones are becoming more sophisticated, most of them carry cameras, and some allow for accessing Internet. The risks concerning mobile phone use are the same as for use of other online technologies like the Internet: high expenditure, bullying, grooming, and exposure to harmful content. However, the risks might become even more pronounced as the mobile phones is seen as even more private than Internet use.

The results of the public consultation on "Child safety and mobile phone services" which the Commission (DG INFSO E.06) carried out between 25 July and 16 October 2006 underlines this: "There is a wide consensus that, along with all the benefits that mobile phones bring to young people, some risks exist. Main risks identified confirm the evaluation made in the consultation report: harassment and bullying, grooming and sexual discussions, mis-contracting with minors, access to chargeable content, fraud and spam, high expenses, exposure and access to illegal/harmful/adult content, pornography and violence and risks concerning children's privacy, in particular due to the inappropriate use of camera phones and location services"[61].

3.2.13. Health risks

There are concerns about the possible **health risks** linked to the excessive use of mobile phones. There is also worry about the possible impact that radiation emitted from mobile phones might have, in particular on children and young people.

Some children spend a lot of time in front of their computers or using their mobile phones, to play games or to gamble, and develop **addiction** to these activities. As a consequence, they may break contact with friends, spend less time on physical activities, and even drop out of school.

---

59 Home Office Task Force on Child Protection on the Internet: Good Practice Guidance for the Providers of Social Networking and User Interactive Services 2007, p. 8.

60 Study by the 'My Child Online Foundation' (2006), quoted in Home Office Task Force on Child Protection on the Internet: Good Practice Guidance for the Providers of Social Networking and User Interactive Services 2007, p. 11.

61 Summary of the results of the public consultation " "Child safety and mobile phone services", p. 3 (http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_mobile/public_consultation_rsults_en.pdf).

3.3. Who is affected? Target groups

Noticing that the risks for children in the online environment are great, and that they have increased during the years since 1996, the **main target group** of the proposed programme will be **children and young people**. But it is not only the children who need to be addressed:

- Parents, carers, including medical staff and therapists, teachers and other adults responsible for children have a special role in educating and supporting children and young people in how to stay safe online.
- State authorities, i.e. governments (national, regional and local), official bodies with responsibility for industry, education, consumer protection, families, children's rights and child welfare, law enforcement authorities (police, public prosecutors and judges), and regulators (media, data protection) are concerned with the issue of illegal and harmful content in different contexts.
- The industry is concerned as it has a strong interest from a business point of view in a safe environment engendering consumer confidence. At the same time content providers, technical intermediaries (including network operators and Internet Service Providers), mobile network operators, as well as industry self-regulatory bodies are typically interested in operating in an environment in which undue restrictions and the burdens of regulation do neither hamper their activities nor produce additional costs.

Industry already plays, and will increasingly come to play, an important role in helping to provide solutions for a safer and more trustworthy environment because of their expertise, their technical role in provision of services and their contacts with end-users. Network operators, for example, have a clear technical capacity to identify and prevent risk situations for children, but also manufacturers of software could make their products safer.

- A variety of non-governmental organisations are working on issues related to child safety online. These are organisations active in the fields of consumer protection, families, children's rights, child welfare and civil society issues. Other activists are concerned at the implications for civil liberties of measures taken to restrict circulation of content or access to content, particularly where measures taken ostensibly to restrict access by children to potentially harmful content also restrict access by adults to content which is legal for them.
- Finally universities and research institutes do investigations in fields which improve our knowledge base, as for example understanding better how children use online technologies, how the education can be efficiently organized, how perpetrators operate and the way they use online technologies. Furthermore, they can investigate new technical safety solutions and technology-enhanced support systems for crime investigation etc.

4. OBJECTIVES

4.1. General objective and Specific objectives

The envisaged new programme has the **general objective** to protect children better against risks which can manifest when using the Internet and other communication technologies.

Based on the consultation process, the lessons learned from the past (especially those derived from programme evaluations and Eurobarometer) and the risks for children identified, the envisaged initiative will have the following **4 specific objectives**:

- Reducing illegal content and tackling harmful conduct online
- Promoting a safer online environment

- Ensuring public awareness
- Establishing a knowledge base

Additional **Operational objectives** specify a series of targets which are expected to facilitate attainment of the above general goals:

4.2. Illegal content and harmful conduct/content

- Providing the public with contact points for reporting online illegal content and harmful conduct
- Dealing effectively with harmful conduct online, in particular grooming and bullying
- Stimulating development and application of technical solutions for dealing with illegal/harmful content and harmful conduct online

4.3. Promoting a safer environment online

- Encouraging industry engagement in creating a safer online environment by stimulating development and implementation of self-regulation systems
- Stimulating cooperation between relevant stakeholders concerning promoting a safer environment and tackling harmful content

4.4. Awareness-raising

- Empowering users to stay safe online
- Providing the public with a coordinated and effective effort to raise awareness and to disseminate information about risks and safety measures
- Stimulating enhancement and development of awareness raising methods and tools concerning online safety
- Stimulating the involvement of children and young people in creating a safer online environment

4.5. Establishing a knowledge-base

- Encouraging a co-ordinated approach concerning investigation across the EU with a view to increasing child safety online
- Ensuring stable knowledge of updated information concerning children's use of online technologies and the subsequent risks
- Broadening knowledge concerning children's own strategies for dealing with online-related risks
- Promoting studies on online-related sexual exploitation of children

4.6. All actions

- Enhancing co-operation, exchange of information, experience and best practice between relevant stakeholders on EU and international level.

The (specific and operational) objectives take the lessons learned / recommendations described in section 1.3 in the following way into account:

- The objective "Providing the public with contact points for reporting online illegal content and harmful conduct" (section 4.2) takes up the recommendations to provide "the public with contact points for reporting online illegal content and harmful conduct" and (in combination with enhanced awareness raising; section 4.4) "to increase the visibility of hotlines in public";

- The recommendations "to devote a higher proportion of the programme budget to awareness raising" and to "focus awareness-raising more on specific target groups, especially … to address children, parents or teachers" are integrated into the objectives under section 4.4 ("Empowering users to stay safe online", "stimulating … development of awareness raising methods and tools", "providing the public with a coordinated and effective effort to raise awareness…");
- The recommendations "to focus awareness-raising more on specific target groups, especially to pursue tailored strategies to address children, parents or teachers" and "to focus more on children under 10 …" are specifically taken up in the objectives under section 4.4 of "stimulating the involvement of children and young people in creating a safer online environment" and of "stimulating … development of awareness raising methods and tools"; and under section 4.5 ("Ensuring stable knowledge of updated information concerning children's use of online technologies and the subsequent risks");
- The recommendations "to provide information through channels to suit the needs of the parents and the age of the children (schools, ISPs, media)" and "to promote more active involvement by the media in awareness campaigns" is introduced into the objectives "Stimulating cooperation between relevant stakeholders concerning promoting a safer environment and tackling harmful content" (section 4.3) and "Providing the public with a coordinated and effective effort to raise awareness and to disseminate information about risks and safety measures" (section 4.4). The first takes also the recommendations "to facilitate discussion among national administrations … on school education concerning safer use of online technologies" up;
- The objective of "Stimulating cooperation between relevant stakeholders concerning promoting a safer environment and tackling harmful content" corresponds to the recommendation of encouraging "wider involvement of ISPs and other relevant industry players";
- "To encourage industry self-regulatory solutions at European level…codes of conduct, content labelling and rating systems" (recommendation) is taken up in the objective (section 4.3): to foster "industry engagement in … development and implementation of self-regulation systems";
- "Age verification systems" (recommendation) fall under the objective "stimulating development and application of technical solutions" (section 4.2), "to develop actions taking account of changing risk situations…" (recommendation) is introduced into the objectives under section 4.2 ("Dealing effectively with harmful conduct online, in particular grooming and bullying") and 4.5, specifically the objective of creating "stable knowledge of updated information concerning children's use of online technologies and the subsequent risks";
- The recommendation "to continue to engage with actors external to the European Union" is introduced into "all actions" (section 4.6).

5. STRATEGIC POLICY OPTIONS

5.1. Formulation of policy options

The aim of the following analysis is to identify the option which offers a convincing / the best range of expected effects (impact) which at the same time can be achieved in a cost-efficient way. When assessing the alternative options, the question will be whether the same effects (the same impact) could be achieved by a lower cost by using a different approach or other instruments.

There are many possible ways to address the issues relating to child safety online and the risks for children. Hence, divers options can be imagined, but they always will respond to two basic approaches: either to limit actuation to certain areas (vertical approach) or to strive for a cross-cutting solution which covers all / as many as possible areas but at different levels of intensity (horizontal approach).

As regards the vertical approach a possible option is that the Commission limits itself to stimulating self-regulatory solutions in the industries, especially as there are some indications of promising results in reducing illegal content and the access to it. The need to enhance such agreements and the positive role which the Commission can play in this respect has been highlighted in the past evaluations. However, self-regulation would definitely not tackle all the risks and challenges by itself. Self-regulation can be part of the solution but within the given limitations only. Many of the issues in the field of internet safety go beyond the reach of industries and require the participation of organisations which have specific missions. This

applies for example to the role of schools in media education or of child care organisations in counselling, advising and supporting children, their parents and other caretakers. Furthermore, it should be noticed that the actuation of industry players can be hampered by conflicting interests in the market.

A basic lesson learned during the implementation of the preceding programmes, a basic conclusion in past evaluations is that any policy for the fight against illegal content, to protect children from illegal and harmful content and from illegal and harmful forms of conduct must, due to the nature of the subject-matter, be of a multi-faceted nature. To be truly effective, several measures and actions will have to be combined in a complementary way, such as creating reporting facilities which cooperate with law enforcement, awareness-raising and empowerment of children as users of these technologies, self-regulatory elements or the setting up of structures for cooperation between different stakeholders. For this reason the "**lessons learned**" (section 1.3), the **recommendations** and conclusions of the **evaluations** and the Eurobarometer findings opt for the horizontal approach, address a variety of divers issues and underline the roles of multiple stakeholders, such as to enhance the Hotlines' cooperation with the police, to put efforts in more effective and intensive awareness raising, to involve the media more systematically, to facilitate discussion among national administrations or to promote technological tools like age verification systems.

For this reason the services responsible for this impact assessment has decided to **formulate options** on the basis of the **horizontal approach** as this appears to be the appropriate way to respond to the lessons learned, the recommendations of previous evaluations and the objectives formulated on this basis. Each of the chosen options therefore **deals with all risks** (with the exception of option 4 which is a single case); the options do not imply a pre-selection of risks. The options differ essentially in the intensity with which they tackle the risks identified in section 3.2 (exception: option 4), and in which they respond to the given objectives, to "lessons learned" and in the costs of the proposed measures.

The objective of the Impact Assessment is to identify the option which could offer the best balance between a convincing range of impacts on the protection of children and economic effects including cost-efficiency.

The Commission services have therefore considered the following four options:

- **Option 1**: Make no change - continue activities in this area as set out in the Safer Internet plus programme 2005 – 2008 without any modification
- **Option 2**: Modify - adjust the scope of current activities and add new activities to deal with new risks and to enhance effectiveness
- **Option 3**: Slow down - reduce the scale of activities
- **Option 4**: Stop - cease activities completely

The main instruments which could be considered (except for Option 4) are provision of (co-) funding for projects by the Commission and the enhancement of activities to promote best practices and of divers initiatives (e.g. encouragement of self-regulatory initiatives at European level, organisation of stakeholder meetings, studies), which may be (co-) funded or not.

Legislative action is not considered under any of the options as a variety of legislative instruments already exist (see chapter 1.2 and Annex 1) covering well the field of online child protection.

5.2. Analysis of the impact of the policy options

The basis for the assessment of the chosen policy options is the risk analysis: there are a significant number of dangers to which children using online technologies can be confronted. Regarding the 4 chosen policy actions, the questions to be analysed in each case will be: how effective would the option be in protecting children using online technologies (positive impact)? To which extend can the objectives set be reached? Are there possible negative impacts, such as additional administration costs or negative economic impact?

Regarding the assessment of options, the most important impacts fall into the category of social impacts – i.e. on-line safety and security of children, awareness raising, fight against illegal content. The assessment is based on available evidence, such as experience from the previous programmes, independent evaluations of the previous programmes, input from the public consultation, Eurobarometer and other studies, etc. Most impacts are inherently difficult to quantify, also due to the lack of availability of comparable data and figures (as pointed out in the problem definition section). However, despite this problem, the main impacts can still be determined and options compared in a qualitative manner.

The key criteria of analysis considered are impact on reducing illegal content and harmful content online, impact on public awareness, impact on third countries and impact on new on-line risks and challenges. Cost-effectiveness of measures and economic impacts are also considered.

It should be noted that none of the proposed options affects the **rights of privacy and freedom of expression**. It is common to all options (with the exception of option 4, which is a special case) that the network reporting points assess each reported case against the national legal situation. If the content reported is illegal (ex.: child sexual abuse) it is forwarded to the competent law enforcement authority which decides on the next steps. If the content is harmful but in conflict with the national law regulating childrens' access to it they take the appropriate action following the national provisions. The same applies for awareness activities on harmful content/conduct which aim at user-empowerment, i.e. empowerment for making better choices and for taking appropriate actions for protecting themselves. Filters are meant for parents to install on private PCs. They can filter "too" much thus reducing the possible choice; this is the reason why the envisaged programme puts an eye on this – to avoid this disturbing side-effect. Self-regulation is aiming at children not at adults and moves within the limits of youth protection regulations (e.g. mobile phones which block certain functions for children). Filter tools allow adults to de-activate them when desired, thus the adults remain in full control of their filtering effect.

5.3. General policy option 1: Make no change

Continue activities in this area as set out in the Safer Internet plus programme 2005 – 2008 without any modification

This option is the **baseline scenario** against which the impacts of the other options will be compared. It implies to propose an extension of the existing Safer Internet plus Programme with unchanged scope and actions. It would aim at ensuring continuity of the aquis achieved. The 4 actions / strands of the Safer Internet plus Programme would continue. These actions are characterized as follows:

Action 1 (Fighting against illegal content) builds on a system of Hotlines which allow citizens to report illegal content. The Hotlines pass the reports on to the appropriate body (Internet Service Providers (ISP), police, correspondent Hotline) for action. In order for the Hotlines to develop their full potential, Europe-wide coverage and cooperation, increased effectiveness through exchange of information, best practice and experience, is ensured. The Hotline

network structure contributes to this. Links between this network and Hotlines in third countries (particularly in other European countries where illegal content is hosted and produced) shall be promoted, enabling common approaches to be developed and know-how and best practice to be transferred. Hotlines should be linked to Member State initiatives and be supported at national level.

Action 2 (Tackling unwanted and harmful content) focuses on technological tools and self-regulatory actions. The effectiveness of available filtering technology shall be better investigated and better information on the performance of filtering software and services which allow users to make an informed choice be promoted. Rating systems and quality labels can help to enable users to select the content. Funding can be given to projects which aim to adapt rating systems and quality labels to take account of the convergence of telecommunications, audio-visual media and information technology. When developing new technologies, the safety of the end-user should be better taken into account; an exchange of views between child welfare specialists and technical experts shall be fostered.

Action 3 (Promoting a Safer environment) focuses on the enhancement of new activities for making the Internet a safer place, especially by stimulating systems of self-regulation considered as an essential element in limiting the flow of unwanted content. The Safer Internet Forum has an essential role in this respect being a meeting place for actors from all areas, including government agencies and programmes, law enforcement authorities, standards bodies, industry, user organisations (e.g. parent and teacher organisations, child protection groups, consumer protection bodies and civil and digital rights organisations). It specifically provides a platform for national co-regulatory or self-regulatory bodies to exchange experience and an opportunity to discuss ways in which industry can contribute to the fight against illegal content.

Action 4 (Awareness-raising) shall address a range of categories of illegal, unwanted and harmful content (including, for example, content considered unsuitable for children and racist and xenophobic content) as well as new forms of interactive information and communication brought about by the Internet and mobile telephony (peer-to-peer services, broadband video, instant messaging, chatrooms, etc.). Awareness raising activities will be run by a network of awareness-raising nodes in each Member State and candidate country. European added value is provided by a coordinating node, which ensures effective communication, information flow and exchange of best practice between the nodes. It will offer technical assistance and training, build an infrastructure for a single transnational repository (web portal) of relevant information and expand links with awareness-raising activities outside Europe.

By assembling the different network functions (Hotline, awareness nodes, helplines) under single roofs, synergies will be better exploited.

5.3.1. Social impacts

The recent evaluation reports on the preceding programmes (see Annex 2) have recognized the positive impacts of the preceding programmes on the society.

Through providing funding for Hotlines (Action 1)[62], the Commission "has made a significant contribution to combating illegal content"[63]; the number of reports sent to the police by national hotlines has been increasing steadily. [64] The social impact of ongoing Hotline

---

62 Annex 1 to the Safer Internet Plus programmedecision list up 4 actions.

63 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 23.

64 Source: INHOPE website: http://www.inhope.org/fr/news/press_release.php?id=20060426. The INHOPE Association is a network organisation for Internet Hotline providers. Its mission is to

network operation would therefore be high; further web sites offering illegal content would be closed down. By reinforcing the measures envisaged under the Commission's Cybercrime Communication in the area of Internet-based child abuse, it would help to stimulate cooperation between law enforcers and prosecutors across the EU and to use resources more efficiently.

The surveying of technological tools (Action 2), a continued focus on improving their effectiveness and of promoting them in public are expected to have a positive impact on the uptake and efficiency of parental control tools and would thus help to reduce children's access to content harmful to them.

Following the evaluation reports, self-regulatory initiatives (Action 3) instigated by the Commission have been successful.[65] The framework agreement concluded with leading European mobile operators (see section 1) would continue to be monitored under Option 1[66] and other industry sectors would be encouraged to negotiate similar agreements. This would have a positive impact in limiting children's access to harmful content.

The evaluation reports underline the key importance of awareness-raising (Action 4) and highlight the role of the Commission in launching initiatives across Europe. The recent Eurobarometer figures (see section 1) underline the impact already generated by the preceding programmes and it is likely that keeping the activities at the same levels would continue to raise the awareness of parents, teachers, children and other relevant stakeholders.

A secondary effect of Option 1 could possibly be a slow tendency to further adapt national laws towards common standards and definitions.

Also in the public consultation it was made clear that the stakeholders believe that "efforts so far in the fight against illegal content had been positive and successful", at the same time fearing "that these good results would be jeopardized if the fight against illegal content were to cease after 2008. There was almost universal agreement that the fight against harmful, as distinct from illegal, content also needs to continue"[67].

Option 1 is therefore expected to generate *considerable social impacts*. However, online technologies and their use are in continuous progress: cyber-bullying, grooming, new ways of disseminating sexual abuse material, evolving communication features in the co-called "Web 2.0" are expressions of a cyber world undergoing rapid changes. Option 1 does not provide sufficient means to deal with them.

Furthermore, in order to meet these new challenges the policies need to be continuously up-to-dated and increased. Some policies might also be pre-emptive (for example: chat rooms and social networking sites are increasingly used for grooming and for opening distribution channels for child abuse images). In order to develop effective and timely counter-strategies, investigation on behavioural and psychological aspects would be necessary and activities reinforced in order to deal with the increasing risks to children online. Currently there is a noticeable lack of European comparative facts and figures, of robust statistics; ongoing investigations on Member State level are not coordinated within the EU and lack of comparability. Option 1 does neither provide the basis for this.

---

eliminate child abuse material from the Internet and protect young people from harmful and illegal uses of the Internet.

65 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 26.

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

67 Summary of the results of the online public consultation and 20-21 June Safer Internet Forum (Report), not yet published.

Maintaining the pressure on illegal content could make certain activities, specifically the production and dissemination child abuse images, move outside of the EU. Such an effect would call for tighter international cooperation between the EU and third countries, which is not granted under Option 1.

There is a general tendency towards an increasing online-related child abuse and also towards more domestic production of child abuse images in the EU. The fight against the online dissemination of child sexual abuse images may stop some commercial child abuse activities but - *negatively* - may bolster the trend to more domestic production of such images. Such abuse causes even more harm to children as it involves normally family members as predators. These general tendencies can only be reversed by putting more efforts into multi-faceted counter-strategies addressing any form of such child abuse: the pressure on any predator and consumer must not only be maintained but needs to be increased. Option 1 does not go beyond the current counter-strategies.

Regarding possible impacts on the rights of privacy and freedom of expression it is referred to section 5.2.

5.3.2. Economic impacts

Option 1 will help to create a climate of confidence which will promote the use of online technologies and so enhance the economic benefits that greater access to these technologies will bring to society.

The economic benefits of the programme have been demonstrated by the support given by industry to the activities of the preceding programmes. For instance, mobile industry and Internet Service Providers can have an interest to reduce the chances of "collateral damage" to minors where they are able to access content not intended for them with the resulting bad publicity. They therefore have a clear interest in co-operating to develop measures which empower parents to protect minors against harmful content. It is nevertheless difficult to give any figures on "return on investment" since the areas chosen tend to be those which do not have a direct economic return.

On the cost-avoiding side it must be taken into account that the preventive protection of children helps to avoid costs in the health security and social / youth support systems which are caused by the treatment of psychological trauma etc.

Few negative economic impacts can be foreseen, with the possible exception of negative economic impacts for 3rd countries, as Option 1 would maintain the pressure on criminal activities related to child abuse so that some activities may move there as a result. Such effects have already been noted as in a number of Member States the amount of child abuse images on servers has been reduced considerably. Consequently, it appears that such content has moved to servers in 3rd countries. This is certainly primarily the effect of a number of successful and far-reaching law enforcement cases in the recent years. But, it can be assumed that also the preceding Safer Internet programmes have contributed to this effect to some extent, even if this impact is neither measurable nor has been investigated so far. The only way to mitigate these effects is to intensify international cooperation with third countries. Option 1 includes international cooperation, but these activities would need to be further developed.

5.3.3. Costs for public administration

The current annual average budget available under Safer Internet *plus* is of 11.25 million Euros. Option 1 would lead to a slightly reduced annual impact on the Community budget (10.25 million Euros).

The reason for this is that the effectiveness of the administration / management of the envisaged programme within the Commission would be enhanced by making the current structure (the model of the Safer Internet *plus* programme) of the European networks (providing hotline services, awareness nodes and helpline facilities) more effective. Network relays which currently combine different services and functionalities would gather these under one roof in the Member States. This would also reduce the administrative burden for the Commission service. In comparison to the current situation the staff could be reduced by 2 persons (total: 10 persons). The total administration costs within the Commission for 5 years duration are estimated at 6,964,000 €.

The option does not impose administrative burdens on private sector or national public bodies. .Direct costs for the public administration in the Member States are not associated with this option. Indirect costs may appear if the Member States governments decided to co-fund activities such as the running of awareness nodes and Hotlines. This is, however, not an obligation under any of the options discussed here.

5.3.4. Degree of coherence with policy objectives

Option 1 would meet the majority of objectives outlined above. It would fail inasmuch as new pro-active and preventive strategies depend on a reliable knowledge base and increased efforts, for instance in the fight against new dissemination channels for online illegal content. The same applies for more effective awareness-raising methods (designed with input from the knowledge base), most recent relevant information for the public (as much as new trends and behaviours need to be understood better, as for example the grooming process), the better understanding of perpetrator conduct and the impact and risks of existing and emerging technologies.

5.3.5. Added value and respect of the subsidiarity principle

Option 1 complies with the principle of subsidiarity; this comprises different aspects:

– In some Member States, the programme links in with national programmes comparable to Option 1 in terms of scope and remit. In a number of cases, these have been clearly inspired by the Safer Internet Action Plan 1999 - 2004.

– In other Member States, there is still a need for more developed and structured forms of co-operation. The issues cuts across traditional boundaries between ministries - Justice, Home Affairs, Industry, Culture, Education, Family and Social Affairs -depending on how ministerial portfolios are distributed. In decentralized states, the competences are likely to be split between national and regional levels.

– In further Member States there is still the need to enhance the development of more systematic and effective policies in this area.

– Option 1 will certainly give the necessary additional impetus to setting up new forms of co-operation (e.g. co-operation between law-enforcement and industry).

Coordination of cross-border cooperation adds a clear European value, specifically by spreading knowledge of best practices and by making sure that resources are well used. Taking into account the strong cross-border character of the Internet this applies for example for the effective running of the Hotlines, Helplines and Awareness networks or the promotion of the best performing technologies.

A more detailed analysis of the added value and the way the subsidiarity principle has been respected is presented in section 8.1. In order to avoid repetitions it is referred to this section.

5.3.6. Feasibility

The preceding programmes, which are the basis for Option 1, have proved to be feasible. The SIAP, which is being continued by the Safer Internet *plus* Programme, was conceived by all stakeholders as a relevant and effective programme which should continue. The European Union is seen as a pioneer within this field (see section 1) and the launching of hotlines and the development of awareness nodes in Member States is seen as major achievement[68].

5.3.7. Conclusion

Option 1 is viable and will, based on past experience, generate a considerable number of impacts, especially of a social nature as it would be an important ongoing instrument to reduce the risks for children online. The costs are nearly identical to those in the preceding programme and also the impact is expected to be of the same dimension.

However, it would also imply shortcomings when dealing with changing and emerging uses and behaviours leading to new risk situations and which would require specific and more intensive efforts to be taken and additional counter-strategies to be developed.

5.4. General policy option 2: Modify

Adjust the scope of current activities and add new activities to deal with new risks and to enhance effectiveness

This option would mean to further develop a coherent strategy for the fight against harmful effects of online technologies at EU-level. It would consist of two basic elements: to continue with the activities developed and implemented under the preceding programmes (the baseline scenario) and to gather momentum and to enhance a set of new actions which are envisaged to meet new challenges.

Existing activities which have proved to be successful would be strengthened and reinforced (gathering momentum) aiming at further improving their effectiveness and their impact. Such actions would namely be:

- Reducing illegal content by enhancing efficiency and effectiveness of the existing networks (the contact points for reporting illegal content); enlarging their coverage (EU-27); this is Action 1 of the **baseline scenario**
- Initiating the creation of new self-regulatory systems, as for example for ISPs, in view of a safer online environment (Action 2 of the **baseline scenario)**
- Enhancing the development and uptake of technical tools (Action 2 of the **baseline scenario)**
- The Safer Internet Forum (Action 3 of the **baseline scenario)** with a view to stimulating new activities of and between stakeholders
- Awareness-raising, improving awareness-raising methods and tools by identifying, enhancing and disseminating effective and cost-efficient awareness-raising methods (Action 4 of the **baseline scenario)**
- Enhancing global international cooperation, particularly by making existing international instruments more efficient and by stimulating the development and implementation of actions in the relevant fields (all actions of the **baseline scenario)**.

---

[68] Communication COM(2006) 663 on the final evaluation of the Safer Internet programme for the period 2003-2004.

The tackling of new phenomena which are due to developing technologies and societal developments would require introducing new features under this option. Option 2 will give specific and more intensive attention to these areas, such as it has been expressed in the evaluation recommendations (see section 1.3 "Lessons learnt"), specifically in the recommendation "to develop actions taking account of changing risk situations (e.g. chat-rooms, Instant Messaging Services, peer-to-peer technologies)".

Such new features / actions which go **beyond the baseline scenario** would namely be:

- Tackling harmful *conduct* online, especially grooming, cyber-bullying
- Stimulating the involvement of children and young people in creating a safer online environment
- Establishing a knowledge base which would allow a better understanding on how actually children use online technologies and how risk situations develop - continuously updated in order to keep pace with fast changing technologies and services. It would open European-wide access to aggregated data and include a EU-level coordination of investigation activities. This could cover general areas for investigation (for example the way risks evolve into actual harm to children; the precise nature of harmful consequences or the identification of the types of websites which attract both children and potential abusers); Child-specific studies (for example the identification of the most vulnerable groups of children targeted for online abuse, the psycho-social impact on children; behavioural differences in use between age groups; the relationship between young people's sexuality and online grooming; the profiling of risk-taking online behaviour by different groups of children; the children's use of technology such as web cameras and cell phones); and Offender-related investigation (e.g. the ways in which sexual abuse is caused with the help of online technologies; understanding how offenders use online technologies to find and target children; the changing nature of grooming behaviour; the link between consumption of child abuse material and contact sexual abuse; the changing profiles of online child abusers)
- European comparative facts and figures, i..e. to establish more robust statistics (nationally and Europe-wide) concerning for example online sexual abuse and grooming[69]
- Developing strategies to protect children better in evolving environments such as social networking sites and chatrooms.

The option would, apart from the general objective of achieving an optimization of existing and additional means, furthermore envisage taking early-stage, pre-emptive actions against new developments which generate harmful effects of online technologies to children. Further information on the structure of the programme envisaged under Option 2 is given under Annex 2.

5.4.1. Social impacts

Those effects which have been described for Option 1 under the corresponding chapter *fully apply.* The social impacts of Option 2 would however go further than those.

By establishing a knowledge base the impact of **digital convergence** on the ways online technologies are used, on the changes in behaviour and on the development of interlinked risk

[69] Summary Report on the results of the public consultation, Chapter 1.

situations would be better understood and allow to develop adequate counter-strategies. The knowledge base would also help to design pre-emptive measures.

Cyber-bullying needs more efficient prevention strategies, namely in the context of awareness-raising activities. Option 2 provides this.

Social networking sites confront children and young people to serious risk situations (such as bullying, inappropriate content, disclosure of personal information, grooming, glorifying harmful activities etc.; see section 4). Up to now too little has been done to deal with these risks. Access could for example be blocked for children, wherever adequate, by using (improved) age verification systems, accessible sites could be monitored and vetted permanently, specific sites for children could be promoted more emphatically. Option 2 would provide the means for this.

The increased use of webcams has led to children being intimidated or manipulated into recording images of themselves with a sexual background or them being engaged in cyber-flirting, **cyber-sex** or real-life meetings. Counter-strategies still need to be developed - as under Option 2.

The Internet has become one of the main distribution channels of material depicting **sexual abuse of children** with **new dissemination channels** being established (e.g. through the web 2.0); however, there is little knowledge and no reliable figures on the size of these phenomena. Option 2 would investigate this. The mechanisms in place (especially the reporting facilities for citizens) seem to have effect in the Member States as far as web site offers are concerned, but they do not seem to be effective enough to deal with all challenges arising from evolving communication technologies, from evolving dissemination channels and from the international reach of the Internet. Option 2 would provide the knowledge base on these evolving technological and behavioural patterns and will allow developing targeted counter-strategies.

Grooming has become a menacing feature of online activities. Due to the noticeable lack of statistics and hard data on the numbers of children ensnared by potential abusers through grooming, the size of the problem is not even well understood and there is a noticeable lack of awareness in Member State authorities and the public about this form of harmful conduct which has severe consequences on children. Option 2 would give specific attention to understanding the grooming processes better, to build public awareness on all levels and to protect children better against grooming attacks.

The challenge of reducing the risks for children is not static but dynamic. The response to this must therefore be dynamic, too. Action of a multi-faceted is required; the issues explained above would be specific to Option 2 and go beyond Option 1. The ***positive social impacts*** which are expected for Option 2 would comprise those described for Option 1 but at the same time go beyond them:

- With an increased focus on counteracting the production and online distribution of illegal content, the number of sites and the amount of illegal material available to the public will decrease. The mechanisms for reporting illegal content will become available to all European Internet users, and enhanced cooperation on European and international level between relevant stakeholders will stimulate a higher degree of awareness in relevant stakeholders;

- Through a strengthening of the coordinated awareness activities, a large number of stakeholders and citizens will become more aware in efficient and appropriate ways of the risks for children online and of the ways of dealing with those risks;

- The development of technological solutions will be promoted, which support parents and educators in performing informed choices about the possibilities that are offered to their children;
- Industry self-regulatory initiatives and co-ordination will help to protect children better;
- Law enforcement will continue to benefit from the activities;
- A deeper and wider knowledge will be available through increased focus on investigation activities.

Negative impacts

Increasing the pressure on illegal content with the aim of making the Internet safer in Europe could have the effect that certain activities move more and more outside of the EU. This applies specifically to child abuse images. Such content can be produced in one country, hosted in a second and downloaded from a third. Increasing efficiency of law enforcement in the EU could lead to production and hosting moving to 3rd countries (see "Economic impacts", section 5.4.2). The way to mitigate these effects is to intensify international cooperation between the EU and third countries so as to increase its effectiveness. Option 2 would give specific attention to this.

A further possible negative impact of all the actions under this option could be over-reliance by Member States on action funded by the Community, rather than taking their share of the responsibility. Implementation of these actions under Option 2 would therefore pay particular attention to the requirement that all co-funded projects have a strong "European added value" and that there should be support for project activities from public authorities (particularly in the fields of law enforcement, education and media regulation).

By deploying a wider variety of counter-strategies Option 2 would contribute to tackling not only commercial production but also new dissemination channels. This could lead to an overall decrease of the production within the EU. But, a more successful fight against the production and online dissemination of commercial child sexual abuse images may bolster the current shift towards more domestic production of such images (see Option 1, section 5.3.1). The way to stop the rather negative world-wide trend regarding child abuse is to put more efforts into multi-faceted counter-strategies which not only maintain but increase the pressure on any predator and consumer. This is what Option 2 intends to do.

Regarding possible impacts on the rights of privacy and freedom of expression it is referred to section 5.2.

5.4.2. Economic impacts

Option 2 is expected to generate similar effects as Option 1 but at higher levels: it will help to create a climate of confidence for the use of Internet enhancing the economic benefits of evolving communication technologies. The exact economic impact of the programme in this respect is, however, not easy to define as it will be quite indirect.

For the industry the aspects of avoiding “collateral damage” to minors where they are able to access content not intended for them and of being associated in the public with illegal content such as child abuse images can result in bad publicity causing negative economic consequences.

Even if it is difficult to predict the exact economic impact in such an area it can be stated that the preventive effect of the envisaged programme (e.g. by self-empowering children or by

blocking access to inappropriate content) would have a considerable potential of avoiding costs on the side of medical and socio-psychological institutions as psychological trauma and physical harm to children will to a certain extent be avoided.

A further, also quite indirect economic impact which is not easy to quantify, will be an increased efficiency of EU cross-border law enforcement processes, especially in the field of child sexual abuse, which will be enhanced by a variety of (novel) activities reinforcing those under the Cyber Crime Communication.

Few negative economic impacts can be foreseen, with the possible exception of negative economic impacts for 3rd countries, as Option 2 would increase the pressure on criminal activities related to child abuse in the EU (e.g. via the blocking of dissemination channels) and it may lead to more activities moving to 3rd countries as a result (thus reinforcing a current trend, see Option 1 / section 5.3.2). This may cause negative economic consequences in these countries linked to illegal activities and prepare the grounds for organized crime. The effect, which in absence of analytical data cannot be verified, would presumably, if it happened, be of the same size as under the baseline scenario (Option 1). Option 2 would mitigate this effect better than the baseline scenario by striving for more intensive international co-operation.

5.4.3. Costs for public administration

Option 2 would lead to a Community budget spending in the area of child safety and communication technologies which is nearly identical to the current Safer Internet *plus* programme. The annual average budget available under Safer Internet *plus* is of 11.25 million Euros; Option 2 would lead to an annual budgetary impact of 11 million Euros.

New activities do not necessarily need (significant) additional funding. The enhancement of codes of conducts for example requires hardly any financial resources (demonstrated by the Framework Agreement between the Commission and Mobile Phone Operators); some network partners already involve children, but there is no systematic EU-wide approach or strategy behind it; harmful conduct can be dealt with by refocusing activities in the contact points.

Also under Option 2 attention would be given to improving the effectiveness of the administration / management of the envisaged programme. The current structure of the European networks (see baseline scenario / Option 1) would be further developed by creating network relays which combine different services and functionalities under one roof. This would reduce the administrative burden for the Commission and free manpower capacities for the new challenges. The estimated administration costs within the Commission are calculated at 8,147,000 € (for the 5 year period). The number of staff required would be 12.

Reinforcing the administrative efficiency of the networks would lead to savings on the programme budget side; this will allow subsidizing novel actions.

The option does not impose administrative or financial burdens on private sector or national public bodies. Direct costs for the public administration of the Member States are not associated with this option. Indirect costs may appear if the Member States governments decided to co-fund activities; however, this is also not an obligation under this option.

5.4.4. Degree of coherence with policy objectives

Option 2 would meet the objectives outlined to a large extent. Its design would be in line with the recommendations gathered in the public consultation. It would safeguard the current

achievements and allow new pro-active and preventive strategies designed with input from the knowledge base.

5.4.5. Added value and respect of the subsidiarity principle

Option 2 complies with the principle of subsidiarity as much as Option 1 (baseline scenario). The arguments unfolded under the corresponding chapter apply fully. A detailed analysis of the added value and the way the subsidiarity principle would be respected is presented in section 8.1. In order to avoid repetitions it is referred to this section.

5.4.6. Feasibility

The preceding programmes, which are the basis for Option 2, have proved to be feasible. This has been highlighted by previous evaluations (see Option 1; section 5.3.6). Any new actions to be designed in the future will be rooted in and supported by the existing structure and will benefit from an ongoing learning process and from increasing experience in the field.

5.4.7. Conclusion

In order to efficiently combat the harmful effects of online technologies it is necessary to adapt the actions and means of the Commission to the changing landscape.

5.5. General policy option 3: Slow down

Reduce the scale of activities.

Although reducing the scale of current activities a core set of activities would still be safeguarded, taking into account that they have, following the evaluation reports of the previous programmes, proved to be successful. New initiatives would not be taken.

The safeguarded activities are mainly those which have gained an international outreach beyond the European Union and which, at least in a number of Member States, would not be able to carry on without the EU's financial support[70]. More specifically and compared to the **baseline scenario (**Option 1) it implies:

- to continue with Action 1 (Fighting against illegal content) of the baseline scanerio, supporting a system of Hotlines which allow citizens to report illegal content and which is coordinated and enhanced by a network organisation;
- to carry on the Safer Internet Forum under Action 3 (Promoting a Safer environment);
- and to continue with Action 4 (Awareness-raising) addressing a range of categories of illegal, unwanted and harmful content. Awareness raising activities would be run by the network of awareness-raising nodes supported by a network coordinating body.

The difference between Option 3 and Option 1 is therefore that Option 1 would continue with the same budget and basically the same structure of the programme as in the previous years, while Option 3 heads for reducing the scale of activities, cutting the budget by 40%, focusing only on core activities (Hotlines, awareness nodes, Safer Internet Day) and dropping other activities.

[70] Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p.41: 34 % of the projects would be endangered for "uncertain" future funding. This is mainly due to the fact that the majority of organisations involved are NGOs not oriented towards commercial benefits.

5.5.1. Social impacts

The objective of Option 3 is to keep the existing core infrastructure running. In practise Option 3 will imply the continued running of mechanisms for the public to report illegal content and the coordination of awareness activities.

It has already been explained under Option 1 that the recent evaluation reports on the preceding programmes have come to the conclusion that the Commission's activities have generated positive impacts on the society, because they notably contribute to making the Internet and mobile communication a safer place for children. Furthermore, the major awareness event, the Safer Internet Day, has gained significant visibility over the years; in 2007 the number of participating countries rose to 45 and the press and media coverage reached a very important level.

The most recent evaluation report points out that the "consistency of… actions" is "crucial as, each year, a new group of children begins to use the Internet and other technologies for the first time. As a result, the need to renew and refresh safety and awareness messages in this area will clearly be an ongoing responsibility for society"[71]. At the same time the evaluation reveals that one third of the Commission's contractors would not be able to go on without Community funding. This illustrates the effects which Option 3 would generate: to ensure that the momentum gathered persists and that the visible impacts of the past will continue to happen:

- The Commission would continue making "a significant contribution to combating illegal content";[72]
- The positive impact of the past awareness-raising activities (increase of awareness levels in all Member States; see section 1) would be ongoing[73];
- The annual Safer Internet Day would continue playing a key role in this context.

On the other hand, Option 3 would also generate *negative impacts*. It can only be regarded to be a **minimum solution** as it would not seize all opportunities to protect children which the Commission has at hand. Child safety online is a complex issue as it encompasses a large variety of multi-faceted stakeholders and responsibilities. An effective answer to this challenge cannot be but a complex one. It also has to encompass hands-on actions such as considering technological solutions (filtering, age verifications systems, forensic), self-regulation, and better cooperation mechanisms between relevant stakeholders (e.g. law enforcement bodies on cross-border level). The changing online environment leads to new risks for children who will need to be better understood; hence investigations are needed to complete the knowledge base and consequently new actions might be needed. If such new strategies were not developed the door would be left open to new dissemination channels of illegal and harmful content, growing organized criminality, namely regarding online-related child abuse, open spaces for harmful forms of conduct etc.

In the public consultation and overwhelming number of stakeholders have called for a large number of *new* actions on top of those which have proved to be effective, hardly any voice has voted for reducing current efforts.

---

71 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006, p. 22.

72 Ibid. p. 23.

73 All evaluation reports and the recommendations in the public consultation underline the key importance of awareness-raising.

Regarding possible impacts on the rights of privacy and freedom of expression it is referred to section 5.2.

5.5.2. Economic impacts

Option 3 would, to a certain extent, help to create a climate of confidence in the use of Internet and new online technologies and so enhance the economic benefits that greater access to these technologies will bring to society. The effect would, however, be more limited than under Option 1 and 2 as the measures envisaged under this option are more restricted.

On the cost-avoiding side, the preventive protection of children could help to avoid costs in the health security and social / youth support systems which are caused by the treatment of psychological trauma etc.; however, this effect would again be more limited.

Under Option 3 criminal activities related to child abuse which show a tendency to move to 3rd countries may - to a very limited extent - feel "enhanced" to do so. Some negative economic impact could therefore be generated there. On the other side it is expected that Option 3 would rather reduce the pressure on these activities than maintaining it in the same way as Safer Internet *plus* has done it. This might even lead to a coming back of some of the illegal activities to the EU.

5.5.3. Costs for public administration

In comparison to the preceding Safer Internet *plus* programme a reduction of the budgetary impact would be expected due to the fact that only core activities under the established previous programmes would be maintained. The reduction of the budget, compared to Safer Internet *plus,* would be of 40%, i.e. an annual decrease of 4.5 million Euros[74]. Due to the reduction of activities also the administrative costs in the Commission would decrease; they are estimated at 5,774,000 € (for a period of 5 years).

The option does not impose administrative burdens on private sector or national public bodies. No direct costs for the public administration of the Member States are associated with this Option. Indirect costs may appear if the Member States government decided to co-fund the envisaged activities. Co-funding is, however, not an obligation under Option 3.

5.5.4. Degree of coherence with policy objectives

Option 3 would only meet a limited number of objectives. These are mainly to maintain the reporting facilities throughout the EU and beyond, to make the public aware of Internet risks and to provide the public, especially children and their carers, with updated information about online child safety. To a lesser extent it would promote cooperation between relevant stakeholders within Europe and on international level and to an even lesser extent it is expected to have an impact on the level of political agendas in the Member States as Option 3 will concentrate on operational activities only. It would not contribute to any investigation activity (knowledge base), and would not be designed to deal with possible technical solutions in safety issues, with risks resulting from emerging technologies or with industries safety product development.

Option 3 would also not allow for developing up-to-date counter-strategies against the changing behaviours and ways technologies are used as this will require work to update the knowledge base and more intensive exchange of information.

---

[74] The current annual average budget available under Safer Internet *plus* is of 11.25 million Euros.

5.5.5. Added value and respect of the subsidiarity principle

Option 3 complies with the principle of subsidiarity as it focuses on operational level activities. These actions would *complement* activities in the Member States (see Option 1; section 5.3.5). In those Member States where more systematic and effective policies in this area need to be developed, Option 3 would only offer limited incentives. A more detailed analysis of the added value and the way the subsidiarity principle has been respected is presented in section 8.1. In order to avoid repetitions it is referred to this section.

In all cases the enhancement of cross-border cooperation would add a clear European value; Option 3 would allow a (continued) joint learning process by spreading knowledge of best practices and exchanging experiences, although to a limited degree. It will also stimulate cost-effectiveness by enhancing the use of materials, methods and practises which have been successfully developed in one Member State and which can be replicated in others.

Option 3 would imply to limit to core activities and to abandon a number of actions. This would theoretically give Member States opportunity to finance and develop their own activities (while it has to be borne in mind that Member States also have the opportunity in all other options). However, there is a real risk that Member States would not provide sufficient financing, and part of the European added value would be lost (see for details in section 8.1; findings of previous evaluations) and children would as a result of this be less protected in a number of Member States as they currently are.

The lack of Community actions is neither expected to be compensated by self-standing industry (self-regulation) initiatives. Past experience has shown that public intervention is necessary to launch and stimulate such processes (see the European Framework for Safer Mobile Use by Younger Teenagers and Children; section 1); market forces alone are not expected to lead to sufficiently coherent initiatives (for more details see under Option 4).

5.5.6. Feasibility

The envisaged activities under this option stand for a continuation of the core activities of the preceding programmes, which have already been set up and which are operational. These activities have been confirmed to be feasible in the evaluation reports.

5.5.7. Conclusion

Option 3 is a viable solution: it would be feasible and generate impacts on operational level with high probability such as it has been proven in the past. It would help to reduce the risks for children online by allowing for mechanisms where the public can report illegal online content, and for increasing public awareness concerning online risks and how to deal with them.

However, Option 3 is at the same time a minimal solution only. It aims at safeguarding core infrastructures of the preceding programmes which have been gaining visibility in the perception of the European public[75] and internationally. It would neither lead to any further actions nor cope with new challenges. Positively, it could be expected in the long run that access to illegal content will be more restricted in the Member States as there is a tendency to control this issue better - which is to a certain extent an impact of the Commission's policy - but negatively it can be anticipated that the distribution of illegal content increasingly will take place through peer-to-peer communication, 3G mobile phones etc. This will certainly require further and new counterstrategies, which Option 3 cannot deliver.

---

[75] As said above the Eurobarometer 2006 states that average awareness level of the EU15 countries have risen from 41% in 2003 to 54% in 2005.

5.6. General policy option 4: Stop

Cease activities completely.

To cease funding activities in the area of safer use of online technologies would mean that no general horizontal action is taken in this field by the Commission any more and no pro-active policy in this area is carried out on EU level. This would nevertheless imply that:

- The Commission would be able to continuously assess the need for possible targeted legislation or policy action and take appropriate action when needed possibly at later stage.

- The Commission would follow existing international projects and activities against harmful effects of communication technologies, but neither support them nor pro-actively initiate such projects.

This option would imply to stop funding activities in the area of safer use of online technologies.

5.6.1. Social impacts

The main direct consequences of a "no new action" scenario regarding harmful effects of online technologies for children would be that the facilities for citizens to report illegal content ceased functioning in a number of Member States (see also section 9.1).[76] The support to law enforcement and prosecution of the respective forms of cyber crime is expected to weaken as the fight against these forms of cyber crime and especially prevention efforts would be in danger to be more fragmented.

The same would apply for the network of awareness nodes; activities would in a number of Member States either cease or continue on a lower level.[77]

For those actions possibly continuing their operation without the financial support of the Commission, the benefits of networking would fall apart. The cross-border network coordination has been systematically developed over the past years in the preceding programmes and it stands for a richness of expertise and best practice which, spread over the whole of the reporting points and awareness nodes, allows a continuous process of learning and improvement in effectiveness and societal impacts.

The lack of Community actions is not expected to be compensated by self-standing industry self-regulation initiatives. Past experience has shown that public intervention is necessary to enhance the industry's sense of responsibility and that the Commission has an important co-ordinating and catalytic role[78]; market forces alone are not expected to lead to appropriate initiatives. Even if self-regulation is certainly part of the solution it would definitely not allow tackling all the risks and challenges to be addressed: due to their cross-cutting nature many actions are not limited to the competences of industries, but address to other appropriate organisations and their specific functions (e.g. child care organisations, schools).

The lack of a future European-wide initiative to interlink public and/or private efforts to fight harmful effects of online technologies for children is therefore expected to generate *further negative effects*.

---

[76] The latest evaluation report confirms that one third of Hotlines and Awareness nodes are not able to continue operation as they lack alternative funding sources.

[77] Ibid.

[78] See the European Framework for Safer Mobile Use by Younger Teenagers and Children; Section 1.

In view of the limited range of possible impacts of self-regulation systems a further option in the impact assessment which would limit the Commission to initiating such initiatives only was not considered. However, self-regulation initiatives have been defined as one of the operational objectives.

5.6.2. Economic impacts

Option 4 would not produce any direct economic impacts. However, there are follow-up problems in the societies which will have a clear indirect negative economic impact on the health and youth protection systems in the long run: children suffering for example from physical and psychological damages or copying negative forms of conduct such as "Happy Slapping" or "bullying" will demand for more supporting treatments. Such economic impact is hard to quantify.

The lack of any horizontal initiative in the field of online child protection can furthermore produce a risk of a growing feeling of uneasiness for the EU citizens using online technologies. This can in the long run negatively affect the development of the Information Society industry. It should be remembered that Option 4 would leave place for political inactivity in this field which is still notable in some Member States.

Criminal activities related to child abuse are not expected to significantly move less to 3rd countries under this option, but the movement could slow down; it will rather happen that the problem also within the EU increases due to reduced pressure on the criminal actors. This could also lead to better conditions for the evolvement of organised crime within the EU.

5.6.3. Costs for public administration

The option would lead, in comparison to the current annual average budget available under the Safer Internet *plus* (11.25 million Euros) to an equal reduction of the Community budget spending. This applies also for the administration costs within the Commission as the staff working under Safer Internet *plus* would be unburdened.

No costs would occur for public administrations in the Member States under this option.

5.6.4. Degree of coherence with policy objectives

The option to cease activities completely is not in coherence with the policy objectives. Option 4 would not meet any of the objectives.

The only argument which would justify abandoning all activity in this area is that the Commission's intervention is not needed as the objectives would be reached at an adequate level on Member State level only. As said above, this is not or not yet the case.

Reducing support to the running and networking of reporting facilities for illegal content furthermore contradicts the Commission policy in the field of cyber-crime. The Commission has pointed out in its Communication "Towards a general policy on the fight against cyber crime" that "law enforcement action against such sites is extremely difficult, as site owners and administrators are often situated in countries other than the target country… The sites can be moved very quickly… and the definition of illegality varies considerably from one state to another."[79] The Communication therefore suggests that "a strengthened operational cooperation between Member States' law enforcement and judicial authorities" is necessary in order to enhance the effectiveness of law enforcement on Member State level due to its cross-

[79] Communication ibid. p. 3.

border nature.[80] The network of reporting facilities, which Option 4 would abandon, enhances the efficiency of cooperation between relevant stakeholders.

5.6.5. Added value and respect of the subsidiarity principle

No action that could add value would be taken.

5.6.6. Feasibility

A "no action" option is obviously feasible from a theoretical point of view. But a decision not to take any horizontal action in this field would risk political criticism as especially the use of the Internet requires an international approach due to its cross-country operational nature.

5.6.7. Conclusion

The option to take no action at all in this field does not seem to be viable; it would not be a sufficient response to existing challenges. A passive approach would be likely to result in negative impact on the dimension of risks children are confronted with when using online technologies. Any draw-back in dealing with these risks will lead to a situation where the door would be left open to harmful and illegal activities. The potential long-term negative impact of a "no action" scenario is therefore considered to be very high.

Many actions developed under the preceding programmes have been gaining visibility in the public; if the were stopped the momentum created would be lost and the efforts of the past years would be jeopardized.

6. COMPARISON OF THE STRATEGIC POLICY OPTIO

6.1. Comparison

The previous chapter assessed economic and social impacts of the four options identified. The aim of this chapter is to compare the four options against a set of criteria, using **Option 1** (no change) as a **baseline**. The tables below indicate only an order of magnitude of the impacts because, as noted above; a precise quantification of impacts cannot be provided as most of them occur in the social sphere. Option 1 forms a basis for the assessment; the remaining three options are compared to Option 1 and net effects are assessed.

The awards in the tables essentially summarize the analysis of options and their impacts carried out in the previous chapters. In order to make the results better comparable scores have been attributed to each criterion under each option. As Option 1 is the baseline it received under each criterion the score "3". The scores for the other options express the differences in expected impacts, being similar, (positively) higher or (negatively) lower. The scale used is characterized as follows:

Score	Description
6	Much higher (i.e. more positive) impact (than under Option 1)
5	Higher (positive) impact
4	Slightly higher (positive) impact

[80] Ibid. p. 10.

3 (baseline)	*Similar impact (as under Option 1)*
2	Slightly lower (i.e. more negative) impact (than under Option 1)
1	Lower (i.e. more negative) impact
0	Much lower (i.e. more negative) impact

In case of the criteria "Cost of medical and psychological treatment", "Cost for public administration", "Impact on third countries" **the scale is inverted** (e.g. *higher* costs than under Option 1 / the baseline lead to a *lower* score as the impact is more negative).

Table 1 focuses on the essential impacts of the programme – i.e. the social impacts. The four criteria chosen correspond at the same time to the general objective and the four specific objectives of the proposal. From that perspective, they also measure the effectiveness with which the four options achieve the key objectives. It should be underlined that the impacts of the proposed strategies may not be visible immediately and direct, rather they will be visible in a long-term perspective.

Table 1 – Social impacts

	Protection of children	***Improve security,*** ***enhance law enforcement***	***Impact on awareness raising and (media) education***	***Meet new challenges and risks***
Option 1 " no change" **(baseline)**	high level of protection	Improved law enforcement and security	Improved public awareness, media education	No particular attention devoted to new risks
Score **(baseline)**	*3*	*3*	*3*	*3*
Option 2 "adjust the scope"	Slightly higher impact than Option 1	Similar to Option 1	Higher impact on more efficient awareness methods and tools & on promoting media education than Option 1	Substantial improvement, much higher impact, compared to Option 1
Score	4	3	5	6
Option 3 "slow down"	Lower impact than Option 1	Slightly lower impact than Option 1	Slightly lower impact on public awareness and media education than Option 1	Similar to Option 1
Score	1	2	2	3
Option 4 "cease"	Much lower impact than Option 1: low	Lower impact, smaller improvement	Much lower impact than Option 1: small to no impact on	Similar to Option 1

	to no level of protection (depending on MS activities)	(improvement stemming from COM Cybercrime actions, furthermore depending on MS activities)	awareness & media education, depending on MS activities	
Score	0	1	0	3

Table 2 summarizes the main economic impacts of the four options. Here again, the assessment is based on comparison with the baseline Option 1. The criterion "deployment and use of ICT" refers to the impact of options on creating safer and secure on-line environment which would encourage the use of ICT having an indirect impact on the e-economy. The criterion "cost of medical and psychological treatment" represents a negative economic impact, i.e. a cost to be avoided. The total cost of each option for the Community budget (costs for public administration) is compared in the third criterion. As regards Member States budgets, the co-funding is voluntary and there are no precise indications of the use of Member States budgets for the previous programmes. If a Member States decides to co-fund an activity, it does so voluntarily.[81] Finally, Table 2 also compares impacts of the four options on third countries and on EU value added.

Table 2: Economic impacts

	Deployment and use of ICT	***Cost of medical and psycholog. treatment***	***Cost for public administration***	***Economic impact on third countries***
Option 1 no change **(baseline)**	Indirect positive impact as a result of safer online environment	Further reduction of costs	€ 10.25 million annual budget. Slightly reduced administration costs in COM[82]. None to low costs in MS.[83]	Limited risk of a shift of criminal activities to third countries generating negative economic impact
Score **(baseline)**	*3*	*3*	*3*	*3*
Option 2 adjust the scope	Similar to Option 1	Similar to Option 1	€ 11 million annual budget. Administration costs in COM higher than under Option 1 (14,53	Similar to Option 1

81 The response of Member States to cuts in the Community budget (Option 3 and 4) will be probably very different, depending on the activities of individual MS in this area. However, it can be said that the likelihood that Member States will take over the programme under Options 3 and 4 is generally low (see Section 8.1).

82 In comparison to the current Safer Internet plus programme

83 Low impact only in the case that Member States decided to co-fund activities which is not an obligation.

			%). None to low costs in MS .[84]	
Score	3	3	2	3
Option 3 slow down	Slightly lower impact due to reduced scope of the programme	Slightly higher risk of an increase, compared to Option 1	€ 6.75 million annual budget Administration costs in COM reduced by 17%. None to low costs in MS.[85]	Slightly lower risk than in Option 1
Score	2	2	5	4
Option 4 cease	Much lower impact	Higher risk of an increase, compared to Option 1	0 for Community budget (MS spending probably generally low)[86]	Lower risk than in Option 1
Score	0	1	6	5

6.2. Ranking of options and preferred option

The assessment of the 4 options leads to the following ranking in terms of their expected positive impact. The combination of 4 social and 4 economic assessment criteria allows identifying the **best ratio between social impacts and economic aspects**. The criteria are **not weighted** giving them equal rank.

Level of positive impact	**Score**	**Option**
Highest impact	29	Option 2 "adjust the scope"
	24 (baseline)	Option 1 "no change"
	21	Option 3 "slow down"
Lowest impact	16	Option 4 "cease"

Not to take any action in this field (**Option 4**) does not seem to be viable; many of the expected impacts are noticeably negative. This is underlined by the attained score.

To just continue with the same activities as in the past (**Option 1, baseline**) shows in comparison to Option 2 weaknesses on the level of social impacts when it comes to the challenges due to evolving technologies, technological convergence and changes in social

84 Ibid.
85 Ibid.
86 The likelihood that Member States will take over the programme under Options 3 and 4 is generally low (see Section 8.1).

behaviours. These aspects will need to attain more attention and more intensive work; otherwise new "doors" will be opened at the cost of the most vulnerable citizens – the children.

The same applies to **Option 3**, however, the shortcomings of Option 3 specifically on the level of social impacts are more serious than those of Option 1; Option 3 would to a much lesser extent provide an adequate level such impacts.

As a result of the analysis, the **preference** has been given to **Option 2**, which safeguards and reinforces the *aquis* of the preceding programmes and prepares for the emerging challenges and possible risks in the future. The preferred option is the strategy which best responds to the specific objectives of the impact assessment. It shows the **best ratio between social impacts and economic aspects**.

The public consultation clearly supports this result as stakeholders with almost universal agreement called for maintaining and reinforcing the running **and** for formulating new actions. The respondents made a clear point about the new needs to be addressed in the future programme. Their recommendations deal largely with upcoming new risks for children and corresponding actions; they also coincide in many points with the recommendations of previous evaluations (section 1.3 "Lessons learned"). The most relevant recommendations are:

- Dealing adequately with the effects of emerging technologies, services and uses, and the subsequent risks for children and young people.
- Addressing knowledge gaps through comparative and qualitative studies, particularly focusing on children as 'actors'
- Involving children and young people directly in the Programme
- Proposing a number of new actions for key stakeholder groups, including on law enforcement, education and awareness raising
- Educating and empowering parents and teachers, and promoting media literacy through school curricula
- Involving more stakeholders, especially people and organisations with PR, public awareness campaigns, and media expertise
- Working cross-boundaries
- Embedding awareness projects into social institutions to ensure sustainability beyond EC funding

These recommendations will be well addressed under Option 2. A summary of the conclusions of the public consultation is attached as Annex 3.

7. RISKS AND ASSUMPTIONS

The envisaged programme is based on the following assumptions:

The problem and risks analysis as outlined in section 3 will remain valid over the expected period of five years from 2009 on;

There is an ongoing distinct added value to tackling the underlying problems on the European level;

The programme will be accepted by the multi-stakeholder world it is addressing to;

The financial resources foreseen in the programme assume that co-funding will be readily available from other funding sources;

There will be sufficient staff available and sound management structures in place at Commission level to manage a more ambitious programme according to high standards;

All relevant programme data will be collected in order to allow for an in-depth evaluation of the implementation process and the impact of the programme and – if necessary – for a fine-tuning of its actions.

Risk	Counter-measure
The problem and risks analysis will not remain valid over the period 2009-2013.	The programme provides to build a knowledge repertoire and to do a mid-term evaluation of the programme. Any changes in the risk situation identified there would be taken into account in the annual work programmes.
The distinct added value to tackling the underlying problems on the European level will cease to exist.	It may happen that the actuation of the Member States will be stimulated so much that some activities would need less support on EU level (nevertheless past experience does not support such a scenario). In such a case the Commission would in its annual work programmes decrease its support to such areas and at the same time analyse whether its support to non-affected issues may - taking into account ongoing technological and behavioural developments - be intensified. Alternatively it could be considered not to spend the programme budget fully.
There are not enough applications for, or interest in, certain programme actions.	This is highly unlikely as the programme is based either on tested and successful actions of the preceding programmes or on results from stakeholder consultations. If however needed, targeted information and awareness-raising could be provided via the awareness raising network in order to stimulate interest.
The financial resources needed for co-funding will not be available from other funding sources.	The Commission has no control over the financial situation of stakeholder organisations. However, past experience in the preceding programmes, where co-funding was required, is in general positive. The case given the Commission could consider raising its own share of funding in certain cases (e.g. for NGOs).
It turns out to be difficult to manage a more ambitious programme.	The number of single-standing contact points / nodes will be reduced by establishing consortia which run the different network functions under one contract; this will alleviate the current administrative burden and unleash capacities for new tasks.
There is no data collection system in place which allows for the evaluation of the programme.	A data collection system for the preceding programme is already in place and tested. It will be fine-tuned in the envisaged programme. The results of the planned mid-term evaluation will furthermore allow adapting the system to changing needs.

8. A PROPOSAL FOR A NEW PROGRAMME

The final choice, Option 2, consists of a coherent strategy for protecting children when using online technologies. Option 2 will be built on the principles of continuity and enhancement:

- Continuity: reinforce the achievements of the preceding initiatives so as to ensure that their effects continue and gather momentum taking account of lessons learned;

- Enhancement: meet new threats, understand better the evolvement of existing conduct and new threats, ensure and deepen European added-value, broaden international outreach.

The final choice is not expected to lead to any negative impacts on any target group - they have been described in chapter 4.1 (other than producers and distributors of child sexual abuse material and other illegal content). It is neither expected to generate negative economic impacts nor additional administration costs on the side of the Member States. The beneficial impacts will be wide-spread; it is the option which will help most effectively to reduce the risks for children using online technologies.

This Decision respects the fundamental rights and observes the principles reflected in the **Charter of Fundamental Rights of the European Union**, in particular Articles 7 and 8. It specifically aims at safeguarding the physical and mental integrity of children and young persons; it does so in agreement with Article 3 of the Charter.

Candidate countries will be invited to be integrated into the new programme. Third countries will also be involved in activities. In appropriate cases, subject to the approval of the Programme Committee, the co-funding of projects in third countries is envisaged so as to increase the impact of the programme having regard of the global scope of online technologies.

The programme will be implemented via calls for proposals and / or tenders leading to the financing of projects, best practice actions, networks, and accompanying measures. In case of reporting structures and coordination of awareness activities on national level, a longer contract period would bring an additional stability into this infrastructure. Typical duration of projects will therefore be in the order of 30 – 48 months.

For further details on the envisaged programme see Annex 2.

8.1. European Added Value and the principle of subsidiarity

As access to online technologies becomes more widespread throughout Europe and the rest of the world, children themselves increasingly become active users. The issues addressed are of a global nature and therefore need national, European and international solutions.

Illegal content, more specifically material depicting or documenting child sexual abuse may be produced in one country, hosted in a second, but accessed and downloaded all over the world. Commercial payment systems operating worldwide may be used to fund sale and purchase of the images.

This trans-national element makes it particularly problematic for law enforcement in this area of crime[87]. To determine which country has jurisdiction to start an investigation and to prosecute the suspect, the *locus delicti* has been, and continues to be, of decisive importance. In most cases, there is more than one *locus delicti*. When possession, distribution and production of child sexual abuse material are considered a crime, it is common practice that

[87] Child Pornography Legislation within the European Union, Europol 2005, p. 9.

these three crimes take place in different countries. The new programme will play a supportive role in this area, and will encourage and support law enforcement in the identification of victims of online-related sexual abuse.

The example shows that actions on all levels (global EU level / national / regional / local) are necessary. However, they are not alternatives but show their best effectiveness when working together **complimentarily**.

Action at Member State level is essential, involving a wide range of actors from national, regional and local government, industry, parents, child welfare NGOs and social workers to teachers and school administrators. The Community can stimulate best practice in Member States by carrying out an orientation role both within the EU and internationally and providing support for European-level benchmarking, networking and adding to the knowledge base. The national activities can help to produce a "multiplier effect" whereby the benefit of best practice can be distributed more widely than would otherwise be the case. The re-use of tested tools, methods and strategies, the promotion of the best performing technologies (like parental control tools) or access to updated data about users (as for example on uses and risks to children in the online environment) on European level will furthermore enhance the cost-efficiency and the quality of operation of actors on the Member State level.

In the area of child safety and protection in the context of online technologies the measures which are in place in Member States are not of a uniform nature, i.e. the protection level varies between the countries: there are more activities in some Member States than in others, in varying degrees of intensity. Specifically in some New Member States "the measures concerning the protection of minors … do not seem to be as far-reaching" as in others[88]. The design of the new programme aims at maximising synergy with national activities through networking and EU initiatives (e.g. deployment of supporting technologies, investigation into changing behaviours and risks).

Synergy can also be expected with Commission policy and actions in the area of protection of minors in audiovisual and information services, in all actions relating to network and information security and those in the area of criminal law (cyber crime). The new programme will avoid overlapping with or doubling of efforts with other EU initiatives or programmes.

The evaluations of the preceding Community activities have shown that there exist a significant number of activities which would not have been taken at all without the intervention of the previous Community programmes. In other cases, activities would not have benefited from the exchange of best practice with other European countries. The evaluation reports of the preceding programmes give indications about the **added value** of the Community action and allow a prediction on the expected degree of additionality in the new programme: 57% of all organisations indicated they would not have become involved in projects in the absence of EU funding[89]. Once involved (only) 58% would have been able to continue if EU funding had ceased (but a number of organisations would have had to reduce objectives and tasks when doing so)[90].

Also, the reports show that without EU funding, no coordination between the activities on national level would have been established as the European networks of hotlines / awareness

---

88 Second evaluation report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity - COM(2003) 776, p. 17.

89 The Evaluation of the Safer Internet Action Plan 1999-2002, Technopolis, July 2003.

90 Final Evaluation Report of the Safer Internet Action Plan (2003-2004), IDATE, May 2006.

nodes would not have been set up[91]. This indicates that, although some progress would have certainly been achieved without the previous programmes, the networking effect and the pan-European coverage would not have been achieved.

Over the years, the EU interventions have generated a more extended "infrastructure". As a result of previous Community actions "the number of hotlines and codes of conduct has increased significantly [after the year 2003]. The launch of campaigns in most Member States to encourage safer use of the Internet is a very positive development"[92].

The Commission, in cooperation with Member States and other partners, is well placed to coordinate these activities.

It will in any case take action in this field by respecting the **principle of subsidiarity**, i.e. only if, and insofar as, the objectives of the proposed action can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level, will the Commission take action. Networking and access to good practise, spreading and generation of knowledge (e.g. via updating the knowledge base), co-ordination of activities (e.g. Safer Internet Day), cross-cutting co-operation between different public bodies, ministries on national and regional levels, NGOs, law-enforcement and industry are issues where the new programme will give the necessary impetus.

Since online technologies have a global dimension, **international co-operation** is also essential and can be stimulated through the Community networking structures and other international activities as for example by cooperating with organisations with a global scope. Third countries can provide useful indications about the way in which children are using the technology and new ideas on how to equip them and their parents, carers and teachers with the necessary knowledge. The awareness network will ensure that an exchange of experience beyond the borders of the EU happens. There is already a variety of action in organisations with membership wider than the EU Member States, and the Commission is involved in these together with the Member States.

Finally, the new programme is also **complementary** and coherent with other **Community actions**. Chapter 1.3 gives an overview on relevant activities. Specific attention will be given to those measures directed at law enforcement and at the financial sector (e.g. purchase of child sexual abuse material through credit cards) in order to ensure full coherence and close co-operation with the actions taken under the Commission's Cyber Crime Communication.

9. COST-EFFECTIVENESS

The proposed intervention is estimated to cost 70 million Euros.

9.1. Justification of the cost of the proposed intervention

The evaluations of the preceding programmes have confirmed that spending constitutes good value for money.

From a financial perspective, the envisaged programme remains to be a rather small one. The planned overall budget is of 55 million Euros and equals an annual budget of 11 million Euros.

---

91 The Evaluation of the Safer Internet Action Plan 1999-2002, Technopolis, July 2003.

92 Ibid. However, at the same time the 2006 evaluation report states that if Commission funding ceased still one third of Hotlines and Awareness nodes would not be able to continue for the lack of alternative funding.

Attention will be given to improving the effectiveness of the implementation of the envisaged programme. The current structure of the European networks (see baseline scenario / Option 1) will be further developed by creating network relays which combine different services and functionalities under one roof (for details see under the section 5.4.3.). This will reduce costs and allow (co-)funding those new activities which require so. The latter concerns overall the increase of the budget share for awareness raising and the broadening of the knowledge base.

9.2. Cost-effectiveness of the funding mechanism

The programme will be executed through indirect actions – calls for proposals and calls for tender as appropriate – and include international activities. Measures devoted to the commercialisation of products, processes or services, marketing activities and sales promotion are excluded. They comprise:

(1) Shared-cost actions

- Pilot projects and best practice actions. Ad-hoc projects in areas relevant to the programme, including projects demonstrating best practice or involving innovative uses of existing technology.
- Networks and national actions bringing together a variety of stakeholders to ensure action throughout the Europe and to facilitate co-ordination activities and transfer of knowledge.
- Europe-wide investigation carried out on a comparable basis into the way adults and children use online technologies, the resulting risks for children and the effects of harmful practices on children, on behavioural and psychological aspects with emphasis to child sexual abuse related to the use of online technologies, research on upcoming risk situations due to transforming behaviours or technological developments etc;
- Technology deployment projects.

(2) Accompanying measures

Accompanying measures will contribute to the implementation of the programme or the preparation of future activities.

- Benchmarking and opinion surveys to produce reliable data on safer use of online technologies for all Member States collected through comparable methodologies;
- technical assessment of technologies such as filtering designed to promote safer use of Internet and new online technologies;
- studies in support of the programme and its actions;
- exchange of information through conferences, seminars, workshops or other meetings and the management of clustered activities;
- dissemination, information and communication activities.

The above analysis has demonstrated that the **same results cannot be achieved by lower costs.** This would necessarily imply to save costs by reducing actions which would lead to a non-compliance with the whole set of objectives. Nor is it possible to achieve **more results with the same costs**, taking into account that :

- the largest part of the budget will be spent on the networks and on the national actions which build the basic EU-wide infrastructure for fighting considerable and serious risks for children;

- a larger part of the funding would be directed to non-governmental organisations (often the best partners to take necessary steps in this field): their low overheads and ability to call other organisations for support help them to provide high impact for a relatively small Community contribution;
- the cost share incumbent on the Community for running an individual node is rather low and therefore cost-efficient.

There is no alternative mechanism to produce comparable results.

In the light of the above, it can be concluded that no other instruments would allow for the same or better results to be achieved at the same or even less costs.

	Effectiveness	**Cost**	**Risks**	**Administrative overheads**
Pilot projects, Best practice actions, technology deployment	High	Medium to High	Medium to High	High
Networks / nodes	High	Medium*	Low	Medium
Investigation of user issues	High	Medium	Low	High
Accompanying measures	Medium	Low	Low	Medium
Meetings	Medium to High	Low	Low	Low

* The individual costs of each node in the networks are low, but there are currently about 25 of them in each network, plus the network co-ordinators.

The above analysis has shown that networking will create benefits by creating leveraging effects. Work on technical issues (e.g. deploying technological tools), Investigation of user issues (e.g. children's use of online technologies), accompanying measures and meetings organised by the Commission all give worthwhile results for the cost and efforts involved as it has been demonstrated in the past and been confirmed by the evaluation reports.

10. MONITORING AND EVALUATION

The implementation of the programme, including monitoring, will be carried out by Commission services. Monitoring of the programme will be ongoing. It will be based on:

- two programme evaluations with the assistance of outside experts;
- the information obtained directly from beneficiaries, who will submit interim and final activity and financial reports, including performance indicator criteria set out in the project contracts. All projects and actions will be contractually obliged to implement project-run evaluation provisions, run by external experts or internal sources, and contain performance indicators and guidelines for follow-up.

Sources of data for the indicators can be divided into programme level and project-level data sources.

10.1. Programme level data sources

2 programme evaluations will be used to measure the direct or indirect impact of measures co-funded by the new programme. As the previous Safer Internet programmes have already been evaluated by external contractors (2001, 2003 and 2005), any further evaluations will allow us to judge the long-term impact of the Community actions and on the evolving changes in society. Programme evaluations will be carried out by independent companies specialising in evaluations, following tendering procedures in line with Commission standard practices. The design and implementation of the evaluation is a task shared with DG INFSO's evaluation unit and it is accompanied and supervised by a Steering Committee which includes outside experts.

The Eurobarometer surveys cover a scientifically selected sample of EU citizens and citizens of candidate countries. Three surveys have been carried out (2003-2004, 2005 and 2007). Also in this case future surveys will allow understanding the long-term impact of the Community actions and the way societal behaviours evolve.

10.2. Ex-post assessment of the results on programme level

An interim evaluation will be carried out in the second year of the programme. This evaluation will assess the programme effectiveness and efficiency, review its implementation logic and – if applicable – formulate recommendations to redirect the programme actions.

An *ex post* evaluation focused on the impact of the action will be carried out at the end of the programme. The indicators defined on project level and those on programme level as listed below will be defined as part of the competitive procedures designed to award contracts to carry out this task.

10.3. Project level data sources

Projects are required to produce progress reports for the Commission every 6 months. These reports are subject to approval by the Commission Project Officer and form part of the material for the review by external experts at least once during the life of the project.

The Commission will include systematic reporting requirements and appropriate indicators into the project application forms (standard work packages and deliverables) for networks and national activities and, following this, in the technical annexes of contracts. These data will allow judging the performance and impact of individual projects as much as of the action line as a whole. Corresponding provisions will be implemented in all other contracts supported under the new programme.

The financial implications are measurable through the documents submitted by the projects – the estimated budgets and the periodic cost statements.

Audits of individual projects and/or on the programme implementation will be carried out on a regular basis, as part of the annual programming of the Information Society DG.

For the purpose of effective evaluation and assessment of cost-effectiveness the following indicators have been identified:

Specific Objectives	Indicators
Illegal content and harmful conduct/content	
Providing the public with contact points for reporting online illegal content and harmful conduct	Quantitative/qualitative data on the establishment and operation of reporting points; n° of reporting points, MS coverage, n° of reports received, n° of police actions implemented thanks to reporting points (feedback needed from police), n° of web pages withdrawn from ISP thanks to reporting points tips; degree of public awareness of reporting points
Dealing effectively with harmful conduct online, in particular grooming and bullying	The degree of awareness of EU citizens about harmful conduct online
Stimulating development and application of technical solutions for dealing with illegal / harmful content and harmful conduct online	Number and coverage of projects for technical solutions
Promoting a safer online environment	
Encouraging industry engagement in creating a safer online environment by stimulating development and implementation of self-regulation systems	The number of successful meetings and conferences organised and/or participated in. Code(s) of conduct: quality assessment, number of self-regulatory operations implemented
Stimulating cooperation between relevant stakeholders promoting a safer environment and tackling harmful content	The number of successful meetings and conferences organised and/or participated in. The number of projects and initiatives enhanced
Awareness-raising	
Empowering users to stay safe online	The development of awareness levels of EU citizens about empowerment issues
Providing the public with a coordinated and effective effort to raise awareness and to disseminate information about risks and safety measures	Quantitative/qualitative data on the awareness activities - MS coverage, n° of staff involved, - n° of awareness actions, - visibility (e.g. web hits, media coverage), - development of awareness levels of EU citizens, no of stakeholders reached (schools visited, trainers trained…)
Stimulating enhancement and development of awareness raising methods and tools concerning online safety	Number of replicable awareness tools (which proved to be effective)
Stimulating the involvement of children and young people in creating a safer online environment	The number of children involved, the number of activities with children involved
Establishing a knowledge base	

Encouraging a co-ordinated approach concerning investigation across the EU with a view to increasing child safety online	The number of themes covered, the number of countries addressed
Ensuring stable knowledge of updated information concerning children's use of online technologies and the subsequent risks	The number of projects and/or of publications
Broadening knowledge concerning children's own strategies for dealing with online-related risks	The number of projects and/or of publications
Promoting studies on online-related sexual exploitation of children	The number of projects and/or of publications
All actions	
Enhancing co-operation, exchange of information, experience and best practice between relevant stakeholders on EU and international level	The number of successful meetings and conferences organised and/or participated in

ANNEX 1

Legislative instruments

A variety of legislative instruments exist which lay down rules that Member States are required to implement. For the purpose of this Impact Assessment, the following legislative and non-legislative measures have been analysed, particularly in relation to possible overlapping.

The *Electronic Commerce Directive*[93] regulates the liability of intermediary service providers for "mere conduit", caching and hosting. The Directive excludes any obligation of network operators to monitor the information they transmit or store.

The *Directive on privacy and electronic communications*[94], besides containing provisions on spam, envisages also an obligation for service providers to take measures to safeguard security and to inform users in case of particular risk of breach of security of the network.

The *Directive on the retention of data*[95] is aimed at preventing, investigating, detecting and prosecuting criminal offences which in particular covers those related to the sexual abuse of children and documentation of such abuse, as it ensures at EU level that certain data, in the course of the supply of communications services, are retained for a certain period of time.

The *Recommendation on the protection of minors and human dignity in audiovisual and information services* adopted by the Council in 1998 was the first legal instrument concerning the content of on-line audiovisual and information services made available on the Internet. It makes recommendations for Member States, the industry and parties concerned and the Commission including indicative guidelines on protection of minors. The Recommendation was evaluated twice, for the first time in 2000/2001[96]. The second evaluation report[97] (adopted on 12.12.2003) showed that the Recommendation is still being applied in different ways by the Member States (25), but that the developments are, in general, positive. It also showed that even though self- or co-regulation was still less developed in the broadcasting sector, the relevant systems seemed to be working quite well. The involvement of consumer associations and other interested parties in the establishment of codes of conduct and other self-regulatory initiatives still leaves a lot to be desired.

On 20 December 2006 the European Parliament and the Council adopted a *Recommendation on the Protection of Minors and Human Dignity and on the Right of Reply.* It builds on and supplements the 1998 Council Recommendation on the same subject, which will remain in force, taking into account recent technological developments and the changing media landscape[98]. It extends the scope to include media literacy, the cooperation and sharing of experience and good practices between self- and co-regulatory bodies, action against discrimination in all media, and the right of reply concerning online media. The Recommendation calls for a further step to be taken towards establishing effective cooperation between the Member States, the industry and other interested parties as regards the protection of minors and human dignity in the broadcasting and Internet services sectors.

---

93 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

94 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

95 Directive 2006/24/EC on the retention of data generated of processed in connection of the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

96 COM(2001)106.

97 Second evaluation report from the Commission to the Council and the European Parliament on the application of Council Recommendation concerning the protection of minors and human dignity - COM(2003)776.

98 2006/952/EC; OJ L 378 of 27.12.2006

The *Council Decision to Combat Child Pornography on Internet*[99] calls Member States to promote and facilitate investigation and prosecution, to encourage Internet users to report to competent authorities, to use the existing points of contact, to cooperate with Europol and Interpol and also to build up dialogues with the industry.

The *Council of Europe Convention on cyber crime*[100] is no doubt the most important and comprehensive international instrument in this field and it explicitly refers to "Offences related to child pornography", but its significance depends also on its application. By 1 March 2007 only 10 Member States and 9 non EU Member States had ratified the convention, letting it be implemented into national law. The Convention on cyber crime aims to facilitate international cooperation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive and procedural law and for jurisdiction. The Convention only covers a number of specific legal and procedural questions, whereas the planned new programme under this Impact Assessment exercise will envisage concrete actions to combat the risks for children when using online technologies.

The EU *Framework Decision on child pornography*[101] sets out minimum requirements for Member States in the definition of offences and appropriate sanctions. Forms of conduct that are punishable as "an offence concerning sexual exploitation of children" whether undertaken by means of a computer system or not are the production of child pornography; the distribution, dissemination or transmission of child pornography; making child pornography available; the acquisition and possession of child pornography. Member States had to take the necessary measures to ensure that the instigation of one of the listed offences, or an attempt to commit that offence, is punishable (Art. 4) by 20 January 2006 (Art. 12).

The recent *Council of Europe Convention on the Protection of children against sexual exploitation and sexual abuse* (adopted by the Committee of Ministers on 12 July 2007) establishes the various forms of sexual abuse of children as criminal offences, including such abuse committed in the home or family. In addition to offences traditionally committed in this field - sexual abuse, child prostitution, child pornography - the text also addresses the issue of "grooming" of children for sexual purposes and "sex tourism"[102].

The Commission's Communication "*Towards an EU Strategy on the Rights of the Child*"[103] is a cross-cutting document addressing internal and external policies on children's rights in a coherent way, fully consistent with the already existing community action plans and programmes.

The *Specific Programme "Prevention of and Fight against Crime"* (Council Decision of 12 February 2007)[104] has the objective of "providing citizens with a high level of safety within an area of freedom, security and justice". This covers various forms of crime, namely with a strong cross-border dimension, explicitly including victimized children ("offences against children" and also "trafficking in persons").

The European Parliament and the Council adopted on 20 June 2007 a *"Specific programme to prevent and combat violence against children, young people and women and to protect victims and groups at*

---

99 Council Decision 2000/375/JHA of 29 May 2000 to combat child pornography on the Internet.

100 Council of Europe Convention on Cyber crime, 2001: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

101 Council Framework Decision 2004/68/JHA of 20 January 2004 on combating the sexual exploitation of children and child pornography.

102 Adopted by the Committee of Ministers on 12 July 2007at the 1002nd meeting of the Ministers' Deputies. The Convention will be opened for signature at the Conference of European Ministers of Justice on 25 and 26 October this year.

103 COM(2006) 367, 4.7.2006.

104 Council Decision 2007/126/JHA of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme "Prevention of and Fight against Crime".

risk" ("Daphne III" programme).[105] The programme intends to benefit children and young people who are, or risk becoming, victims of violence.

The Commission's initiative on *Media Literacy* aims at highlighting and promoting good practices in this field adding a further building block to the European audiovisual policy under the i2010 initiative. A public consultation on media literacy took place at the end of 2006.[106] A Communication on Media Literacy is planned to be adopted by the Commission still in 2007.

The Commission has made a proposal on a modernized "Television without Frontiers" Directive, called *Audiovisual Media Services Directive*. The proposal introduces the notion of audiovisual media services and distinguishes between "linear" services (e.g. scheduled broadcasting via traditional TV, the Internet or mobile phones, which "push" content to viewers) and "non-linear" services (such as video-on-demand, which the viewer "pulls" from a network). The proposal addresses the issues of protecting minors and of non-discrimination. The Directive is envisaged to enter into force by the end of 2007.

The Commission's Communication "*Towards a general policy on the fight against cyber crime*" of May 2007 also focuses on illegal content regarding child sexual abuse material on the Internet. The Communication aims at strengthening operational law enforcement cooperation, improve international cooperation, providing adequate training for police forces as well as supporting public-private cooperation[107].

---

105 Decision No 779/2007/EC of the European Parliament and the Council of 20 June 2007 establishing for the period 2007-2013 a specific programme to prevent and combat violence against children, young people and women and to protect victims and groups at risk (Daphne III programme) as part of the General Programme "Fundamental Rights and Justice".

106 http://ec.europa.eu/avpolicy/media_literacy/consultation/index_en.htm

107 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - COM(2007) 267, 22.5.2007

ANNEX 2

The structure of the new programme

The concrete policy will have the overall aim to promote safer use of Internet and other communication technologies, especially by children and can be divided into four main actions, which take up the above defined general objectives:

Action 1: Reducing illegal content and tackling harmful conduct online

The activities aim at reducing the amount of illegal content circulated online and dealing adequately with harmful conduct online, with particular focus on online distribution of child sexual abuse material, grooming and bullying. It is proposed to provide funding for contact points which facilitate the reporting of online illegal content and harmful conduct. These contact points should liaise closely with other actions at national level, such as self-regulation or awareness-raising and cooperate on a European level to deal with cross-border issues and to exchange best practice.

Further activities will be aimed at stimulating development and application of technical solutions for dealing with illegal content and harmful content online, and at promoting cooperation and exchange of best practice of a wide range of stakeholders on European and international level.

Action 2: Promoting a safer online environment

The activities will aim to bring together stakeholders to find ways to promote a safer online environment and to protect children from content and conduct that may be harmful for them. It will encompass cooperation and exchange of experience and best practise between relevant stakeholders on European and international level, it will encourage the development and implementation of systems of self-regulation and of technical solutions and to ensure users with instruments and applications adequately supporting them when dealing with harmful content or conduct.

A specific focus will be to stimulate the involvement of children and young people with the aim of understanding their views on and experiences with using online technologies better and of benefiting from their contributions when designing awareness actions, tools, materials and policy strategies.

Action 3: Ensuring public awareness

The activities will aim at increasing the awareness of the public, in particular children, parents, carers and educators, about opportunities and risks related to the use of online technologies and means of staying safe online.

Actions will be taken to promote public awareness by providing adequate information about possibilities, risks and ways to deal with them in a coordinated way across Europe and by providing contact points where parents and children can receive answers to questions about how to stay safe online. Activities will encourage cost-effective means of distributing awareness information to a large number of users.

Specific attention will be given to the development and/or identification of effective awareness instruments, methods and tools which, in cost-efficient way, can be replicated throughout the network and also internationally. Actions will also aim at ensuring exchange of best practices and cross-border cooperation on European and international level.

Action 4: Establishing a knowledge base

Changes in the online environment happen fast, and new trends in the use of the technologies emerge all the time. There is a need for establishing a knowledge base for dealing adequately both with existing and emerging uses, risks and consequences, and mapping both quantitative and qualitative aspects in this context. The knowledge will feed into the implementation of the Programme as well as into designing adequate tools for ensuring safety online for all users.

This will cover the coordination of investigation activities in relevant fields within and outside of the EU. They will specifically (but not exclusively) target child sexual abuse (linked to online technologies): actions will cover technical, psychological and sociological issues, in particular related to online child sexual abuse material and grooming. The (evolving) way children use online

technologies (and associated risks) and the (harmful) effects the use of online technologies can have of them will be studied. Studies can concern awareness-raising methods and tools, successful co- and self-regulatory schemes, the effectiveness of different technical and non-technical solutions, as well as other relevant fields.

ANNEX 3

Summary of the results of the public consultation (Online public consultation and Safer Internet Forum 20-21 June 2007)

Many respondents expressed a need to keep in mind the overwhelmingly positive potential of the internet, to inform, educate, entertain and – as far as industry is concerned – to drive business success. At the same time there is now a growing understanding that the idea of creating a risk free internet for children and young people is an illusion, and that they have to be equipped and learn how to avoid hazards and deal with risks.

Convergence of technologies opens up new routes for education and socialising and potentially risky activities; it can also be a positive and effective way of providing multiple, easily accessible support to children and young people.

Nevertheless, there remains a common vision and sense of urgency regarding tackling online-related sexual abuse of children, both in terms of illegal content and of conduct, such as targeting children for grooming and potential contact abuse. Solid evidence is building up indicating that multi-stakeholder collaboration works, with the expectation that the visible, combined efforts of an increasing number of stakeholders and actions under the new call for proposals in 2007 will increase the speed and effectiveness of developments.

Projects which demonstrably have worked well require promotion and financial support to enable their multiplication across Europe as models of good and effective practice.

Many contributors to the online consultation listed a number of other illegal online activities, from selling alcohol to children, to racism/xenophobia, drugs promotion, anorexia/bulimia sites, glorification of war, bomb-making, sale of weapons etc. Whilst prioritising the tackling of child abuse over all of these, some stated that action should also be taken against a broader range of illegal activities.

Parents and professionals need to acquire a better understanding that children and young people live in a world of ever increasing sophistication of technological means, with content globalisation and its ongoing availability on the internet and supporting new global forms of social networking, also via mobile devices.

Specific conclusions and recommendations

Illegal and inappropriate content

EU-level action with regard to legislation and law enforcement cooperation should be taken. Whilst many stakeholders now use the term 'images of child abuse' rather than child pornography, the definition should be open-ended and include any and all forms of sexual exploitation of children and young people, including pseudo-images and non-photographic material such as texts.

Many stated that efforts so far in the fight against illegal content had been positive, and that these good results must not be jeopardised. Online child abuse is expected to grow dramatically, take on new forms, have an increasingly common financial route as part of organised crime, and become more trans-national.

Prime responsibility for fighting against any illegal activities and illegal content such as child sexual abuse material, should rest with the police. Law enforcement bodies' capacity should be strengthened, to be able to take a more proactive approach and be able to engage in cross-border co-operation. More sting operations with the police and hotlines cooperating were considered effective ways of combating online child abuse.

Update legislation

Different legislation across Europe exists concerning online child abuse, grooming and physical contact arising thereof. There is a need for greater clarity and standardisation.

Awareness raising and training

Professionals working with children, particularly within the judicial and child protection systems, should receive qualified training about the dynamics of child sexual abuse and its relationship to the production and distribution of child abuse images. Networking opportunities should be provided. Specific measures to close the widening gap between parents, teachers and children are being proposed, with education and awareness raising playing a key role.

Many proposals were made with respect to empowering children and young people. Measures are required to strengthen children's capacity to be creative and innovative, alongside promoting an understanding that children are consumers and potential victims as well as actors – in both positive and negative ways – with regard to the new technologies.

There is a need to improve the understanding of the relationship between online and offline worlds with regard to risks, and the nature and reasons for children's risk-taking activities. The Commission should therefore also support the development of websites with good and attractive content for children as a positive, preventive measure.

Learning from other public awareness campaigns, robust measures should be developed to assess the impact of awareness campaigns at different levels and on different target audiences. The role of the Safer Internet Day remains crucial.

Education should focus on empowering and building the capacity of children and adults themselves to take and disseminate preventive and educational measures. Such education should be integrated into the curriculum and promoted as 'media literacy', be compulsory, and part of citizenship education.

Stakeholders working together

There was a consensus that multi-stakeholder, public/private partnerships can be very successful, evidenced by a growing number of good practice examples. The continuing independence and ethics of awareness nodes need to be safeguarded. The need for a comprehensive approach was stressed, with multiple stakeholders working together as individual actions by individual agencies have limited impact and effectiveness. Multi-stakeholder partnerships should be expanded and fortified. Good practice models of joint projects should be promoted and financially supported. Closer relationships with the media should be built. NGOs need more effective support with their work and in accessing existing networks.

Technical solutions

There is a widely shared understanding that a combined solution, of improved education and greater awareness, and better technical solutions is required. Specifically, there should be support for the development and use of software to trace, analyse and block websites disseminating online child abuse material, tighter age identification/verification systems and implementation mechanisms.

Political and other actions

The Commission was asked to provide support and to promote a holistic approach to cooperation between different stakeholders, in particular governments at national and European level and to move the tackling of child sexual abuse higher up the European political agenda. The Commission was urged to work with education ministries to integrate media literacy into citizenship education, and embed online use and awareness raising into school curricula throughout Europe. Teachers need to be empowered with appropriate support, guidelines, and e-safety training to fulfil the tasks.

International cooperation

The work of INHOPE, the international network of hotlines, supported by the Safer Internet *plus* Programme, as well as that of national hotlines, is highly valued and most, though not all, contributors argued for their continuation with more support. There were several suggestions on how the hotline model 'needs to evolve', including the need to adjust to higher volumes of reports, reviewing whether the data collected is made full use of, and collaborating more closely with law enforcement, and with awareness nodes.

An international network of NGOs was suggested, one that can engage with the public and lobby governments. Illegal websites should be blacklisted giving priority to certain countries.

Self regulation

A framework agreement along the lines of the one created by EU mobile operators was suggested, to promote a self-regulated code of ethics for the industry stakeholder groups including Internet Service Providers, Network Operators, companies providing hosting services and web designers, and with governments developing monitoring systems to see whether the code is actually applied. Other industry representatives stressed the need for, and gave examples of a co-regulatory approach.

Recommendations for the Knowledge base

There was a strong sense of the need to establish reliable facts and figures, and to coordinate effectively what is known. A convincing case was made to invest in more qualitative, in-depth investigation, and to develop comparative research. Research findings should made available more widely. Many specific areas for new investigation were identified.

The need to pool existing research more effectively to help identify and address current knowledge gaps was identified. All stakeholders are requested to contribute their research material, especially on access through mobile devices in addition to that through the so-called fixed internet.

Overall, the need to carry out further investigation on the safer internet was paramount, as was the call for such research to be comparative and of high quality. Below is a summary of the most urgent knowledge gaps identified, relating to psycho-social, quantitative and technical aspects. There are a number of preparatory and procedural issues to be dealt with, including developing tools and methodologies for more refined analyses of, for example, different levels of danger, and prioritising risks.

The Commission, governments and 'big industry' were urged to continue investing heavily in investigation. Collaborative investigation involving children's NGOs was suggested.

General areas for investigation which were recommended are inter alia:

- The importance of the broader context for the consequences of online communication
- To improve the understanding of risk in the relationship between online/offline worlds
- The impact of online incidents: how the use of online communication complement abuse through traditional methods; more data on types, methods and rates; and tracking of online child abuse incidents
- Identifying which types of websites attract both children and sexual predators
- The (emerging) link between depression and grooming, in both abuser and abused
- Risks evolving into actual harm to children; the precise nature of harmful consequences
- Measuring the level of trust in trans-generational communication
- Auditing online content aimed at children

Investigation is to be structured into 3 Cs (content, contact, conduct) while recognising that a child using online services can fall into all three categories. Increasingly the focus should be on the child as actor as existing research recommendations indicate. Research has to address what happens in reality, on- and offline, not what adults think is happening, especially regarding changing attitudes to sex and sexuality. Regarding the "3 Cs" the following areas have been specifically recommended to be better investigated:

Content: the child as recipient

- identifying the most vulnerable target groups of children for online abuse, with the help of social workers, psychologists, and specialists
- the psycho-social impact on children, ranging from accessing offensive images online, to being abused
- children and young people's own perceptions of risk and harm

- children and young people's reactions to online predators
- reasons for not disclosing abuse
- technologies and procedures for victim identification
- ways of supporting victims

Contact: the child as participant

- differences in use between age groups
- children's understanding of content globalisation and its ongoing availability on the internet
- age verification

Conduct: the child as actor

- communication patterns among children themselves
- communication patterns between children and adults, in particular parents and teachers
- what users do as opposed to what they say they do online
- the relationship between young people's sexuality and online grooming
- the psycho-social impact on children from accessing offensive images
- profiling of risk-taking online behaviour by different groups of children
- children's use of technology such as web cameras and cell phones
- children's own reaction to regulations (e.g. filtering) and how they bypass restrictions
- age verification

Further recommended areas are:

Families and parents

- changing attitudes towards strangers between different generations
- the relationship between the quality of parenting and grooming
- exploring strategies and effectiveness of parental regulation

Offenders

- new ways in which sexual abuse is caused by new technologies
- how offenders use the internet, e.g. how they find and target children
- the progression from accessing images of child abuse to grooming
- the changing nature of grooming behaviour
- the link between consumption of child abuse images, and contact sexual abuse
- new and changing profiles of online child abusers
- how to limit distribution of child abuse materials through newly appearing content production tools
- the link between children and young people downloading images of child abuse and the cross-over into sexually harmful behaviour
- the dividing line between normal adolescent behaviour and sexually harming children

Law enforcement

- how investigations into child abuse images are handled

European comparative facts and figures

- robust statistics (nationally and Europe-wide), particularly on online sexual abuse and grooming

- comparative study of relevant legislation
- co-ordination, harmonisation and standardisation of procedures, e.g. online undercover operation in chatrooms, avoiding the charge of entrapment

ANNEX 4

Information sources and documentation used

In addition to the legislative and policy instruments (section 1.3 and Annex 1) sources used for the Impact Assessment include:

Programme evaluations

- Evaluations of the Safer Internet Action Plan (1999 to 2004) and the Safer Internet *plus* programme

Implementation report of Safer Internet *plus* (2005-Mid-2006)

Ex-ante evaluation for Safer Internet *plus*

Final evaluation of Safer Internet 2003 – 2004

Evaluation of Safer Internet 1999 - 2002

Evaluation of Safer Internet 1999 – 2000

http://ec.europa.eu/information_society/activities/sip/programme/evaluations/index_en.htm

Eurobarometer surveys on Safer Internet

The Eurobarometer survey presents the attitude of European Union citizens towards illegal and harmful content on the Internet and their knowledge of how to protect their children against it.

Eurobarometer survey 2007: Safer Internet For Children, Eurobarometer Qualitative Study in 29 European Countries: Summary Report (May 2007) and 29 Country Reports (2007)

Eurobarometer survey 2005

Eurobarometer surveys 2003-2004

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

Public consultations

- Public consultation on Safer Internet and online technologies for children launched on 12 April 2007, open until 7 June 2007.

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

- http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htmChild safety and mobile phone services

The public consultation was launched on 25 July 2006 and was open until 16 October 2006. The consultation document "Child safety and Mobile phone services" explored the issues raised by the use of mobile phone services by children and young people.

Public consultation site and summary report

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

Research

- "The Appropriation of New Media by Youth" (Mediappro research project) – final report

Mediappro aims to enhance user safety by identifying how young people appropriate digital media and how their practices differ within different contexts of use (at school and at home, for example).

http://www.mediappro.org/publications/finalreport.pdf

- Media Literacy website

http://ec.europa.eu/comm/avpolicy/media_literacy/index_en.htm

Public consultation on media literacy (results to be published in April 2007)

http://ec.europa.eu/comm/avpolicy/media_literacy/consultation/index_en.htm