



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.3.2004
SEC(2004) 148

COMMISSION STAFF WORKING PAPER

EX ANTE EVALUATION

**Safer Internet plus
(2005-2008)**

{COM(2004)91 final}

COMMISSION STAFF WORKING PAPER

EX ANTE EVALUATION

**Safer Internet *plus*
(2005-2008)**

TABLE OF CONTENTS

0	Introduction.....	3
1	Problem analysis and need assesment.....	3
2	What is the main objective the programme intends to achieve?.....	7
3	What is the intervention logic proposed?.....	10
4	The expected impacts.....	17
5	Monitoring and evaluation.....	20
6	Stakeholders' consultations.....	22
7	Commission draft proposal.....	24
8	Lessons from the past.....	27

0. INTRODUCTION

This document was prepared following the ex ante evaluation guidelines¹ to support the process leading to the proposal for a multiannual Community programme, Safer Internet *plus* (2005 – 2008).

The proposed programme is based on the experience and the success of the Safer Internet Action Plan (1999 – 2004)².

1. PROBLEM ANALYSIS AND NEED ASSESMENT

1.1 Problem analysis

Illegal and harmful content and conduct on the Internet is a continuing concern for lawmakers, industry and parents. The European Union has been a forerunner in the fight against illegal and harmful content since 1996³.

There are now new challenges both in quantitative and qualitative terms.

Qualitative terms: new technologies include ever-increasing processing power and storage capacity of computers, broadband allowing distribution of content such as video which requires high bandwidth, and the increased capacity of the latest generation of mobile telephone networks. The new generation of mobile phones will be able to distribute "adult" content and discussions are under way how to restrict access to this type of content so that parents can have phones with blocking devices to prevent children stumbling across explicit Web sites and unsuitable online chat rooms.

In quantitative terms, the technological changes already described contribute to an increase in the volume as well as in the types of content distributed.

The level of use of Internet and new technologies is growing. Internet access in the home now accounts for a growing share of the market, and children are exposed even to it in school even where they do not have it in their homes. Internet penetration in the home stands at more than 42% for citizens; it exceeds 90% for businesses and schools. In the 13 months from April 2002 to April 2003, the number of European surfers using high-speed connections (which includes DSL, LAN and Cable Modem) grew by 136%, according to the latest research from Nielsen/NetRatings. In some countries the growth rate was higher, with the UK experiencing the largest increase at 235%.

Broadband users are spending significantly more time online, using the web more often, and visiting more websites than their slower, dial-up counterparts. In Germany, for instance,

¹ Ex ante evaluation – a practical guide for preparing proposals for expenditure programmes – December 2001

² Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors (OJ L 33, 6.2.1999, p.1) as amended by Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 (OJ L 162, 1.7.2003, p. 1)

³ Communication on illegal and harmful content on the Internet COM(96) 487 and Green Paper on the protection of minors and human dignity in audiovisual and information services COM(96) 483.

narrowband users spend on average seven and a half hours on the web every month, whereas for broadband users this increases to 21 hours, equivalent to almost one day per month.

According to a recent survey carried out by one of the awareness projects funded under the current programme covering Denmark, Ireland, Iceland, Norway and Sweden, 97% of children in these countries aged 9 to 16 years have used a computer.

4 out of 10 children who have chatted on the Internet say that people they have only met on the net have asked to meet them in person. 14% of the children have met someone they first met on the net, while only 4 % of the parents think the children have done this. 44 % of the children who use the Internet have visited a pornographic Web site by accident or on purpose. One fourth has received pornographic material through the net. 30 % of the children have seen Web sites with violent material, while only 15 % of the parents think their children have seen this.

This increase in connectivity by children will see a corresponding increase in benefits for them but also risks of "collateral damage".

The proliferation of unsolicited commercial e-mail, or 'spam', has reached a point where it creates a major problem for the development of e-commerce and the Information Society. A significant proportion of spam consists of advertisements for pornography, some of it clearly illegal in all circumstances. It is estimated that over 50 percent of global e-mail traffic will soon be spam.

1.2 Legislation

An essential distinction has to be made between illegal content on one hand and unwanted or harmful content on the other hand - although unwanted or harmful content may also be illegal.

The two categories require different techniques to deal with them.

Illegal content and conduct is whatever is so defined by the applicable national law and although there are 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 police to arrest the offenders and for them to be brought before the courts and convicted and punished if found guilty. 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).

In new media such as the Internet, this process is complicated by the fact that the elements of the offence may be spread out over different countries, and that it may be difficult to exercise jurisdiction over the prime culprits. International co-operation is therefore needed.

Unwanted content is content that certain users do not wish to receive it (a prime example being spam). Harmful content means content which adults responsible for children (parents or teachers) consider to be harmful to those children. There may also be legal provisions restricting distribution of harmful content to adults only (legal pornography, for instance).

A variety of means exist to deal with unwanted and harmful content, all of which need to be used in combination in order to increase their effectiveness: enforcement of legal provisions, self-regulation, technical means such as filtering, and awareness-raising.

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. There is also a divergence of the sensitivity in different Member States to public exposure of nudity and sexual activity and exposure of children to nudity and violence.

However, there are instruments which lay down rules which Member States are required to implement.

The Electronic Commerce Directive⁴ regulates the liability of intermediary service providers for "mere conduit", caching and hosting.

The EU was a first mover on the legal front against spam by adopting a Directive on privacy and electronic communications⁵ that will lead to a pan-European 'ban on spam' to individuals.

The Recommendation on protection of minors and human dignity⁶ makes recommendations for Member States, the industry and parties concerned and the Commission and includes with the indicative guidelines on protection of minors. The implementation of the Recommendation was evaluated for the first time in 2000/2001. The report on the application of this Recommendation⁷ published in 2001 showed that the application of the Recommendation was already then overall quite satisfactory. The Commission is working on a second report on the implementation of the Recommendation, which will be adopted at the end of this year on the basis of a questionnaire, which was sent to both the Member States and the acceding States.

The proposed Framework Directive on child pornography⁸ sets out minimum requirements for Member States in the definition of offences and for sanctions.

1.3 What would happen under a “no further intervention scenario”?

It is possible to make predictions on the new media landscape and the problems likely to be seen in 2005 and beyond, based on current trends:

- New technologies and new ways of using existing technologies will be developed. These will provide new opportunities to the vast majority of law-abiding businesses and citizens;
- Use of new media by children will be an important part of their lives;

⁴ 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).

⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications (OJ L 201 31.7.2002, p. 37).

⁶ COM(2002) 263.

⁷ COM(2001)106 final

⁸ COM(2000) 854.

- However, criminals will use new media for carrying out their activities and will devise new ways of defrauding businesses and consumers.
- Alongside more structured professional structures of production and distribution familiar to traditional media, the distinctive feature of the Internet will remain the possibility for atomised production, reinforced by ways of ensuring secrecy and production of video-on-demand;
- At the same time, technology offers scope to devise new ways of preventing and detecting crime and identifying the criminals;
- The sexual exploitation of children will continue through production of child pornography and use of new technologies to contact possible victims of sexual abuse.

1.4 Who is affected?

a) The main target of the proposed programme is **children** and those responsible for them, their **families** and **teachers** in schools. Children are eager consumers of content distributed by Internet and new online technologies. They are frequent users of these technologies as a means of communication and contact. They are also potentially the most vulnerable since they are open to deception and exploitation.

b) **Governments** (national, regional and local) and 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, unwanted and harmful content.

As far as *illegal content* is concerned, the point of departure is that what is illegal offline is illegal online.

One concern is to ensure that the law, both substantive and procedural, is adapted so that it reflects the values of society and deals with new social phenomena. A second concern is that those charged with upholding the law should be given the necessary training and equipment. A further area of concern is the degree to which national law can be applied to activities taking place on a global network, whether under application of national rules of conflict of law or in practice. This is a particular difficulty if acts are punishable in one country and not punishable in another.

As far as *harmful content* is concerned, a balance must be struck between possible harm to minors and the preservation of the freedom of expression. Existing regulatory mechanisms must be adapted to meet the challenge of convergence of telecommunications, media and information technology.

c) **Industry** including content providers, Internet service providers and mobile network operators, as well as industry self-regulatory bodies, is also concerned, because industry has a strong interest from a business point of view in a safe environment engendering consumer confidence. Commercial content providers and technical intermediaries (including network operators and Internet Service Providers) need an environment in which to operate which allows them to go about their normal business without undue restrictions. They typically wish to avoid the costs and other burdens of regulation. In particular, they do not wish to have roles thrust upon them for which they are not best qualified and which are properly the role of other bodies representing the public interest. Industry can play an important role in helping to

provide solutions because of their expertise, their technical role in provision of services and their contacts with end-users.

d) **Non-governmental organisations** active in the fields of consumer protection, families, children's rights and child welfare are concerned by the potential harm to children caused by exposure to inappropriate content. Groups active against racism and xenophobia see the network as a means of distributing racist material and circumventing national laws. 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.

e) **Universities and research institutes:** can play an important part in a variety of areas, contributing to the knowledge of how children use new media and the best way to deliver the safety message. Research can also throw light onto the *modus operandi* of criminals using new media, investigate new technical solutions or provide an independent view of reconciling the interests involved in the self-regulation process.

2. WHAT IS THE MAIN OBJECTIVE THE PROGRAMME INTENDS TO ACHIEVE?

2.1 What is the overall policy goal?

The programme has the following overall aim:

- to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end user.

The programme focuses on the end-user – particularly children at home under the responsibility of their parents and in schools under the responsibility of their teachers.

The new programme will be inspired by the principles of *continuity* and *enhancement*:

- Continuity: continue doing what Europe does best by taking account of lessons learned and by building on the achievements of the initiatives already funded so as to ensure that their effects continue;
- Enhancement: meet new threats, ensure European added-value, stimulate a multiplier effect and broaden international outreach.

The programme has two aspects:

- a pronounced social dimension that focuses on domains where it would be wrong to rely either on regulation alone or on market forces to ensure the safety of users of Internet and new online technologies;
- an economic dimension by helping to create a climate of confidence and to promote the use of Internet and new online technologies and so to enhance the economic benefits that greater access to these technologies will bring to society.

2.2 Specific objectives

- Allow users to report illegal content. Expected results: hotlines in each Member State.

- Tackle unwanted and harmful content. Expected results: a) filtering technology: greater information of end users through benchmarking, increased effectiveness through benchmarking and funding development of filtering software and services b) content rating: adaptation of existing content rating systems to take account of the availability of the same content through different delivery mechanisms (convergence) c) facilitating and co-ordinating exchanges of information and best practices on effective enforcement against spam.
- Promote self-regulation. Expected results: a) development and deployment of European Codes of Conduct for industry (network operators, access providers, content providers and aggregators), pilot projects
- Increase awareness about safer use. Expected results: awareness actions designed to reach European children, European families with children and European schools, with multiplier actions in Member States.

2.3 Indicators

Sources of data for the indicators can be divided into two groups: programme level and project-level, corresponding to the ways in which data will be collected and matching the Commission's monitoring methods – in other words, leveraging and enhancing the existing mechanisms.

2.3.1. Programme level data sources

Three instruments are available to collect data.

The 2-yearly programme evaluation will be used to measure the direct or indirect impact of measures co-funded by the Safer Internet, as opposed to measures which might have occurred in the absence of any Community funding programme. Evaluations of the existing Safer Internet programme by external contractors have already been carried out in 2001 and 2003, and a third evaluation will take place in early 2005. The design and implementation of the evaluation is a task shared with DG INFSO's evaluation unit. The evaluation process is accompanied and supervised by a Steering Committee with outside experts on which DG BUDG is normally represented.

The Eurobarometer questionnaire is a significant innovation. There are 9 questions (see annex I), based on the experience of similar surveys carried out by Safer Internet projects. The survey covers a scientifically selected sample of between 1000 and 2000 people (check). The first is being launched at the end of 2003 in each of the 15 Member States. A corresponding study will be carried out in the 10 new Member States in 2004. This will therefore provide a set of baseline data. This survey will be repeated at regular intervals of between 12 and 24 months, budget permitting. It will allow society's attitudes towards Safer Internet to be monitored.

A third tool is the questionnaire about the Recommendation on protection of minors and human dignity, which gives feedback from the Member States on a significant number of questions directly relevant to Safer Internet (see annex II). There have now been two such questionnaires, in 2001⁹ and 2003¹⁰, and the results are collated and published by the

⁹ COM (2001) 106

Commission, so again a set of baseline data is already available. This questionnaire will be repeated every 2 years.

2.3.2. *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 is already including systematic reporting requirements for appropriate indicators as part of another significant innovation, the standard work packages and deliverables for network nodes in the application forms under the current call for proposals (see the example for awareness nodes in annex 3). These will become part of the technical annexes of contracts. Since new projects will start in mid-2004, the first data under this approach will start arriving at the end of 2004 and will be supplied through the life of the projects.

The “input” in terms of financial contributions is measurable through the documents submitted by the projects – the estimated budgets and the periodic cost statements. Contributions in kind are measurable in terms of input, even if not in money terms – and in some cases also in terms of results or impact, an example would be a television programme (number of viewers) or free banner space on a heavily-visited Web site (number of page views).

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

General objectives	Indicators
To promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end user	<ul style="list-style-type: none"> - Quantitative/qualitative data on actions, reports and other results of these actions - Quantitative/qualitative data on society’s perceptions as to the impact of the programme ;
Operational Objectives	Indicators
1. Allow users to report illegal content.	Quantitative/qualitative data on the establishment and operation of hotlines - n° of national nodes, MS coverage, n° of reports received, n° of staff involved in hotlines, - n° of police actions implemented thanks to hotline cooperation (feedback needed from police), n° of web pages withdrawn from ISP thanks to hotline tips
2 Tackling unwanted and harmful content.	a) Number of benchmarking reports, measured variation in effectiveness of filtering software and services, number and

¹⁰ COM() (not yet adopted)

	coverage of projects for filtering software and services b) number of content rating systems reviewed to take account of convergence, changes made c) reporting point or co-ordinated reporting points for spam.
3. Self-regulation	Code(s) of conduct: quality assessment, number of self-regulatory operations implemented.
4. Increase awareness about safer use	Extent of awareness-raising activities, data on level of awareness, no of national nodes, coverage, visibility (web sites hits etc)

3. WHAT IS THE INTERVENTION LOGIC PROPOSED?

3.1 What is the approach taken to reach the objective?

According to the *Safer Internet 1999- 2002* programme evaluation, there was a consensus among those consulted that relying on the regulatory framework alone was not enough to deal with the global nature of the problem.

Regulation has to be backed up by practical measures to assist those responsible for enforcing the law (action 1), to provide tools for users to protect themselves and the children for whom they are responsible against unwanted and harmful content (action 2), to encourage industry to find self-regulatory solutions (action 3), and to inform and educate parents, teachers and children about the problems and the best ways to deal with them (action 4).

The basic philosophy is that of empowerment of the user.

As explained above, the new programme will be inspired by the principles of *continuity* and *enhancement*. The new programme does therefore include elements of the Safer Internet Action Plan which have shown their worth and which were revised for the second phase 2003 – 2004. However, it also integrates a number of new elements to meet new threats, ensure European added-value, stimulate a multiplier effect and broaden international outreach.

A number of areas were suggested to the programme evaluators as possible additions. Among these, spam is an area where the Commission has decided to take a vigorous lead. The Commission is expected to publish a Communication on the subject which identifies a series of actions that are needed to complement the EU rules and thereby make the ‘ban on spam’ as effective as possible. Tackling spam will fall within the actions and the instruments chosen - there is for instance clear synergy and added value in including spam under filtering, supporting self-regulation pilot projects and awareness actions.

The opportunity has also been taken to suggest alternative or additional instruments under the accompanying measures. The budget request has been increased to take account of the increased scope and geographical coverage of the programme.

The programme aims to maximise its impact on the target audience by using networking and the multiplier effect.

The approach chosen builds on the results of Safer Internet 1999-2004, while bringing in additional elements that take account of new challenges. These elements add strength to the actions, which mutually reinforce each other, and keep their coherence without reducing the relevance to the target population.

This is the approach which has been translated into operational objectives covering well defined areas of action and instruments for the implementation set out in further detail in section 7.

3.2 Cost effectiveness

What is the cost of the proposed intervention?

The proposed intervention is estimated to cost 50 mio euro.

Do the objectives justify the cost ?

The two programme evaluations have confirmed that the current level of spending constitutes good value for money.

The budget of 50 mio euro would be significantly more than the cost of the current programme (at the rate of the draft 2004 budget for 25 Member States).

While 50 mio euro is a significant amount, it is not extravagant when bearing in mind the very broad geographical coverage (all 25 Member States) and reach (all Internet users and in particular parents, teachers and children). The use of Internet by children is one of the fastest-growing areas of Internet use overall. The age at which children first access the Internet is getting younger and younger.

Direct economic benefits from actions against spam can be expected for all Internet users - businesses, government bodies at all levels, educational organisations, non-profit organisations and individual. The Research Institute Ferris has estimated that in 2002, spam cost European companies 2.5 billion € just in terms of lost productivity.

The current spending level of 7.5 mio euro was based on a request made by the Commission which was at the low end of what was then needed. Certain costs in 2004 could only be met by stopping funding of development of filtering software and services and transferring the amount saved to other items.

The reasons for requesting a substantial increase in funding in 2005- 2008 are as follows:

- a) The increased scope of the programme to deal with the changes of technology and the way technology is being used, particularly the spectacular growth in their use by minors, the reinforcement of awareness activities and the foreseeable rise in the workload of hotlines due to the amount of illegal content in circulation and the number of reports made.
- b) The enlargement of the EU from 15 to 25. Adequate resources are required in order to allow national nodes to be set up in the 10 new Member States for the network of hotlines (Action 1) and the awareness network (Action 4), and for the additional needs of the two network co-ordinators created by a larger number of nodes to co-ordinate. The momentum should be kept.

- c) The programme will include not only Internet and other new technologies such as mobile phones, but also unsolicited commercial e-mail ("spam"). Including spam will involve additional expenditure under a number of actions. The most significant increase needed is for support to develop filtering technologies including spam and a possible reporting point for spam under Action 2: Tackling unwanted and harmful content. There will also be impacts on the self-regulatory activity and awareness-raising.
- d) It is further proposed to put resources into pilot projects for self-regulation, which could help generate more intensive activity in this area at European level.

3.3 Which alternatives have been considered?

Could the same results be achieved by a lower cost by using a different approach or other instruments, or could more or better results be achieved with the same cost by using a different approach or other instruments?

The approach chosen and the instruments suggested seem to be the most appropriate in order to achieve the overall objective and the ways in which intervention using funding from the Community budget can be used.

Three other options were considered:

- Cease, or drastically reduce, funding activities in the area of safer use of the Internet and new online technologies;
- Propose a further extension of the existing Safer Internet Action Plan with unchanged scope and actions.
- Merge the programme with another funding programme

The analysis carried out by the Commission shows that the problem of safer use of the Internet is still a real one and that action at Community level is effective. New platforms and the potential of new technologies have even increases the problem. It would therefore have been difficult to justify abandoning all activity in this area.

Although there are strong elements of continuity with Safer Internet 1999-2004 in the new programme, there is a need to propose further adaptations to take account of new realities and an approach which includes full involvement of acceding countries and strengthening international co-operation.

The Safer Internet programme has quite different "constituencies" and objectives to other funding programmes, as pointed out in the programme evaluations. Merger with other programmes would result in a loss of focus and visibility, and thus in effectiveness, without any particular cost advantages to counterbalance this.

3.4 Which are the trade-offs associated with the current proposal?

The main trade-offs are a consequence of the fact that the budget requested, although significantly larger than for the predecessor programme, is still modest compared to the magnitude of the issues and the need to cover 25 Member States.

One compromise which could **not** be made was on **the geographical spread** of the programme. This must not only cover 25 Member States, but also reach out internationally because of the global nature of the Internet and new technologies.

The first compromise was taken in the **scope of the programme**. A number of areas related to illegal content and conduct where action is required are not covered. In some cases, such as the area of network and information security, this is dealt with by other Commission initiatives. In other cases, in particular copyright, the main contribution of the European Union is to provide an appropriate legal framework in an ongoing process of harmonising the laws of the Member States where necessary. The programme concentrates on areas of illegal content and conduct where the need for public funding of countermeasures is greatest, and has given priority to protection of vulnerable persons, particularly children.

The second compromise is in **terms of reliance on networking and on the multiplier effect**. Action against illegal, harmful and unwanted content is necessary at all levels, internationally, at European Union level, nationally, regionally and locally and in each school and family, but the funds are insufficient for covering action at all these levels. Actions therefore aim to target specific projects which provide maximum European added value, and whose results can then be put into practice by multiplier organisations at national, regional and local level. Networks are the main instruments in the field of Action 1. Fighting against illegal content, and Action 4. Awareness-raising. This ensures a comprehensive European coverage and strong support in each country for the national node. This approach has the advantage of obtaining maximum value for money.

3.5 European Added Value – why act at Community level

Critics of the Safer Internet plus proposal might challenge the basis for action funded by the Community budget. On one hand, if the problem is global, would it not be better to act through organisations with a global scope? On the other hand, if safer use of the Internet and new media needs to be taught at the level of every child, then national, regional and local bodies are far better equipped to do so.

Each of these arguments are based on a correct premise, but the conclusion is at best an oversimplification - as is demonstrated by the fact that the two conclusions apparently contradict each other.

The correct conclusion is in fact that both global and national / regional / local actions are necessary but they are complementary to action at EU level, not alternatives.

International co-operation is also essential and can be stimulated, co-ordinated, relayed and implemented by action through the Community networking structures. There is already a variety of action in organisations with membership wider than the current 15 Member States, and the Commission is involved in these together with the Member States. (see table below). While their discussion cover a wide range of policy issues, none of these organisations currently fund actions similar to what is proposed, for the simple reason that those for whom it might be considered to be within their scope do not have budgets to do so. The INHOPE Association has members in the United States, Australia and South Korea.

Action at Member State level is essential involving a wide range of factors from national, regional and local government, network operators, parents, teacher 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 applied research. The need for hotlines to work together is evident since their role is to transmit reports which are likely to be in another country. The awareness nodes and pilot projects on self-regulation can help to produce a “multiplier effect” whereby the benefit of best practice can be distributed more widely than would otherwise be the case.

What measures are in place and what is already being done in the same field in the Member States?

A convenient source for a comparative overview of measures in place in the Member States, nationally, regionally and locally is the report on the application of the Recommendation on protection of minors and human dignity referred to in section 1.2 above, currently being updated. The picture is not a uniform one: there are more activities in some Member States than in others, in varying degrees of intensity.

What measures are in place and what is already being done in the same field within the Commission?

The actions of the Commission in related fields are covered in sections 1.2 and 2.2 above.

Will the intervention will be complementary to and coherent with action in Member States and with Commission activities?

As far as existing activities in Member States are concerned, it is quite clear that in a significant number of cases, there are activities which would not have happened at all without the intervention of the Safer Internet programme. In other cases, the activities would not have benefited from the exchange of best practice with other European countries. This was confirmed by the authorities in Member States who responded to the Commission’s surveys. See also section 3.6 below on subsidiarity.

The intervention will be complementary to and coherent with other Commission activities in the areas of policy and funding programmes. The services involved keep each other regularly informed and will continue to do.

To what extent can synergy effects be expected and, if so, what kind?

The design of the new programme aims at maximising synergy with national activities through networking. 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 intended to protect the consumer on the Internet, actions against spam, those relating to network and information security and those in the area of criminal law (child pornography).

3.6 How is subsidiarity and proportionality taken into account?

An additional advantage of the reliance on networking and on the multiplier effect mentioned above is that it complies with the principle of subsidiarity.

In some Member States, the programme will link in neatly with a variety of national programmes directly comparable to Safer Internet *plus* 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 might be among the typical ministries who need to be involved depending on how ministerial portfolios are distributed. In a federal state, the competences are likely to be split between national and regional levels.

The necessary co-operation between law-enforcement and industry may run counter to deeply-held views about their appropriate respective roles, the exact ways in which such co-operation could be implemented and any changes which would need to be made to the law as a consequence. There may not even be a single body to speak for the industry.

Safer Internet *plus* and its various actions will certainly give the necessary additional impetus to setting up new forms of co-operation. The financial incentive offered by Community co-funding should not be the main driving force, but it will help to overcome any reluctance to co-operate because of the costs involved.

Relationships of Safer Internet with other EU programmes

AGIS	The AGIS Framework programme on police and judicial co-operation in criminal matters runs for the period 2003 to 2007 with a budget of EUR 65 million. Preceding programmes included STOP and STOP II. In 2000 the STOP programme co-funded an International conference on fighting child pornography on the Internet that following up the conference «Combating Child Pornography on the Internet» held in Vienna in 1999. The programme also funded the COPINE project and a follow-on which analysed the behaviour of offenders collecting child pornography and the setting-up of an operational database of child pornography using automatic indexing and search systems.
DAPHNE	The Daphne Programme for the years 2000-2003 is a European Community preventive action programme to fight violence against children, young people and women. Violence is understood in the widest possible sense, from sexual abuse to domestic violence, from commercial exploitation to bullying in schools, from trafficking to discrimination-based violence against handicapped, minority, migrant or other vulnerable people. DAPHNE has funded several related projects, some of which (e.g. INHOPE) have subsequently been funded under the Safer Internet Action Plan and a project on identifying victims of child pornography.
ECCONTENT	The eContent programme, as part of the eEurope Action Plan, contributes to its third objective: "stimulate the use of internet" The eContent programme is aimed at supporting the production, dissemination and use of European digital content and to promote linguistic diversity on the global networks. The eContent programme is based on three main strands of action where EU added value can be maximised: Improving access to and expanding use of public sector information, Enhancing content production in a multilingual and multicultural environment, Increasing dynamism of the digital content market
INFORMATION SOCIETY TECHNOLOGIES PROGRAMME (IST)	Information access, filtering, analysis and handling (IAF): The overall objective of IAF is to develop advanced tools and techniques for the management of multimedia content to empower the user. IAF further focuses on audio-visual content which today is streamed over the Web, CD or DVD, but which will also be available in the next years over interactive TV, multimedia home platforms and wireless multimedia networks.
ELEARNING	The Commission has adopted the "eLearning" initiative to adapt the EU's education and training systems to the knowledge economy and digital culture. This initiative has four components: to equip schools with multimedia computers, to train European teachers in digital technologies, to develop European educational services and software and to speed up the networking of schools and teachers. Schools are one area in which awareness of illegal and harmful content and means of dealing with it are important. The network set up in the context of "Learning in the Information Society" will provide a channel for disseminating the content created for the Action Plan on promoting safer use of the Internet. Internet safety issues were discussed as part of the 2001 eSchola event organised by the European School Net.

Relationships of Safer Internet with EU policy initiatives

Recommendation on Protection of Minors and Human Dignity	The Recommendation offers guidelines for the development of national self-regulation regarding the protection of minors and human dignity. Self-regulation is based on three key elements: first, the involvement of all the interested parties (Government, industry, service and access providers, user associations) in the production of codes of conduct; secondly, the implementation of codes of conduct by the industry; thirdly, the evaluation of measures taken.
Communication on Computer Crime	The Commission has adopted a Communication Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime COM(2000) 890 which discusses the need for and possible forms of a comprehensive policy initiative in the context of the broader Information Society and Freedom, Security and Justice objectives for improving the security of information infrastructures and combating cyber-crime, in accordance with the commitment of the European Union to respect fundamental human rights. This announced a number of legislative and non-legislative initiatives..
Framework Decision on child pornography	Following the Decision on child pornography on the Internet, a measure under the EU "third pillar" (co-operation in justice and home affairs) which invites Member States to take a number of steps to increase the effectiveness of law-enforcement against child pornography on the Internet and to encourage collaboration between law-enforcement authorities of the Member States, the Commission has proposed which defines constituent elements of criminal law, common to all Member States, including effective, proportionate and dissuasive sanctions.
Communication on Network and Information Security	This proposes a European policy approach aimed at improving network and information security. It is based on an analysis of the need to supplement market solutions with policy actions. It lists a series of concrete policy measures, as was requested by the Stockholm European Council. The proposed policy should be seen as an integral element of the existing framework for electronic communication services and data protection and – more recently – cyber-crime policy
Transparency Directive	Directive 98/48 provides for notification by Member States of new measures relating to information society services and a mechanism for dealing with possible objections by the Commission or other Member States.
Electronic Commerce Directive	Directive 2000/31/EC covers a number of legal issues of electronic commerce including establishment, commercial communications and electronic contracts. In particular, it contains provisions relating to the liability of intermediaries (network operators, service providers) for third-party content and encourages adoption of codes of conduct.

Relationships of Safer Internet with other policy initiatives

WSIS	
World Simm Geneva 2003, Tunis 2005	Commission official delegation.
OSCE	
Organisationon Secutri i Europe	Has organised and racism . Commission speakers and official delegations.
COUNCIL OF EUROPE	

Convention on cyber-crime	The Convention aims to facilitate the detection, investigation and prosecution of cyber-crime at both the domestic and international level, and to provide arrangements for fast and reliable international co-operation. It is open for signature by countries which are not members of the Council of Europe. The European Commission took an active part, as are the US, Canada and Japan. The Convention covers both substantive law (offences against the confidentiality, integrity and availability of computer data and systems and computer-related offences, and also child pornography) and procedural law (preservation, search and seizure and real-time collection of computer data and international co-operation including extradition and mutual assistance and a point of contact available on a 24 hour, 7 day per week basis). The Additional Protocol to the Convention on cyber-crime deals with racist and xenophobic content.
Declaration on freedom of communication on the Internet	The Council has adopted a Declaration on freedom of communication on the Internet and a Recommendation on self-regulation which are clearly influenced by the EU's approach. A handbook on awareness-raising is currently being prepared with the co-operation of the Safer Internet programme.
G8	
"Lyon Group"	10-point Action Plan, Washington Dec 1997. Institutes 24-hour contact points (subsequently extended to all MS)
ICANN	
	Californian not-for-profit corporation with responsibility for Internet name space. Commission member of the Governmental Advisory Committee and currently hosts GAC secretariat.
UNESCO	
Child pornography and paedophilia on the Internet	Innocence in Danger network set up following UNESCO conference in Paris on 18-19 January 1999 on child pornography and paedophilia, at which the Commission was represented, and an Action Plan was proposed for follow-up by members of UNESCO.
INTERPOL	
	Contact between INHOPE Association and INTERPOL. Child victims' database with EU funding
EUROPOL	
	Contact between INHOPE Association and EUROPOL .Safer Internet Police-hotlines Workshop with EUROPOL participation.

4. THE EXPECTED IMPACTS

4.1 What are the expected impacts in terms of economic and social consequences?

The social impacts of the programme are considerable:

- the reporting mechanisms (hotlines) and information about tools to deal with unwanted or harmful content will be available to all European Internet users
- self-regulatory Codes and spam co-ordination will also benefit all European Internet users

Other benefits include:

- creating a climate of confidence which will promote the use of Internet and new online technologies and so enhance the economic benefits that greater access to these technologies will bring to society

- European networking will help actors save money by the re-use of available knowledge, skills and content.

The economic benefits of the programme are demonstrated by the support given by industry to the activities of the Safer Internet Action Plan. For instance, the business model of the new mobile industry largely relies on the ability to sell “adult material” to paying adult customers, but they know that they need 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 with measures which empower parents to protect minors against harmful content.

It is difficult to give any figures on “return on investment” since the areas covered by Safer Internet *plus* and the instruments chosen tend to be those which do not have a direct economic return. This is the result of a deliberate choice of directing funding to areas of illegal and harmful content where those most directly affected (families) are not able to organise themselves and fund counter-measures out of their own resources. Often those best able to take necessary steps are non-governmental organisations with limited resources. Their low overheads and ability to call other organisations for support help them to provide high impact for a relatively small Community contribution.

4.2 How large is the additionality effect that can be attributed to the proposal, i.e. those effects over and above a “no intervention” scenario.

The additionality effect can be examined in two ways:

- effects which would not happen at all if there were no intervention (pure additionality)
- effects which would happen but to a lesser degree, less rapidly, less effectively or with a more restricted geographical distribution (partial additionality)

The evaluation of the Safer Internet Action Plan 1999 – 2002 gives some useful indications about this and allows a prediction to be made of the degree of additionality to be expected of the new programme. In terms of pure additionality, 57% of all organisations indicated they would not have become involved in projects in the absence of EU funding. It is, for instance, likely that without intervention a smaller number of national hotlines would have been set up without any linkage between them and that the European network of hotlines and a number of national hotlines would not have been set up.

However, partial additionality is relatively high. 41% would still have gone ahead without EU funding, but would have undertaken their projects with reduced objectives and finances, with fewer partners and over longer time-scales. Almost 9% of the organisations which would have gone ahead with their project, commented that they would have done so without international collaboration.

This indicates that, although some progress would have certainly been achieved without the programme, the networking effect and the pan-European coverage would not have been achieved. The networking effect and the pan-European coverage are necessary to achieve the desired result.

The Commission has acted as a pioneer in this area and has set orientations which the Member States have followed.

4.3 Are there especially severe impacts expected on a specific social group, economic sector (including size-class of enterprises) or region?

No negative impacts are expected on any group (other than producers and distributors of child pornography and other illegal content).

The beneficial impacts will be wide-spread, concentrated on Internet users particularly on families with children and use of the Internet by children in schools. The Northern European have traditionally had high levels of Internet use in the home and schools, above the rate of the United States in the case of Sweden for example. Now, Southern Europe is catching up fast – Italy and Spain being particularly striking examples. The new Member States are likely to see the same phenomenon during the lifetime of the programme.

4.4 What is the impact outside the Union on the Candidate Countries and/or third countries?

Candidate countries and the new Member States (accession countries) will be integrated into the Safer Internet Action Plan during the period covered by the Work Programme 2003 – 2004, and the new programme will allow this extension of scope of safer Internet activities to continue to produce effects.

Third countries will also be involved in activities. One important proposed innovation for 2005 - 2008 is to allow co-funding of projects in third countries in appropriate cases subject to the approval of the Programme Committee.

4.5 What are the impacts over time?

The programme will be implemented via calls for proposals leading to the financing of pilot projects and best practice actions, networks, applied Europe-wide research and accompanying measures.

Experience has shown that projects need more time to take account of start-up at the beginning and the need to disseminate results at the end of the contract period, and of factors specific to European projects such as the additional time needed to ensure cross-border co-ordination.

The hotline and awareness nodes would benefit in particular from the additional stability that a longer contract would bring. Typical duration of projects will therefore be in the order of 30 – 48 months.

The impacts will be concrete and highly visible over the lifetime of the projects. They consist of:

- continuing and increasing availability of complaints mechanisms for illegal content on the Internet;
- availability of new tools and new information resources relating to safer use of the Internet;
- large-scale rollout of awareness-raising campaigns throughout the enlarged European Union and candidate countries;
- creation of new partnerships at international, European, national, regional and local level.

Long-term effects include:

- exchange of expertise and training in the area (including knowledge about use of Internet by criminals particularly for sexual exploitation of minors, technological solutions, children's use of new media, promotion of media literacy through training the trainers);
- increase of organisational and networking capacity of the participants.

5. MONITORING AND EVALUATION

5.1 How will the programme be implemented?

The programme will be executed through indirect actions – calls for proposals and calls for tender as appropriate – comprising:

- 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 bringing together a variety of stakeholders to ensure action throughout the European Union and to facilitate co-ordination activities and transfer of knowledge. They may be linked to best practice actions.
 - Applied Europe-wide research carried out on a comparable basis into the way people, especially children, use new media.
- accompanying measures
 - Accompanying measures will contribute to the implementation of the programme or the preparation of future activities. Measures devoted to the commercialisation of products, processes or services, marketing activities and sales promotion are excluded.
 - benchmarking and opinion surveys to produce reliable data on safer use of the Internet and new online technologies for all Member States collected through a comparable methodology;
 - 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, including self-regulation and the work of the Safer Internet Forum, and the preparation of future activities;
 - awards for best practice;
 - exchange of information, conferences, seminars, workshops or other meetings and the management of clustered activities;
 - dissemination, information and communication activities.

	Effectiveness	Cost	Risks	Administrative overheads
Pilot projects, Best practice actions	High	Medium to High	Medium to High	High
Networks	High	Medium*	Low	Medium
Applied research	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 network are low, but there are 25 of them, plus a co-ordinator

A conclusion of this analysis is that particular attention should be given to networking in order to benefit from a leveraging effect. Applied research (e.g. children's use of new media), accompanying measures and meetings organised by the Commission all give worthwhile results for the cost and efforts involved. Some areas by their nature (such as development of filtering technology) can only be covered by pilot projects and best practice actions despite the higher cost, higher risk and higher administrative overhead involved.

5.2 How will the programme be monitored?

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

a) on regular two-yearly programme evaluation by external contractors

b) on the information obtained directly from beneficiaries, who will submit interim and final activity and financial reports, including performance indicator criteria set out in the selection process. All projects and actions will include built-in evaluation, or provision for assessment by external experts or internal sources, and contain performance indicators and guidelines for follow-up.

A detailed set of indicators at programme and project level will be used - see point above 2.3 above.

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.

5.3 What arrangements are made for an ex-post assessment of the results?

An interim evaluation will be carried out on the second year of the programme. This evaluation will assess the programme effectiveness and efficiency, review its implementation logic and – if applicable – to 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. Indicators of success will be defined as part of the competitive procedures designed to award contracts to carry out this task.

Both the interim and the final evaluation will be carried out by independent firms specialising in evaluations, following tendering procedures in line with Commission standard practices.

6. STAKEHOLDERS' CONSULTATIONS

6.1 Which stakeholders were consulted, when in the process and for what purpose?

A number of consultations were held with stakeholders¹¹ that informed the process leading to the present Commission proposal.

The process started with the definition of the Work Programme 2003 – 2004. This implements the second phase of the Safer Internet and has a number of innovative features which are precursors of the new proposal.

The adoption by the Commission of the Work Programme on 3 September 2003 was preceded by a lengthy and thorough preparation phase. A hearing¹² took place in Luxembourg on 27 and 28 November 2002 attended by 100 people¹³ representing Internet service providers, content companies, Member States, and acceding countries, non-governmental organisations candidate, public sector organisations, and participants in hotline, filtering and awareness projects. A background document was distributed and made available online¹⁴. Presentations at the hearing were made by Commission officials and outside speakers and a lively discussion took place in workshops¹⁵. An online consultation took place closing on 7 January 2003. 11 contributions were received¹⁶.

In the context of the review of the Television without Frontiers Directive and the Recommendation on protection of minors and human dignity, a consultation was organised by the Education and Culture DG covering a total of 6 themes, of which protection of minors and public order and the right of reply was one. Background papers were published¹⁷. A hearing on the theme of protection of minors was held in Brussels on 24 June 2004 which was attended by 200 participants. 142 online contributions on this and the other themes covered by the consultation questions were received by the closing date of 15 July 2003.

A final public consultation took place in Luxembourg on Friday 12 September 2003 and it was attended by 150 participants representing a broad range of actors involved in the area of Internet safety. The possibility was also given to make online contributions by Monday 15 September 2003. A summary of the meeting results and a collection of written submissions from interested parties is available on the Europa Web site¹⁸.

¹¹ Stakeholders are defined in the

¹² http://www.saferinternet.org/resources/esafe_present.asp

¹³ <http://www.saferinternet.org/downloads/eSafe%20Hearing%20-%20Registered%20Participants.pdf>

¹⁴ <http://www.saferinternet.org/downloads/eSafe-Directions-2003-2004.pdf>

¹⁵ <http://www.saferinternet.org/resources/working-groups.asp>

¹⁶ <http://www.saferinternet.org/resources/eSafe-publictable.asp>

¹⁷ http://europa.eu.int/comm/avpolicy/regul/review-twf2003/twf2003-theme4_en.pdf

¹⁸ http://europa.eu.int/information_society/programmes/iap/info_day/pub_const_home/index_en.htm

The consultation covered the following points:

- Scope of a follow-up programme (e.g. action against "spam")
- Roles and contributions of the different actors
- Subsidiarity, respective roles of action at European level and at national, regional and local levels, need for international co-operation
- Amount of Community funding for different actions
- Instruments to be used

A survey of stakeholders was carried out in conjunction with the programme evaluation. This was in two parts. Participants in the Safer Internet Action Plan were contacted and asked to fill out a questionnaire. In total, 138 questionnaires were despatched to successful applicants. This corresponds to the total number of participants in projects with whom contracts were concluded in the first phase. Responses were received covering all but one of the projects (many organisations participating in more than one project). In addition, a series of 35 telephone and face-to-face interviews were held with participants and with stakeholders who were not participants in projects and who had been identified by the evaluators on the basis of information supplied and their own research. The results of this process are contained in the evaluation report, quoted in several instances in this working paper.

Meetings have been held on specific aspects such as a police-hotlines workshop (Brussels 9 October 2002, 80 participants), quality labels¹⁹ (Luxembourg 27 Feb 2003 , attended by 95 participants) and racism (workshop²⁰ in Brussels in September 2002 with 40 experts). Project meetings have touched hundreds of stakeholders in all Member States.

Member States were also consulted. The programme committee that includes representatives from Member States and (at its most recent meeting) acceding countries discussed the background document at its meeting of November 2002 and discussed both the draft Work Programme and the draft programme evaluation report at its meeting of 16 May 2003.

The Commission has moreover kept constantly in touch with the views of interested parties through the 37 shared-cost projects and the 136 organisations taking part in them, through the Awareness Exchange²¹ and Selfregulation.info projects²² funded by the Commission, by attending meetings organised by international organisations and by the stakeholders in Member States, and by its own ongoing review of events and developments in Europe and world-wide.

6.2 What were the results of the consultation?

The consultation process resulted in three main outputs:

¹⁹ <http://www.saferinternet.org/news/Quality-label-workshop.asp>

²⁰ <http://www.selfregulation.info/iapcoda/rxio-background-020923.htm>,

<http://www.selfregulation.info/iapcoda/rxio-rapporteur-020923.htm>

²¹ <http://www.saferinternet.org/> which distributes a monthly newsletter in English, French and German to 2500 subscribers

²² <http://www.selfregulation.info>

- Confirmation of the relevance of the action and the need for continued support at European Union level. There was agreement that the problem of safer use of the Internet continued to be a real concern and the problem was aggravated by the new technologies and new ways of using such technologies which were emerging. Different types of actions were required at different levels, local, regional, at European level and internationally - awareness actions in particular had to be carried at the level of end users, parents and children, using a multiplier effect. In all cases, action by the European Union could ensure European added value. Stakeholders particularly emphasised the need for international co-operation.
- Agreement on the extended scope of the programme actions; in particular the coverage of unsolicited commercial e-mail (spam). Some stakeholders suggested other areas for reinforced action, including exploitation of children for commercial purposes, network and information and data protection. It was also emphasised that inclusion of new areas should not be at the expense of the existing coverage which continued to be important.
- Generally held view that a higher level of funding was needed in order to cover both existing and new areas adequately. In particular, concern was expressed that it would not be possible to fund the hotlines and awareness networks to cover both the existing 15 EU Member States and the 10 new Member States on the basis of the funding available for 2003-2004, if complete coverage was to be achieved.

7. COMMISSION DRAFT PROPOSAL

7.1 What is the final choice and why?

The final choice, as already referred to in section 2, is inspired by the principles of *continuity* and *enhancement*:

- Continuity: continue doing what Europe does best by taking account of lessons learned and by building on the achievements of the initiatives already funded so as to ensure that their effects continue;
- Enhancement: meet new threats, ensure European added-value, stimulate a multiplier effect and broaden international outreach.

There will be four Actions: fighting against illegal content, tackling unwanted and harmful content, promoting a safer environment and awareness-raising. In each case, international co-operation would be an integral part of the action.

7.1.1. Fighting against illegal content

It is proposed to continue funding for network co-ordination and for individual hotlines. In this context, ways need to be explored in which industry can contribute with its technical expertise to the fight against illegal content. The network should be extended to cover the new Member States and candidate countries, and other European countries where illegal content is hosted and produced.

Such hotlines should liaise closely with other actions, such as self-regulation or awareness-raising and could be run by organisations which are involved in such actions.

The hotline network should ensure coverage and exchange of reports of the major types of illegal content of concern - extending beyond the area of child pornography. Different mechanisms and different expertise may be required to deal with other areas such as racist content.

7.1.2. Tackling unwanted and harmful content

The programme will provide funding for technological measures which empower users to limit the amount of unwanted and harmful content which they receive, such as assessing the effectiveness of available filtering technology and supporting the development of filtering technology.

Other initiatives to deal with unwanted and harmful content will include further work on content rating to take account of the availability of the same content through different delivery mechanisms (convergence) and funding for measures to facilitate and co-ordinate exchanges of information and best practices on effective enforcement against spam.

Implementation of this action will be closely co-ordinated with the actions on promoting a safer environment (self-regulatory action) and awareness-raising (informing the public about means of dealing with unwanted and harmful content).

7.1.3. Promoting a safer environment

The European Union has emphasised its support for a self-regulatory approach offering flexibility and understanding of the needs of the medium in an area combining high technology, rapid change and cross-border activity. Different models of Codes of Conduct are possible, but they should share essential features such as effectiveness, fairness and transparency.

There is still work to be done in this area both in developing working self-regulatory approaches at national level and in setting up a platform at European level for those working in this area.

Self-regulation does not necessarily come about by itself, nor does it exclude the need for some form of legal underpinning: a more pro-active approach may be required in order to stimulate agreement on an appropriate set of rules and their implementation.

The Safer Internet Forum has been set up under the second phase (2003-2004) of the existing Safer Internet Programme as a unique discussion forum including representatives of industry, child and welfare organisations and policy makers, and will provide a platform for national co-regulatory or self-regulatory bodies to exchange experience. It will be also give the opportunity to discuss ways in which industry can contribute to the fight against illegal content. Pilot projects will be funded for examples of self-regulatory initiatives.

7.1.4. Awareness-raising

There is overwhelming agreement among policy-makers and specialists of the continuing need for systematic information about safer Internet use, particularly for personalised, interactive and mobile applications, linked with other EU actions on media education and Internet literacy.

So as to make best use of funds available, the Commission should concentrate on pump-priming, encouraging the multiplier effect and exchange of best practices through a network.

7.1.5. Changes compared to predecessor programme

The actions are influenced by the structure of the predecessor programme (continuity), but a number of changes have been made (enhancement).

The main enhancements relate to scope. Activities are divided into four main actions as compared to three action lines in 1999 - 2004. A separate action has been created for self-regulation - Action 3 Promoting a safer environment.

Quality labels (formerly part of self-regulation) are grouped with content rating and filtering, under Action 2 Tackling unwanted and harmful content.

New elements include the possibility of funding development of filtering software and services, since this is a clear candidate as a technical means of combatting spam and there is clear synergy here with filtering for protection of minors. The possibility is opened of funding third-country partners - the intention being to stimulate actions in countries where illegal content is hosted or produced.

The relative balance of the action lines has been re-evaluated as a result of the creation of a fourth action. The largest amount (40 - 45 %) goes to awareness-raising under Action 4, which is very resource-intensive. The amounts for awareness and hotlines under Action 1 (18 - 23 %) take account of the need to fund European-wide networks. Self-regulation (Action 3) requires human resources but a lower degree of financing (8 - 10%), since it is intended to finance ad-hoc projects rather than the operations of self-regulatory bodies. The amount for Action 2 (20 - 25%) leaves scope for significant funding for funding development of filtering software and services.

7.2 Why a more/less ambitious option not chosen?

The size and scope of the proposed action is commensurate with the perceived needs and mobilises the necessary human resources and the expertise available in order to implement it.

7.3 What are the trade-offs associated with the chosen option?

See section 3.3.

7.4 In case of insufficient knowledge, why is a decision taken now?

Not applicable.

7.5 Have any accompanying measures to maximise positive and minimise negative impacts been taken?

The relation between financing actions and the legislative background underpinning the action is explained in the preceding paragraphs.

8. LESSONS FROM THE PAST

The Safer Internet Action Plan covered the period 1999 – 2004.²³

The objective of the programme, as specified in the European Parliament and Council Decision²⁴, was promoting safer use of the Internet and encouraging, at European level, an environment favourable to the development of the Internet industry.

The programme covered the four-year period from January 1999 to December 2002 with a reference budget of 25 million euro. The programme was implemented through three main action lines:

- creating a safer environment (creating a European network of hot-lines and encouraging self-regulation and codes of conduct);
- developing filtering and rating systems;
- encouraging awareness actions.

During the years 1999 – 2002, 37 projects were co-financed, involving over 130 different organisations. Two service contracts were concluded for advice to self-regulatory bodies and for exchange of information about best practices²⁵.

The Decision was amended by Decision No. 1151/2003/EC of the European Parliament and of the Council of 16 June 2003²⁶ extending the duration of the programme until 31 December 2004, increasing the indicative budget by 13.3 million euro and making a number of changes to the title and scope of the programme and to its implementing actions.

Safer Internet Action Plan is a major element in the Commission's activity in the field. The programme has set up a European network of hotlines, encouraged self-regulation and codes of conduct, supported development of filtering and rating systems and stimulated awareness actions.

As demonstrated by the programme evaluation 1999 - 2002 carried out by independent consultants which gave a positive assessment of the achievements of the current Safer Internet programme²⁷, the programme has made a significant contribution during the first 4 years but the complexity of the issues and the multiplicity of the actors involved means that there is still a need for further action.

²³ Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors (OJ L 33, 6.2.1999, p.1) as amended by Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 (OJ L 162, 1.7.2003, p. 1).

²⁴ Decision no 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (OJ L 33, 6.2.1999, p.1).

²⁵ see the www.selfregulation.info and www.saferinternet.org Web sites.

²⁶ OJ L 162, 1.7.2003, p. 1.

²⁷ COM(2003) xx. currently in inter-service consultation (INFSO 740929).

The evaluators recognised the positive impact of the current programme, particularly in fostering networking and providing a wealth of information about the problems of safer use of the Internet and their solutions.

More specifically it was concluded that:

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.

At the policy level, the programme has **been successful in putting the issues of developing a safer Internet firmly on the agenda** of the EU and the Member States. The **foresight of the European Commission in identifying these issues early on in the development of the Internet should be recognised**.

The evaluators made a number of detailed recommendations with regard to the action lines and how they should be implemented:

- Extend emphasis/objectives to encompass new and emerging communication technologies that will in particular influence children's use of the Internet (e.g. 3G mobile telephones).
- Review the Action Line on filtering and rating.
- Continue to move towards networks of nodes for awareness-raising in the Member States.
- Continue to engage with actors external to the European Union
- Encourage wider involvement of ISPs and other relevant industry players
- Focus programme where it is likely to have the most impact which is at the European/International level through networking and multipliers

The Commission had already anticipated many of these findings in its proposals for an extension of the Safer Internet Action Plan will implement them as part of the Work Programme 2003-2004. The design of Safer Internet *plus* takes full account of these findings.

EUROBAROMETER QUESTIONNAIRE

- Q.1. a) Do you have, in your household, any child under your responsibility in each of the following age bans? (SHOW CARD - MULTIPLE ANSWERS POSSIBLE)
- b) (INT.: ASK FOR THE CHILD WHO'S BIRTHDAY IS CLOSEST TO DATE OF INTERVIEW)
And is it a boy or a girl?

	READ OUT	Q.1.a.	Q.1.b.	
			GIRL	BOY
1	Under 6	1	1	2
2	6 - 7 years old	2	1	2
3	8 - 9 years old	3	1	2
4	10 - 11 years old	4	1	2
5	12 - 13 years old	5	1	2
6	14 - 15 years old	6	1	2
7	16 - 17 years old	7	1	2
8	I do not have any child under 18	8		

IF CODE 1 TO 7 IN Q.1.a., OTHERS GO TO Q.9.

- Q.2. Does he/she use the Internet in any of the following places?
(SHOW CARD - READ OUT - MULTIPLE ANSWERS POSSIBLE)

At home.....	1,
At school	2,
At a friend's home	3,
In someone else's home.....	4,
In an Internet cafe	5,
In a library/other public place	6,
Somewhere else.....	7,
He/she does not use the Internet	8,
DK.....	9,

IF "USE THE INTERNET", CODE 1 TO 7 IN Q.2., OTHERS GO TO Q.7.

- Q.3. Have you set any rules for him/her about using any of the following either in your household or elsewhere? (SHOW CARD - READ OUT - MULTIPLE ANSWERS POSSIBLE)

Yes, for the television.....	1,
Yes, for the mobile, cell phone (INT.: USE APPROPRIATE NAMES IN EACH COUNTRY).....	2,
Yes, for electronic games consoles such as Playstation, Xbox, GameCube, Gameboy, etc.....	3,
Yes, for the Internet	4,

Yes, for the computer (apart from the Internet).....	5,
Yes, they are rules, but not set by me.....	6,
No, no rules have been set.....	7,
DK.....	8,

IF CODE 4 IN Q.3., OTHERS GO TO Q.5.

Q.4. What rules have you set regarding how he/she uses the Internet?
(DO NOT READ OUT - MULTIPLE ANSWERS POSSIBLE)

He/she is not allowed to give out any personal information	1,
There are some sites that he/she is not allowed to visit.....	2,
He/she is to tell me/us if they find something on the Internet that makes him/her feel uncomfortable	3,
He/she is not allowed to use rude language in e-mails or chat-rooms.....	4,
He/she is not allowed to meet in person someone he/she only met on the Internet	5,
He/she is not allowed to copy documents/pictures	6,
He/she is not allowed to go to chat-rooms/to talk to strangers in chat-rooms	7,
He/she is not allowed to download music or films.....	8,
He/she is not allowed to download software	9,
Rules regarding how much time he/she is allowed to spend on the Internet	10,
Keeping phone lines free at certain times of the day	11,
Ensuring that access to the Internet is shared fairly between family members.....	12,
Other rules	13,
DK.....	14,

Q.5. Do you feel that you need more information or not about how to protect the children from your household from illegal or harmful content and contact on the Internet?

Yes.....	1
No	2
DK.....	3

Q.6. Would you say that the children in your household know what to do if a situation on the Internet makes them feel uncomfortable?

Yes.....	1
No	2
DK.....	3

IF CODE 1 TO 7 IN Q.1.a., OTHERS GO TO Q.9.

Q.7. From whom would you like to receive information about using the Internet in a safer way? (DO NOT READ OUT - MULTIPLE ANSWERS POSSIBLE)

School(s).....	1,
Parents association (IRL: parents/teacher association)/other parents groups	2,
Government/local authority	3,

The Internet service provider or the telephone company	4,
Software companies	5,
Computer retailer	6,
Your employer.....	7,
Associations, non-profit organisations / non governmental organisations (NGOs)	8,
TV, radio, newspapers	9,
Police	10,
Other source	11,
I don't want to receive such information.....	12,
DK.....	13,

IF CODE 1 TO 10 IN Q.7., OTHERS GO TO Q.9.

Q.8. How would like to receive this information?
(DO NOT READ OUT - MULTIPLE ANSWERS POSSIBLE)

By letter.....	1,
By e-mail.....	2,
From a website	3,
By SMS/text message.....	4,
By telephone (other than text message)	5,
In newspapers	6,
In computer magazines.....	7,
From TV	8,
From the radio.....	9,
In a library	10,
From a CD Rom.....	11,
From another medium.....	12,
DK.....	13,

ASK ALL

Q.9. Do you know where or to whom you can report illegal or harmful content on the Internet?
(DO NOT READ OUT - MULTIPLE ANSWERS POSSIBLE)

Yes, hotlines	1,
Yes, the police	2,
Yes, the Internet service provider	3,
Yes, school(s).....	4,
Yes, parents association.....	5,
Yes, associations, non-profit organisations, non governmental organisations (NGOs)	6,
Others.....	7,
No, I do not know where I can report illegal or harmful content on the Internet	8,
DK.....	9,

Questionnaire

Concerning the Recommendation of the Council of 24 September 1998 on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC)

Internet

1. Has an association of Internet Service Providers (ISPs) been established in your country? Please give details of the ISP association(s).
2. Has a code of conduct been drawn up by the ISPs in your country? If possible, please provide a copy or the web address where it can be accessed.
3. To what extent were public authorities and consumers involved in the drawing up of the ISP code of conduct? Is consultation of public authorities and consumers required when the code is revised or amended?
4. Are there any legal requirements in your country which apply **specifically** to ISPs and how they should deal with illegal or harmful content accessed over the Internet? If so, what are they?
5. Are there any specific requirements for ISPs to inform the police or judicial authorities about illegal content offensive to human dignity, which is available over the Internet?
6. Has a “hotline” for reporting harmful or illegal content been established in your country? If so, please give details (including web and e-mail address) of the hotline(s), including their method of financing.
7. Of the problematic Internet content which has been reported, approximately what proportion of this is hosted outside your country or outside the EU?
8. What measures and initiatives have been taken, either by public authorities or by operators, to raise public awareness of hotlines? Are these measures and initiatives judged to have been effective?
9. Where hotlines have been established, please give, in so far as possible, an estimation of their effectiveness in reducing the extent and accessibility of harmful and illegal content. This could include public opinion as to their effectiveness/efficiency as well as the views of operators.
10. Apart from any involvement in the work currently funded by the Community Action Plan on promoting safer use of the Internet, have any efforts been made, either by industry or public authorities, to develop a filtering and rating system for the Internet in your country? If so, what progress has been made and what are the difficulties encountered?
11. Do any obligations exist, either in law or in relevant codes of conduct, for ISPs to inform subscribers about available filtering and rating systems and age verification software?

12. What measures have been taken at national, local or regional level to spread awareness of safer Internet issues? Have these been part of a larger plan for “media education”? Have they been supported by public funds or by private funding (e.g. from industry or from voluntary associations) or by a mixture of public and private funding?

13. Is there any indication that the development of the Internet in your country has been slowed down by public fears concerning harmful and illegal content which may be accessed over the Internet?

14. Is the current level of international co-operation in this matter, particularly within Europe, seen as sufficient? If not, what measures could be taken to improve it?

15. Have you already covered or do you intend to cover by the above mentioned self-regulation measures or by regulation similar services such as transmission via mobiles, in particular as concerns UMTS?

16. Please describe any initiatives, which have been taken to control online chat-groups, in particular measures taken in order to avoid any abuse, which could be harmful to minors?

17. Please describe measures, which have been taken in order to improve media-literacy (e.g. teaching children how to make a responsible use of new media)?

18. Is there any specific regulation or self-regulation concerning the specific question of the right of reply with respect to online-media? Have there been concrete problems during the last two years concerning these issues, in particular problems involving cross-border aspects?

Broadcasting

19. Have broadcasters in your country established a system of self-regulation relating to the protection of minors? Please give details of this, particularly with regard to membership.

20. Does this system of self-regulation include a code of conduct regarding the protection of minors and harmful content? (Please note, this question does not concern only advertising specifically aimed at minors. It concerns audiovisual content which could be harmful to minors, regardless of whether this is contained in advertising or in general programming.)

21. Are on-screen warning icons required, either by law or by codes of conduct, for potentially harmful television programmes? Are acoustic warnings before such programmes required, either by law or by codes of conduct? Where such measures are used, are they considered to be effective?

22. Do any broadcasters established in your country use technical filtering devices to ensure that minors may not view harmful programmes? If so, what measures and initiatives have been taken to ensure that parents and guardians are aware of these devices and how to operate them. Are these devices held to be an effective means of protecting minors in your country?

23. Please describe measures which have been taken in order to improve media-literacy (e.g. teaching children how to make a responsible use of television)?

Video Game Software

24. Are there any specific legal provisions in your country concerning the sale of video games? (This question concerns the physical sale of video game software, not the provision of software over the Internet for downloading onto computers.)

25. Is there any self-regulatory system in place which covers questions relating to age-rating for video games? (e.g. such as the system of self-rating which has been announced by the Interactive Software Federation of Europe (ISFE)) If so, please give details.

26. Are current measures to protect minors from harmful video games considered to be effective?

27. As online games and computer games, especially on LANs (Local Area Networks), are very similar, have you also included them into measures of self-regulation and/or regulation?

Other Content Delivery Systems

28. With regard to cinema, videocassette and DVD rating systems, have there been any major developments since the year 2000?

General

29. In what way have you associated consumer associations, voluntary associations and non-governmental organisations to the implementation of the Recommendation?

30. Is the lack of coherence between the various rating and classification systems for audiovisual media (cinema, television, videocassettes, video games, Internet) seen as problematic in your country, e.g. in terms of creating confusion among customers? Are any measures or initiatives being considered to introduce greater coherence in the way audiovisual media are evaluated and classified? Has there been any cooperation to this extent with other Member States or organizations from abroad?

31. Have the efforts in your country with respect to the protection of minors been accompanied by scientific boards and specific studies with respect to violence or other harmful content and their impact on minors? Are there any voluntary agreements by broadcasters and by content providers on the Internet?

32. If you are aware of any study or scientific report which has been prepared on this issue during the last two years, please transmit a copy or give the references.

33. The Commission is aware that Member States' authorities may not be in a position to answer all the questions posed here. Nevertheless, the Commission would request that they be answered insofar as possible. Any additional information and any relevant views which might help the Commission in evaluating the effectiveness of the self-regulatory approach laid out in the Recommendation on the Protection of Minors should also be given.

STANDARD WORK PACKAGES AND DELIVERABLES
CALL FOR PROPOSALS FOR AWARENESS NODES

Work Package Overview

Work-packageNo ²⁸	Work Package title	Lead Contractor No ²⁹	Person-months ³⁰	Start month ³¹	End month ³²
1.	Planning, management and reporting			T0	T24
2.	Project assessment			T6	T24
3.	Develop awareness tools and methods			T0	T24
4.	Dissemination			T0	T24
5.	National co-operation			T0	T24
6.	Contribution to European network			T0	T24
	TOTAL				

²⁸ Workpackage number: WP1 – WPn.

²⁹ Number of the contractor leading the work in this workpackage.

³⁰ The total number of person-months allocated to each workpackage.

³¹ Relative start date for the work in the specific workpackages, T0 marking the start of the project, and all other start dates being relative to this start date.

³² Relative end date, T0 marking the start of the project, and all end dates being relative to this start date.

Work Package Description				
Work package number :	1	Start date:	T0	End date: T24
Work package title:	Planning, management and reporting			
Participants involved:				
Person-months per participant:				
Objectives				
Plan the work, monitor progress, provide periodic reports.				
Tasks				
<ol style="list-style-type: none"> 1. Draw up a detailed work plan including mission statement, goals and operational objectives, resources and timetable. 2. Ensure that objectives, deadlines and quality standards are met. Establish adequate progress monitoring, assessment and quality control procedures through suitable indicators. Adapt project plan as required. 3. Liaise with EC project officer. Submit brief quarterly management reports in the first year, 6 monthly progress reports and annual cost statements. Submit an annual public report for publishing. 				
Expected results / indicators				
Delivery on time of work plan and reports of satisfactory quality Adherence to objectives, deadlines and quality standards				
Deliverables				
<ol style="list-style-type: none"> 1. Detailed work plan 2. Quarterly management reports in year 1 3. Six-monthly progress reports 4. Annual cost statements 5. Annual public report 				

Work Package Description

Work package number :	2	Start date	T6	End date:	T24
Work package title:	Project assessment				
Participants involved:					
Person-months per participant:					

Objectives

Assessment of the work and of the results of the project. The assessment will be published.

Tasks

1. Draw up an assessment methodology providing for intermediate and final assessments
2. Draw up the intermediate assessment
3. Draw up the final assessment.

Expected results / indicators

Appropriateness of assessment methodology
Degree to which assessment methodology is implemented
Timeliness and quality of assessments

Deliverables

1. Assessment methodology
2. Intermediate assessment report
3. Final assessment report

Work Package Description

Work package number :	3	Start date:	T0	End date:	T24
Work package title:	Develop awareness tools and methods				
Participants involved:					
Person-months per participant:					
Objectives					
Devise a cohesive, hard-hitting and targeted awareness campaign using the most appropriate media, taking into account best practice and experience in other countries.					
Tasks					
<ol style="list-style-type: none"> 1. Determine the specific objectives, appropriate 'marketing' strategies and effective messages for each target group. 2. Prepare a comprehensive set of awareness tools tailored to meet national needs (including information for users about European filtering software and services and about hotlines) 3. Identify key players (stakeholders, key industrial and institutional circles and multiplier organisations), contact them and ask them to participate. Organise preparatory meetings with key contacts at national level covering the different target audiences. 4. Identify upcoming events (seminars, conferences, discussion forums, theme- workshops, trade fairs, round tables, etc) Activities may be focused on one or several target groups at national/regional level. 5. Design an Activity Plan including distribution of awareness tools and a mass media Communication Plan. 					
Expected results / indicators					
Quality of awareness tools and appropriateness for target audience					
Timely delivery and quality of Activity Plan and mass media Communication Plan					
Number of stakeholders and multiplier organisations identified, contacted and agreeing to take part					
Number of events identified					
Deliverables					
<ol style="list-style-type: none"> 1. Activity plan 2. Mass media Communication Plan 3. A set of awareness tools 					

Work Package Description					
Work package number :	4	Start date:	T0	End date:	T24
Work package title:	Dissemination				
Participants involved:					
Person-months per participant:					
Objectives					
Act as node of the awareness network for [country]					
Tasks					
<ol style="list-style-type: none"> <i>Implement the Activity Plan</i> Organise various awareness and dissemination activities geared towards the different target groups. Focus on training the trainers and other multiplier activities. Promote information literacy as well as information and discussion amongst national “specialists” in crucial areas and within target groups at the national level. <i>Implement the mass-media Communication Plan.</i> Stimulate and co-ordinate media and press coverage and visibility, using different strategies, including: use of traditional media (press, radio, TV) to stimulate public awareness; send awareness packages to media and opinion leaders; use the editorial services of multiplier organisations to promote the dissemination of information (e.g. publication of articles in magazines, web sites, etc.). <i>Organise high-profile events such as a national Safer Internet Day and participate in key events</i> identified under WP 3 					
Expected results / indicators					
Number of tools distributed					
Number of trainers trained					
Number of downloads of tools available online					
Number of TV/press/radio items and audience reached.					
Number of events organised, number of participants					
Deliverables					
<ol style="list-style-type: none"> Implementation of Activity plan Implementation of Mass media communication plan 					

Work Package Description					
Work package number :	5	Start date:	T0	End date:	T24
Work package title:	National co-operation				
Participants involved:					
Person-months per participant:					
Objectives					
Ensure networking with relevant actors at national, regional and local levels					
Tasks					
<ol style="list-style-type: none"> 1. Set up a structured method of concertation (such as a Steering Committee) with the relevant actors at national, regional and local levels 2. Ensure the involvement of a) suitable multiplier organisations to guarantee adequate coverage of the target audiences b) industry and bodies concerned with child welfare (including law enforcement, ISPs, content providers and aggregators from electronic publishing and audiovisual sectors, search engine providers, media regulators, official and voluntary bodies) 					
Expected results / indicators					
Number of organisations involved in structured method of concertation, level of activity / co-operation					
Deliverables					
<ol style="list-style-type: none"> 1. Set up of structured method of concertation 2. Implementation of Structured method of concertation 					

Work Package Description					
Work package number :	6	Start date:	T0	End date:	T24
Work package title:	Contribution to European network				
Participants involved:					
Person-months per participant:					
Objectives					
Co-operate with the co-ordinating node and other national nodes in the European network					
Tasks					
<ol style="list-style-type: none"> 1. Actively co-operate with other national nodes in the European network by exchanging information about best practices, participating regularly in network meetings and designing and implementing a European approach, adapted as necessary for national linguistic and cultural preferences 2. Take part in sharing expertise and technical assistance between nodes in the European network 3. Share resources with other nodes especially regarding web content, newsletters, awareness tools, PR material and branding 					
Expected results / indicators					
Number of organisations involved in structured method of concertation, level of activity / co-operation					
Number of days spent on European network activities (minimum 20 days per node)					
Number of European network events attended by node representatives.					
Deliverables					
<ol style="list-style-type: none"> 1. Participation in activities of European network 					

Deliverables List				
No¹	Deliverable title	Delivery date²	Nature³	Dissemination level⁴
D1.1	Detailed work plan	T3	R	C
D1.2	Quarterly management reports	T3, T9	R	C
D1.3	Six-monthly progress reports	T6, T12, T18, T24	R	C
D1.4	Annual cost statements	T12, T24	R	C
D1.5	Annual/final public report for publishing	T12, T24	R	P
D2.1	Assessment methodology	T9	R	P
D2.2	Intermediate assessment report	T12	R	P
D2.3	Final assessment report	T24	R	P
D3.1	Activity plan	T6	R	C
D3.2	Mass media communication plan	T6	R	C
D3.3	Set of awareness tools	T1 - T24 according to detailed workplan	O	C
D4.1	Implementation of Activity plan	T7 - T24	O	P
D4.2	Implementation of Mass media communication plan	T7 - T24	O	P
D5.1	Set up of structured method of concertation	T3	O	C
D5.2	Implementation of Structured method of concertation	T4 - T24	O	C
D6.1	Participation in activities of European network	T1 - T24	O	C

Reports must be delivered on paper and in electronic form. Public reports must be in a format suitable for publication. Software deliverables (modules, web sites, prototypes, demonstrators) shall be delivered both on CD-ROM and Internet.

¹ Deliverable numbers in order of delivery dates. Deliverable numbers must indicate which work package they relate to, e.g. D2.1 for the first deliverable from work package 2.

² Month in which the deliverables will be available. T0 marking the start of the project, and all delivery dates being relative to this start date.

³ Please indicate the nature of the deliverable using one of the following codes:

R = Report

S = Software/Prototype/Demonstrator

O = Other

⁴ Please indicate the dissemination level using one of the following codes:

P = Public

C = Confidential, only for members of the consortium (plus Commission services and project reviewers) and, except for cost statements, for the network co-ordinator and other members of the network