



**EUROPEAN COMMISSION**  
Information Society and Media Directorate-General

# **Safer Internet and Online Technologies for Children**

**SUMMARY OF THE RESULTS OF THE ONLINE PUBLIC  
CONSULTATION  
AND  
20-21 JUNE 2007 SAFER INTERNET FORUM REPORT**

# Contents

<b>1</b>	<b><u>EXECUTIVE SUMMARY</u></b>	<b>3</b>
<b>1.1</b>	<b>OVERALL CONCLUSIONS</b>	<b>3</b>
<b>1.2</b>	<b>SPECIFIC CONCLUSIONS</b>	<b>4</b>
1.2.1	ILLEGAL VERSUS INAPPROPRIATE	4
1.2.2	UPDATE LEGISLATION	4
1.2.3	AWARENESS RAISING AND TRAINING	4
1.2.4	STAKEHOLDERS WORKING TOGETHER	5
1.2.5	TECHNICAL SOLUTIONS	5
1.2.6	RESEARCH	5
1.2.7	POLITICAL AND OTHER ACTIONS	6
<b>1.3</b>	<b>RECOMMENDATIONS</b>	<b>6</b>
1.3.1	RECOMMENDATIONS FOR ACTION	6
1.3.2	RECOMMENDATIONS FOR RESEARCH	9
<b>2</b>	<b><u>BACKGROUND AND STRUCTURE OF THE CONSULTATION</u></b>	<b>12</b>
<b>3</b>	<b><u>PART 1: ONLINE CONSULTATION</u></b>	<b>13</b>
<b>3.1</b>	<b>RESPONSES TO THE ONLINE CONSULTATION</b>	<b>13</b>
<b>3.2</b>	<b>REPLIES TO INDIVIDUAL QUESTIONS</b>	<b>15</b>
3.2.1	QUESTIONNAIRE 1 - FIGHTING ILLEGAL CONTENT	15
3.2.2	QUESTIONNAIRE 2 - FIGHTING HARMFUL CONTENT	20
3.2.3	QUESTIONNAIRE 3 - USER- GENERATED CONTENT AND ONLINE COMMUNICATION	25
<b>4</b>	<b><u>PART 2: REPORT FROM THE SAFER INTERNET FORUM 20-21 JUNE 2007</u></b>	<b>30</b>
<b>4.1</b>	<b>WORKSHOP 1 – ONLINE-RELATED SEXUAL ABUSE OF CHILDREN, WITH A SPECIAL FOCUS ON THE PROCESS OF GROOMING AND THE CONSEQUENCES FOR CHILDREN</b>	<b>31</b>
4.1.1	THEMES AND KEYNOTE SPEAKERS	31
4.1.2	MAIN CONCLUSIONS	31
4.1.3	RECOMMENDATIONS	32
<b>4.2</b>	<b>WORKSHOP 2 – AWARENESS-RAISING: ASSESSING THE NEED FOR AWARENESS-RAISING TOWARDS DIFFERENT TARGET GROUPS AND INCREASING THE EFFECTIVENESS OF SUCH ACTIVITIES</b>	<b>34</b>
4.2.1	THEMES AND KEYNOTE SPEAKERS	34
4.2.2	MAIN CONCLUSIONS	34
4.2.3	RECOMMENDATIONS	35
<b>4.3</b>	<b>WORKSHOP 3 – THE IMPACT AND CONSEQUENCES OF CONVERGENCE OF ONLINE TECHNOLOGIES</b>	<b>36</b>
4.3.1	THEMES AND KEYNOTE SPEAKERS	36
4.3.2	MAIN CONCLUSIONS	36
4.3.3	RECOMMENDATIONS	37
<b>5</b>	<b><u>ANNEX I – CONTRIBUTORS TO THE ONLINE CONSULTATION</u></b>	<b>38</b>
<b>6</b>	<b><u>ANNEX II – EXPERTS AND RAPORTEURS</u></b>	<b>40</b>

# 1 EXECUTIVE SUMMARY

The current Safer Internet *plus* programme<sup>1</sup> will end in 2008. In order to create a basis for deciding whether to propose a follow-up programme from 2009 to 2013, and how best to address issues relating to online technologies in the future, the Commission carried out a public consultation and a consultation with relevant stakeholders.

The conclusions and recommendations presented herein, as part of the ‘Summary of the results of the online Public Consultation’ which ran from 12 April 2007 until 7 June 2007<sup>2</sup> and 20-21 June 2007 ‘Safer Internet Forum reports’<sup>3</sup>, have been formulated with the support of an independent expert, Dr. Ute Navidi<sup>4</sup>.

The public consultation gathered 93 contributions, from a range of stakeholders: Industry actors and associations, associations (children's rights organisations, consumer organisations, trade unions and political movements), hotlines and awareness nodes, public administration bodies (law enforcement, regulators, governments etc), researchers and universities and a number of individuals. The Safer Internet Forum gathered 125 participants and more than 20 keynote speakers from 29 countries, from the same group of stakeholders as the public consultation.

## 1.1 Overall conclusions

Many respondents expressed a need to keep in mind the **overwhelmingly positive potential of the internet**, to inform, educate, entertain and – as far as industry is concerned – to drive business success.

At the same time there is now a growing understanding that the idea of creating a **risk free internet for children<sup>5</sup> and young people is an illusion**, and that they have to be equipped and learn how to avoid hazards and deal with risks.

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

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

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

---

<sup>1</sup> Decision No. 854/2005/EC of 11 May 2005 of the European Parliament and the Council adopting a multi-annual Community Programme on promoting safer use of the Internet and new online technologies OJ L149, 11.6.2005, p1

<sup>2</sup> For more information see [http://ec.europa.eu/information\\_society/activities/sip/public\\_consultation/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm)

<sup>3</sup> For more information see

[http://ec.europa.eu/information\\_society/activities/sip/si\\_forum/forum\\_june\\_2007/agenda/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/si_forum/forum_june_2007/agenda/index_en.htm)

<sup>4</sup> See Appendix II.

<sup>5</sup> References to ‘child’ or ‘children’ imply children and young people, using the definition of the United Nations Convention on the Rights of the Child, i.e. from birth to 18.

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

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

The way that the internet and other online technologies are used in a more interactive way than before is often referred to as Web 2.0. The differences between the Web 1.0 and Web 2.0 can be summarized in the following table<sup>6</sup>:

<b>Web 1.0</b>	<b>Web 2.0</b>
Downloading	Uploading
Consuming	Creating
Corporate	Personal
Separate Media	Converging Media
Static	Interactive

## **1.2 Specific conclusions**

### **1.2.1 Illegal versus inappropriate**

There is a degree of **‘definitional uncertainty’**, which causes many respondents to believe that the definition of illegal content or material, and consequently actions, should primarily rest at **national** level. Where, however, there is a level of **consistency** (e.g. over the production and distribution of illegal child abuse images, actions against phishing websites, and fraudulent services), **EU-level action** with regard to legislation and law enforcement cooperation should be taken. Whilst many stakeholders now use the term ‘images of child abuse’ rather than child pornography, the definition should be open-ended and include any and all forms of sexual exploitation of children and young people, including pseudo-images and non-photographic material such as texts.

### **1.2.2 Update legislation**

Different legislation across Europe exists concerning online child abuse, grooming and physical contact arising thereof. There is a need for greater clarity and **standardisation**. Attitudes to **harmonising** legal provisions across Member States differ; other forms of cross-border support and self-regulation have strong support. A new offence of possession of ‘non-photographic visual depictions of child sexual abuse’ was proposed.

### **1.2.3 Awareness raising and training**

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

---

<sup>6</sup> As summarized by Carrick-Davis, speaking at the Safer Internet Forum 2007 (see workshop 2 report below)

Many proposals were made with respect to implementing the UN Convention on the Right of the Child with regard to facilitating the **empowering of children and young people** and adults to undertake grass-roots actions in developing, taking and disseminating preventive and educational measures themselves. Measures are required to strengthen children's capacity to be **creative and innovative**, alongside promoting an understanding that children are consumers and potential victims as well as **actors** – in both positive and negative ways – with regard to the new technologies. **Disabled children's** needs and their right to take part in the opportunities and challenges offered by the new communication technologies should be recognised and addressed.

There is a need to improve the understanding of the relationship between online and offline worlds with regard to **risk**, and the nature and reasons for children's **risk-taking activities**, afforded for example by Web 2.0 opportunities. The Commission should therefore also support the development of websites with good and **attractive content** for children as a positive, preventive measure.

Learning from other public awareness campaigns, robust measures should be developed to assess the **impact of awareness campaigns** at different levels and on different target audiences. The role of the **Safer Internet Day** remains crucial and should be used to organise public, highly visible events and produce awareness materials and tools.

#### **1.2.4 Stakeholders working together**

The need for a **comprehensive approach** was stressed, with **multiple stakeholders**, including hotlines, awareness nodes, industry, education ministries, media and children's NGOs working together as individual actions by individual agencies have limited impact and effectiveness. **Good practice models** of joint projects (e.g. cooperation between law enforcement agencies and hotlines) should be promoted and financially supported. There was a call on awareness nodes to build closer relationships with the **media** - press, radio and television. **NGOs** require assistance to keep up to speed with a rapidly changing technological environment, and need more effective support with their work and in accessing existing networks.

#### **1.2.5 Technical solutions**

There is a widely shared understanding that a **combined solution**, of improved education and greater awareness, and better technical solutions (e.g. robust age verification methods) is required. Effective systems to trace, analyse and block websites disseminating child abuse material at European level were recommended, requiring collaboration and legislative support.

#### **1.2.6 Research**

There was a strong sense of the need to establish **reliable facts and figures**, and to **coordinate** effectively what is known, i.e. bringing together existing research to help close gaps in knowledge and understanding. A convincing case was made to invest in more **qualitative**, in-depth research which is culturally sensitive, and to develop tools for and fund **comparative** research. Research findings should also be **disseminated** and made available more widely.

Many specific **areas for new research** were identified and are outlined below, including more refined analyses concerning issues such as grooming, risks evolving into harm, consequences of online communication, communication patters among children themselves, and between children and adults, parents and teachers.

### **1.2.7 Political and other actions**

The Commission was asked to provide support and to promote a **holistic** approach to cooperation between different stakeholders, in particular governments at national and European level. Specific recommendations for action were proposed, such as for the Council of Europe to issue a statement on sexual exploitation of children addressing issues such as grooming and victim identification, and for the Commission to move the tackling of child sexual abuse higher up the European political agenda while encouraging governments to keep themselves informed and to collaborate with each other. **Governments' role** in terms of providing funding, political support and legislation, and raising awareness and initiating education programmes to improve 'media literacy' was also highlighted. To this end, the Commission was urged to work with **education ministries** to integrate media literacy into citizenship education, and embed online use and awareness raising into school curricula throughout Europe. Teachers need to be empowered with appropriate support, guidelines, and e-safety training to fulfil the task.

## **1.3 Recommendations**

Key recommendations are summarised under the headings of actions and research.

### **1.3.1 Recommendations for Action**

Respondents to the online consultation and participants of the Safer Internet Forum were united in recommending the continuation of the Safer Internet *plus* programme.

#### ***Illegal content and online activities***

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

Many contributors felt that there were limits to technology in combating online illegal content: 'we don't think technical measures will greatly help to combat illegal content'; 'the list of issues is infinite', hence the overwhelming focus on combining technical improvements with strong educational and awareness raising measures.

#### **International cooperation**

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

An international network of NGOs was suggested, one that can engage with the public and lobby governments.

Illegal websites should be blacklisted with Russia and the USA a priority.

#### **Political agenda**

- the Council of Europe should make a statement on the sexual exploitation of children
- the European Commission (EC) to push tackling of child sexual abuse higher up the European political agenda
- the European Commission to provide support for and promote a holistic approach to cooperation between different stakeholders
- the European Commission to encourage governments to stay informed on online grooming and related subjects, collaborate with each other and take actions at national and European levels
- governments to accept their role in terms of providing funding, political support and help to create new legislation, and in raising awareness and initiating education programmes.

### **Law enforcement**

Prime responsibility for fighting against any illegal activities and illegal content such as child sexual abuse material, should rest with the police. Law enforcement bodies' capacity should be strengthened, to be able to take a more proactive approach and be able to engage in cross-border co-operation. This requires specialist training for police and the creation of teams which specialise in technology.

More sting operations with the police and hotlines cooperating were considered effective ways of combating online child abuse.

An EU database was considered necessary to fight illegal content more effectively.

### ***Awareness raising***

There was a wide consensus that awareness strategies should be based on a combination of education and media campaigns. Safer Internet Days should continue, as public, highly visible events with dedicated awareness materials.

**Awareness campaigns and programmes** are to

- reflect the 'children's agenda', not that of adults, and recognise that 'children cannot live forever in a virtual world based on filters and parental controls'
- distinguish between different age groups when child audiences are targeted, starting from a much younger age (e.g. 6-year-olds)
- be developed for specific target groups, possibly based on a five-step approach: Knowledge (be aware), Approval (support for new behaviour), Intention (convince target of new behaviour), Practice (put new behaviour into practice), and Advocacy (encourage other to do the same)
- learn from good practices from different countries and from campaigns at European level, and share these more effectively across Europe
- improve the understanding of the implications and consequences of the Web 2.0
- focus on parental under-use of access control and filtering systems
- involve the media, especially press, radio and TV, as key partners; awareness nodes should build a closer relationship with them. However, the media are fragmenting, their traditional editorial content being challenged by user-generated content. The media were urged to move towards a more balanced approach, and give a voice to children and young people themselves when dealing with harmful content.

### **Education**

- Education should focus on empowering and building the capacity of children and adults themselves to take and disseminate preventive and educational measures
- Such education should be integrated into the curriculum and promoted as ‘media literacy’, be compulsory, and part of citizenship education
- Teachers are to combine education on internet use with developing an understanding of its risks, with appropriate support and e-safety training for all teachers, and guidelines, to fulfil this task
- Online safety should be seen as a cultural rather than an ICT issue
- It should start from the age of six and not only with the 8-12 year age group
- To engage and support parents by developing and improving their communication skills based on their existing knowledge, sensitising them to children’s ideas, needs and aspirations
- Education for parents should include informing them of the choice of tools available; this presupposes knowledge about what parents are already doing, and to what effect
- Parents’ responsibility cannot be off-loaded onto schools.

### ***Stakeholder cooperation and exchange of best practice***

There was a consensus that multi-stakeholder, public/private partnerships can be very successful, evidenced by a growing number of good practice examples. The continuing independence and ethics of awareness nodes need to be safeguarded. Multi-stakeholder partnerships should be expanded and fortified. Specifically:

- The European Commission was asked to strengthen stakeholder cooperation, providing co-ordination between all those making a ‘significant contribution’
- The European Commission to provide focused political leadership, continue its support in areas where it is active (e.g. hotlines, umbrella organisations), and examine current legislation and make proposals, e.g. on allowing the ‘interception’ of data
- Focus of cooperation and support should be on
  - sharing information
  - promoting and financially supporting joint projects as models of good practice
  - promoting policies
  - facilitating further professional networking and training (including for mass media workers)
  - supporting the work of NGOs
- Practical measures should include
  - buying the copyright to materials dealing with online related sexual exploitation/abuse of children
  - making such materials freely available to stakeholders and disseminating available items
  - seeking the collaboration for enhanced use of blocking systems by ISPs at European level, with legislative support where necessary
  - creating a general list of websites disseminating online child abuse material, again with the aim of facilitating blocking at the European level.

### ***Technological tools***

- There should be support for the development and use of
  - software to trace, analyse and block websites disseminating online child abuse material
  - tighter age identification/verification systems and implementation mechanisms

- The EC was also asked to participate in developing websites with good and attractive content for children as a positive preventive measure.
- Manufacturers are to consider researching a hardware methodology for interception of data

### ***Self regulation***

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

### **1.3.2 Recommendations for Research**

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

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

In the online consultation the EC, governments and ‘big industry’ were urged to continue investing heavily in research and development. Collaborative research involving children’s NGOs was suggested.

### ***General areas for research***

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

### ***Children***

Research is to be structured into 3 Cs (content, contact, conduct) while recognising that a child using online services can fall into all three categories. Increasingly the focus should be on the child as actor as the research recommendations indicate. Robust methods of age verification also

featured prominently. Research has to address what happens in reality, on- and offline, not what adults think is happening, especially regarding changing attitudes to sex and sexuality.

#### **Content: the child as recipient**

- identifying the most vulnerable target groups of children for online abuse, with the help of social workers, psychologists, and specialists
- the psycho-social impact on children, ranging from accessing offensive images online, to being abused
- children and young people's own perceptions of risk and harm
- children and young people's reactions to online predators
- reasons for not disclosing abuse
- technologies and procedures for victim identification
- ways of supporting victims

#### **Contact: the child as participant**

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

#### **Conduct: the child as actor**

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

#### ***Families and parents***

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

#### ***Offenders***

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

#### ***Law enforcement***

- How investigations into child abuse images are handled

### ***European comparative facts and figures***

- robust statistics (nationally and Europe-wide) particularly on online sexual abuse and grooming
- comparative study of relevant legislation
- co-ordination, harmonisation and standardisation of procedures, e.g. online undercover operation in chatrooms, avoiding the charge of entrapment

### ***Alternative voices***

- to examine the way in which online sexual abuse and measures of combating it are viewed from alternative perspectives, including by civil liberty organisations

## 2 BACKGROUND AND STRUCTURE OF THE CONSULTATION

The Commission launched a public consultation to identify the most effective ways of making the online environment and communication technologies safe for users, in particular children. The current Safer Internet *plus* programme will end in 2008 and the Commission was conducting this consultation to create a basis for deciding whether to propose a follow-up programme from 2009 to 2013, and how best to address issues relating to online technologies in the future.

**The public consultation consisted of two Parts.**

### **Part 1 – Public online consultation**

The public online consultation ran from 12 April 2007 until 7 June 2007, with an extension made to allow for responses until 13 June. A small number of responses arrived after that date, but were nevertheless taken into account.

The online consultation was announced on 12 April via [http://ec.europa.eu/information\\_society/newsroom/cf/itemlongdetail.cfm?item\\_id=3355](http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3355), and six days later on [http://ec.europa.eu/yourvoice/consultations/index\\_en.htm](http://ec.europa.eu/yourvoice/consultations/index_en.htm). Information was sent to subscribers of the mailing list of the Safer Internet website on EUROPA. The consultation itself was published on EUROPA at [http://ec.europa.eu/information\\_society/activities/sip/public\\_consultation/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm).

This part of the consultation was based on a consultation document and a questionnaire structured around three main sections: **Fighting illegal content, Fighting harmful content, and User-generated content and online communication**. Each main question was followed by a sub-set of questions (altogether 24 questions).

Arrangements were made for hard copy submissions; however, none such were received.

The consultation papers were issued in English, French and German requesting responses in English; responses were received in four community languages (English, French, German and Italian).

### **Part 2 – Experts' consultation through Safer Internet Forum**

The experts' consultation was a part of a two-day Safer Internet Forum held between 20 and 21 June 2007 in Luxembourg. It comprised three workshops on Day 1 (see Annex III), covering the following themes: **Online-related sexual abuse of children, awareness-raising, and converging technologies**<sup>7</sup>.

---

<sup>7</sup> Agendas and presentations of key speakers are available at [http://ec.europa.eu/information\\_society/activities/sip/si\\_forum/forum\\_june\\_2007/agenda/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/si_forum/forum_june_2007/agenda/index_en.htm)

### 3 PART 1: ONLINE CONSULTATION

#### 3.1 RESPONSES TO THE ONLINE CONSULTATION

The Commission received 93 electronic contributions altogether by the extended deadline, which came from 19<sup>8</sup> European Union countries, Norway, Russia and USA.

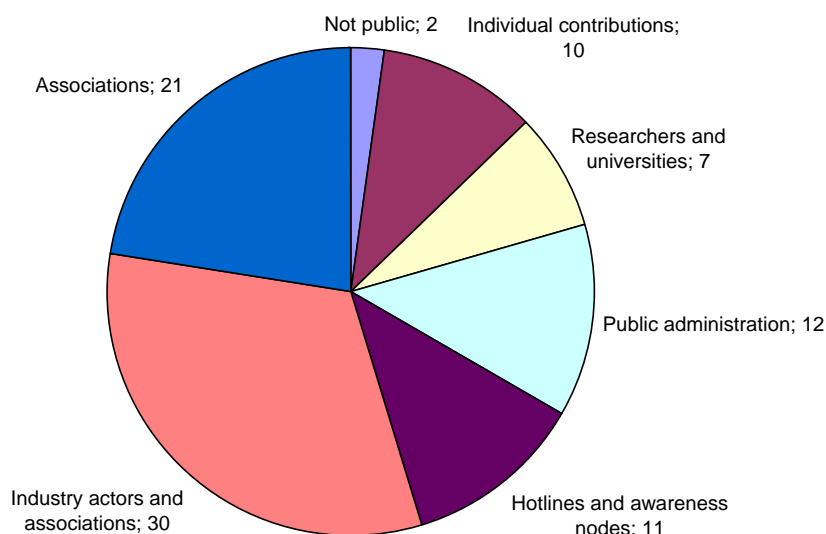
This compares well with the Commission's public consultation on 'Child Safety and mobile phone services' carried out between July and October 2006 where 74 contributions were received. It is also broadly in line with the responses to the public consultation on Media Literacy which closed on 15 December 2006, where 103 submissions were received from 23 EU Member States, as well as from China, Russia and the USA.

#### Main stakeholder groups

<b>Industry actors and associations</b> representing a wide variety of related industries	30
<b>Associations</b> including NGOs such as children's rights and welfare organisations, consumer organisations, trades unions and political movements	21
<b>Hotlines and awareness nodes</b> <sup>9</sup>	11
<b>Public administration</b> including law enforcement, regulators, government departments etc	12
<b>Researchers and universities</b>	7
<b>Individual contributions</b>	10
Two respondents requested that their answers should <b>not be made public</b>	2
<b>Total</b>	<b>93</b>

<sup>8</sup> Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Malta, Poland, Portugal, Spain, Sweden, UK

<sup>9</sup> These contributions were from hotlines and awareness nodes that the Programme funds. However, also contributing organisations from other stakeholder groups run hotlines supported by the Programme, but did not state this in the contribution.



This means that industry and industry-related bodies were represented as the largest single stakeholder group, with 29 per cent of responses. Almost a quarter (24 per cent) came from Associations such as NGOs. European hotlines and awareness nodes contributed 13 per cent of all responses, the same proportion as Public Administration bodies. Eight per cent came from researchers and universities, and 11 per cent were submitted by individuals, including a number of internet experts.

Parents and teachers' organisations were not directly represented in the responses, nor were independent media organisations – all important potential stakeholders in the Safer Internet programme.

Of the 93 contributions, 91 are published on the Internet may be viewed in full and downloaded from <http://ec.europa.eu/saferinternet>. Please see the Annex I for a list of contributors.

## 3.2 REPLIES TO INDIVIDUAL QUESTIONS

### 3.2.1 Questionnaire 1 - Fighting illegal content

#### Introduction

The definition of illegal content varies from country to country due to differing cultural traditions and national legislations. It can be accessed via the Internet, through mobile phones and game consoles. Even though the definitions of what is illegal content varies across countries, from racist and discrimination material to cyber crime, fraud, hacking, identity theft etc., the production and distribution of child sexual abuse material is considered to have the most severe consequences for children, and it is illegal in most European countries.

The production and distribution of child abuse material is facilitated through commercial websites, user generated web sites and peer-to-peer/file sharing networks.

There were **nine** questions to be answered.

#### 1.1 In your opinion, is there a need beyond the year 2008 to pro-actively fight against **illegal content**?

There was unanimity among respondents in welcoming the Commission's consultation on whether to propose a follow-up programme from 2009 to 2013, and how best to address issues relating to online technologies in the future. Many stated explicitly that efforts so far in the fight against illegal content had been positive and successful, and feared that these good results would be jeopardised if the fight against illegal content were to cease after 2008, not least because online crimes against children and illegal content are expected to take on new forms.

There was an overwhelming consensus that the presence of illegal content online is not about to decline but is expected to grow dramatically, and be increasingly trans-national. Much illegal content has an increasingly common financial route, i.e. it is highly profitable and part of organised crime. Therefore the need to tackle the latter more generally was also highlighted.

The distinction between illegal and inappropriate content was welcomed. However, in answering questionnaires One and Two, several respondents found it difficult to adhere to this distinction.

#### 1.2 If so, please give indications on what kinds of illegal content/material should be dealt with.

Many comments indicated a degree of 'definitional uncertainty'. A non-exhaustive definition of what constitutes 'illegal content' is needed, so that it can include any and all forms of sexual exploitation and abuse of children and young people, including pseudo images and non-photographic material, such as texts.

Many respondents agreed that the definition of illegal content or material should primarily rest at the national level, because the interpretation of 'illegal' differs significantly across the borders of EU27. However, in areas where the production and distribution are consistently seen as illegal (e.g. illegal child abuse images), the case could be made for more consistent EU-level legislative and law enforcement actions.

Respondents listed a range of illegal content and material they believed should be dealt with. Top of the list and where focus and priority should remain was 'child pornography'. Stakeholders were however asked to agree on replacing this terminology universally with the

term ‘images of child abuse’ which many are already using. There was a strong recommendation to create a new offence of possession of ‘non-photographic visual depictions of child sexual abuse’.

The list of illegal content/material to be dealt with included a whole range of other issues, from A to Z: selling alcohol to children online, racism/xenophobia, drugs promotion, anorexia/bulimia sites, glorification of war, bomb-making and the sale of weapons, just to name a few.

1.3 Which should be the means of fighting the production and distribution of illegal content, in particular child sexual abuse material, and what stakeholders should take initiatives (industry, governments, NGOs, financial institutions etc.)? Please suggest ways in which the different stakeholders can contribute in fighting against production and online distribution of illegal content.

This Question attracted a large number of extensive comments and detailed proposals.

Prosecution of producers of illegal content should be top priority. An EU database was considered necessary to fight illegal content effectively.

The vast majority of contributions emphasised that fighting illegal content should be based on public/private partnership involving a wide range of stakeholders. Such partnerships should include financial institutions, media, research organisations and universities, in addition to existing or long-standing stakeholder groups.

Many felt that prime responsibility for fighting against any illegal activities, including illegal content such as child sexual abuse material, should be a matter for the police and remain the responsibility of law enforcement bodies whose capacity should be strengthened, including their ability to engage in cross-border co-operation. One submission said that ‘they exclusively should be responsible for actions against criminal activity’ and conduct more proactive policing.

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

Governments too have a role, in terms of providing funding, political support and helping to create new legislation, and in terms of raising awareness and initiating education programmes.

A specific call was made to establish an international network of NGOs that can engage with the public and lobby governments.

Some ‘frustration’ was expressed over the non-use of existing technology to block sites. The online industries have a responsibility to assist with blocking access to sites (e.g.via the ‘cleanfeed’ method), while filtering and parental control software were also mentioned by many.

1.4 A central element of the fight against illegal content for the Safer Internet plus Programme has been to support an international network of civilian hotlines where the public can report illegal content, should they chance upon it online. In your opinion, is this the most appropriate way of dealing with illegal content beyond 2008? How could their cooperation with law enforcement agencies be strengthened?

The work of INHOPE, the international network of hotlines, supported by the Safer Internet *plus* Programme, is highly valued and it should continue to receive support and be strengthened. The work of national, civilian hotlines was considered to be necessary and successful by most contributors. But many agreed that the ‘hotline model needs to evolve’.

Specific aspects of the hotline model were mentioned, and suggestions made regarding the future scope and nature of its activities:

- Those hotlines operated by NGOs were said to be good at engaging the public
- There is a need to adjust to different and much higher volumes of reports
- The question of liability should be reviewed
- A review should take place on whether full use is being made of data collected
- Hotlines should broaden their focus.

A small number of contributions, however, questioned the role of hotlines, as ‘not an appropriate way of dealing with illegal contact’; one explicitly said ‘disband hotlines, leave such activities to the police’.

One contributor pointed out that civilian hotlines can be of crucial importance as providing a link between police and members of society in countries where people hesitate to contact the police on certain matters.

1.5 How can other organisations support national/local and international law enforcement agencies in dealing with the production and online distribution of illegal content?

The raising of awareness about the work and existence of hotlines as such underlines the further success of dealing with illegal content.

Many contributors thought that internet service providers and hosting organisations can help by sharing their technology. Telecommunication companies should also be involved.

Involving financial institutions was necessary, particularly to impose effective sanctions on all who use a credit card to purchase illegal content. They have also experience with age verification methods.

Other organisations have a responsibility to contribute to the law enforcers’ efforts in dealing with the production and online distribution of illegal content. It was suggested that this could best be done by being members of a broad national Safer Internet consultative body.

Sting operations in cooperation with the police and hotlines were considered effective.

1.6 The Internet has a global dimension: illegal content can be produced in one country, distributed from a second and accessed/downloaded in many countries across the world. Please specify which actions should be taken internationally. Are there specific countries which should be focussed on?

INHOPE was called ‘an excellent example of a successful initiative’ in this regard, and the cooperation and information sharing between all hotlines should be strengthened. They should facilitate the creation of a ‘single list’ of addresses of known illegal websites so that all European ISPs or mobile providers can block access to them, a measure which was said to have the support of the industry. Some went as far as calling for an international communication hotline to enable all national police departments to have access to the information to assist them in making arrests, and to be in regular contact with the national hotlines/nodes.

Existing age verification technologies should be made greater use of.

Specific training for police and the creation of teams which specialise in technology should take place.

Some explicitly called for illegal websites to be blacklisted.

The resources issue was also addressed, with one contribution expressing explicitly the difficulty of working on a tight budget yet carrying out non-European work and vetting processes in target countries (countries where illegal content is produced) prior to their participation in the network of hotlines against illegal content on the internet.

Russia and the USA were stated to be the top priority, alongside former countries of the Soviet Union and Eastern Europe; other countries mentioned include Thailand, Vietnam, Laos, and Cambodia; this list reflected the fact of the 'problem growing in Asia'.

1.7 Research and development of efficient technological tools (filtering systems, image recognition etc) can contribute to reducing online distribution and indirectly the production of illegal content. Which are the subjects which should be addressed when supporting the development of technologies?

Considerable diversity of opinion was expressed in responding to this Question, some views contradicting others.

Overall, there was a call for the EC, government and big industry to continue investing heavily in research and development.

Filters were the most frequently mentioned subject to be addressed in the development of technologies. It was said that installing filtering software is 'easy'.

Several contributors urged, however, that a holistic approach be adopted in future technological solutions. 'Technology will not be the primary solution to the problem'. They felt that there were limits to technology: 'we don't think technical measures will greatly help to combat illegal content'; 'the list of issues is infinite'. Individual respondents in particular highlighted that filtering systems can be misused for censorship.

Tools should be developed on a voluntary basis. The governments' role should be supportive rather than prescriptive – for example, the industry was already devoting considerable resources to combat phishing.

Some argued that developments in this area should have a victim focus.

One respondent questioned how to ensure the sufficient and effective blocking technology for all ISPs. Another stressed the high costs of implementing blocking for smaller ISPs.

1.8 Analysis of psychological effects of victims and studies of how offenders use the Internet to distribute the evidence of the sexual abuse of children can also contribute to the fight against illegal online content. Which are the subjects which should be addressed in these areas when conducting research?

There were both general and specific suggestions for future research:

- New ways in which sexual abuse is caused by new technologies
- How investigations into child abuse images are handled

- How to limit distribution through newly appearing content production tools
- Exploring strategies and effectiveness of parental regulation
- Auditing online content aimed at children
- Collaborative research involving children's NGOs

Many comments proposed separately future research regarding victims and offenders:

### **Victims**

- Research about what happens in reality and not what adults think is happening – especially also into changing issues to do with sex and sexuality, on- and off-line
- Need for longitudinal studies
- Who are the vulnerable groups
- How to support victims
- How children and young people react to online predators

### **Offenders**

- How offenders use the internet, e.g. how they find and target children
- The link between children and young people downloading images of child abuse and the cross-over into sexually harmful behaviour
- The link between the consumption of child abuse images and contact sexual abuse of children
- On the dividing line between normal adolescent behaviour and sexually harming children
- New and changing profiles of child abusers

1.9 The legal situation concerning online distribution of illegal content and indeed the definitions of what is illegal differ across the EU Member States. Which are the issues which should be addressed when harmonising legal provisions across Member States?

Attitudes to harmonising legal provisions across Member States differed. Similarly, national sentencing policies and attitudes of law enforcement agencies reflect different national views.

A number of issues were considered suitable to be addressed through greater harmonisation:

- Taking action against phishing websites
- Fraudulent services
- Creating a common list of illegal URLs in Europe

Several contributors mentioned that there is already a Council Framework (2003) in place with a common definition of 'child pornography' and wanted more legal harmonisation to online offences. Some stressed the particular difficulty posed by the vast differences which exist in European countries regarding children's age of consent.

One contributor explicitly expressed the need for harmonisation from the child's perspective: children everywhere have the same rights and adults need to stand by them.

Explicit opposition to harmonisation came from different types of stakeholders, as exemplified by these quotes:

It is "questionable whether there is a necessity for harmonisation" (industry representative)

"I do not support the principle of harmonisation in this field" (response by an individual)

### 3.2.2 Questionnaire 2 - Fighting harmful content

#### Introduction

Harmful content is content that potentially can be harmful or dangerous for children, and includes content which parents and carers do not want their child to have access to. It can be accessed through Internet, mobile phones and game consoles. What is considered harmful for children varies across cultures. However, in most cases it ranges from pornography, violence, racism, xenophobia, self-mutilation, anorexia, suicide sites, dangerous sects or hate speech to child sexual abuse material.

Risks for children who are exposed to harmful/unwanted content are psychological trauma and encouragement of harmful behaviour, such as violence against oneself (self-mutilation, developing eating disorders, and suicide) and others (inflicting violence or sexual abuse of others, bullying, happy slapping etc). In addition, accessing and downloading such content can give rise to security risks: viruses, spam, hacking, identity theft which may cause financial problems and damage to the computer, inadequate advertising, copyright infringement and co-participation in an illegal activity.

There were **seven** questions to be answered.

This questionnaire attracted literally dozens of recommendations. Many of these are also reflected in the reports of the feedback of the conference workshops (see below), i.e. they complement each other well.

2.1 In your opinion, is there a need beyond the year 2008 to pro-actively fight against harmful content? If so, please give indications on what kinds of harmful content/material (subjects to be covered) should be dealt with.

There was almost universal agreement that the fight against harmful, as distinct from illegal, content also needs to continue.

Several indicated that harmful content could best be countered through promoting good practice.

Several queried the use of the term 'fighting harmful content', preferring to talk about the need to educate children and parents about avoiding accessing age inappropriate content.

The list of what kinds of harmful content/material should be dealt with was extensive, and included, for example and in no particular order:

- extreme violence, raw violence
- self-harming, pro-suicide, pro-bulimia/anorexia
- terrorism
- drug taking
- bullying
- fraudulent financial activity
- gambling; games creating the basis for addiction
- buying knives, alcohol, tobacco, adult videos
- encouragement to run away
- promoting physical stunts such as in videos
- identity theft
- racism

2.2 Which are the means of fighting the production and distribution of harmful content and what stakeholders (media, governments, industry, NGOs, schools etc) should take initiatives? Please suggest ways in which the different stakeholders can contribute in the fight against the online distribution of harmful content.

There was a broad consensus that there should be a widely based, national Safer Internet consultative body with representation of all stakeholders engaged in this initiative – all official institutions (ministries, agencies, law-enforcement), associations of IT industry, media, child-care organisations, and NGOs, to give them maximum leverage to lobby for necessary legislative and administrative measures.

Specific new actions mentioned were, among others:

- Age verification mechanisms
- Informing parents of the choice of tools available, which would also require some knowledge about what parents are already doing, and to what effect
- To promote media literacy
- More school based education campaigns
- Improved and targeted awareness campaigns

One respondent was concerned that because non-mainstream culture has traditionally been a source of creativity, the broadening of the definition of harmfulness could have a ‘chilling’ effect on innovation.

One respondent expressed the view that the Safer Internet programme is currently defensive and instead should be promoting positive surfing and communication options. Again, the existence of a common set of European guidelines was referred to.

2.3 In your opinion, should the media take an active part in the awareness-raising in this sphere and in what way?

There was a unanimous ‘yes’ to the question whether the media should take an active part in awareness raising. ‘Yes – absolutely’. ‘Without the media, awareness raising is not possible.’

However, the capacity of the media to engage was questioned by several respondents, particularly noting that:

- The media is fragmenting and user-generated content is attracting attention away from traditional editorial content
- The media should be urged to move away from scare-mongering and sensationalising online dangers, and instead promote media literacy, and provide balanced and factual information about dangers to the public
- The media should give a voice to children and young people themselves when dealing with issues related to harmful content

2.4 Which role could education have in empowering children to deal appropriately with harmful content? Should it be integrated into school curricula? If so, which would be the best ways of doing so?

Many suggestions were made about how to improve education to empower children to be better equipped to deal with harmful content.

Particular recommendations included:

- This should be integrated into the curriculum as ‘media literacy’
- Online safety is often seen as an ICT rather than as a cultural issue
- It should be compulsory
- It should be from the age of 6, not between 8-12 years
- It should focus on empowering children, and be made part of citizenship education

- Guidelines for teachers are needed
- Teacher training organisations need to integrate e-safety as essential training for all teachers.

However the role assigned to education did not receive unanimous support.

Some respondents argued that education should not be seen as the only route to dealing with harmful content. Parents' responsibility cannot be off-loaded onto schools.

One respondent warned that children cannot live forever in a virtual world which is based on filters and parental controls.

An individual's response was that 'I'm not sure that a formal module is helpful.'

2.5 A primary activity of the fight against harmful content for the Safer Internet plus Programme has been to support an international network of awareness nodes which promote public campaigns informing the public of the risks linked to the use of online technologies and on safeguard measures. In your opinion, is this the most appropriate way of dealing with harmful content beyond 2008? If so, please indicate in what ways this line of action can be strengthened.

The Safer Internet *plus* programme and its support for an international network of awareness nodes received a 100 per cent thumbs up – explicitly or implicitly – from the online consultation responses which stressed the need for continuing this important work.

Various suggestions were made on how the Programme might strengthen this work in the future:

- Work in close co-operation with hotline operators
- Educate parents and teachers – don't substitute parental authority but rather support it
- Have a more robust programme with more resources deployed
- Involve more people and organisations with PR expertise
- Avoid duplication by working cross-boundaries
- Develop and employ effective filtering systems
- Ensure awareness projects are established into social institutions before they come to an end, to ensure their sustainability beyond the period of EC funding

2.6 Efficient technologies can help to make the use of the Internet, mobile phones and game consoles safer for children to use (e.g. filtering software by Internet Service Providers or at user's computer, age verification mechanisms etc). Which are the subjects which should be addressed when supporting the development of technological tools?

This question attracted many detailed discussions, particularly on a variety of filtering methods and products – these may be pursued in more detail in the original submissions posted on the internet. The following considerations give an idea of the many issues surrounding filtering in particular, and are evidence that this whole area requires further in-depth consideration and discussion.

The vast majority of responses reiterate the belief that technology alone cannot solve these problems, but needs to go hand in hand with awareness raising activities, particularly also targeting parents.

Robust age verification methods appear to be considered effective and uncontroversial from the responses received.

Many contributions explicitly address the benefits of filtering technologies, with those which can be deployed at the user end rather than by content providers often stated as a preference. In some countries however – like Germany – some filtering is problematic for legal reasons; there ‘pre-censorship is forbidden by the constitution’.

User-end/client side filtering was therefore seen by many as the way forward – though this puts the responsibility often firmly on parents’ shoulders. Hence many argued that filtering methods need to be easy to install, use and handle.

Some contributors raised concerns about the low take-up of effective filtering software even when costs are marginal; some children’s NGOs (especially in the UK) are campaigning to have internet safety software pre-installed on PCs.

Where filtering has been felt to be complicated to use (e.g. in some schools) ‘users are put off and either don’t use it at all or just accept the manufacturer’s default and are then subsequently frustrated’ by over-blocking.

The range of content to be filtered out, blocked, or ‘banned’ mentioned was extensive and varied widely. Many contributors said there should be image and language recognition, and filters to prevent access to child abuse material, to messages with harmful content, hate speech, and racism. Others additionally listed harmful content such as cyber-bullying, xenophobia, fraud, identity theft/respecting intellectual property, and phishing, in addition to violence, nudity, smoking, alcohol consumption, drugs, eating patterns, and disclosure of personal information.

Several respondents referred to the fact that online multimedia (online TV, music, videos, podcasts etc) also require technological tools to detect harmful contents on these digital formats. One highlighted the need to ‘develop tools which could be used by everybody no matter the operating system installed in the computer’.

One respondent pointed to the ‘ongoing problem of social networking sites which set their profile defaults to public’ instead to private, meaning that ‘many users are not aware that their profile is public by default’.

One submission put their views bluntly; while acknowledging the usefulness of filtering etc for very young children; they argued ‘we do not consider this to be an important area for further support beyond 2008’.

2.7 Research on sociological issues and analysis of psychological effects of particularly of the harm to children on different kinds of harmful content can contribute to building knowledge about how to deal with these issues. Which are the subjects which should be addressed in these areas when conducting research?

Research evidence on harm is scant, and there was no shortage of suggestions identifying which aspects require further enquiry. Findings should be put to multiple uses. However, more than one respondent expressed the view that ‘research that is available on this subject dates quickly in line with rapidly changing use of technology by young people’; another proposes a ‘unified study carried out Europe-wide with a meaningful sample of children/adolescents... to obtain the true ‘picture’’. In other words, research ‘will probably always be more reactive than proactive’.

Above all, respondents wished to know more about the motivations of children who look for harmful content, how they develop a ‘rational and critical attitude’ to harmful content, what children are doing online, how we could best communicate with children, the location of being

‘offended’, to identify vulnerable internet groups, on addiction, what children and young people themselves define as harmful content, and which media content they consider to be harmful or unpleasant.

Relevant research findings would be ‘clearly helpful both to government and industry’, and to those working with children ‘who have been disturbed and distressed’ as part of their therapeutic interventions. A range of other stakeholders could benefit from the insights obtained, including teachers and parents.

Harmfulness also depends on age, and is therefore subject to change.

### 3.2.3 Questionnaire 3 - User-generated content and online communication

#### Introduction

Children and adults alike use online technologies for communication. It takes place in a number of different ways; through mobiles, e-mail exchange, sites which facilitate users to create profiles, virtual networks, image exchange sites, Instant Messaging Services, blogs, chats and peer-to-peer services, dating sites and other "social networking sites" and user interactive services. Amongst others, the risks for children using these features are grooming, disclosure of sensitive personal information/images, exposure to harmful content (pornography, sexual speech, violence etc) encouragement to harmful behaviour (e.g. happy slapping"), bullying and harassment.

Internet allows both children and adults to create their own content ("user-generated content") and make it accessible to other users through Internet or mobile phones. Children are particularly vulnerable as they more easily disclose sensitive personal data (information and images), they sometimes engage in behaviour that is risky to themselves and can quickly get out of hand. They can also get traumatic experiences when confronted with illegal and harmful content or conduct. In addition, their use is in some cases associated with copyright infringement.

There were **eight** questions to be answered.

Many themes addressed in the first two Questionnaires were carried over into this final one, with many respondents referring to earlier answers, or repeating elements thereof. One respondent wrote: 'with regards to the risks listed in questionnaire No. 3, it is very difficult to fight against those risks other than by educating parents and children as those risks are increasing and hard to monitor'.

3.1 Which are the best means of addressing these risks with the aim of child online protection, in particular grooming and bullying? Which stakeholders should be responsible for initiatives in this field, and what roles should they have (industry, media, governments, schools, NGOs etc)?

Given the limitations of technical solutions in addressing risks discussed earlier, there was a strong focus on education, in particular educating children to think critically. 'This education in values must be comprehensive, and start at home from a very young age, and continue in schools.'

Effective stakeholder cooperation was put forward as a way of alerting children to the positive as well as negative aspects, through education and targeted awareness campaigns.

This means that governments have a role to play in providing appropriate ICT and citizenship education. Parents too need education ('they are the first line of defence.... and it does not take miracles for the parents to learn to caution the children not to meet someone they met on the internet alone'). Civil society as a whole needs to spread the message and elicit vigilance.

Recommendations made therefore include educational programmes that are responsive and adaptive to technological change and user profiles; and for the setting up of internet helpdesks which children can access, with online operators.

A concern echoed in a number of submissions was, however, that industry should not devolve responsibility to others.

Measures that have been used in monitoring chat rooms for years may be usefully employed (monitoring, sensitising children). 'The dangers are not fundamentally new', but instead may take new forms as we 'open up new communication paths.'

Addressing the risks concerning user-generated content was said to require focusing on the similarities and differences between ‘real’ and ‘virtual’ communication which require further exploration.

However, one respondent said that ‘once again, it is the operators of the platforms who are primarily responsible for protecting against illegal content’, and all existing provisions apply.

One government youth protection agency proposed that operators be required to ensure as a minimum that:

- Users cannot be contacted against their will
- Competent contact persons are available for complaints
- Those who harass children or disseminate illegal content can be excluded effectively or personally prosecuted for violations
- ‘Intelligent’ technical tools are used to detect assaults and illegal content.

3.2 Can you name further, not listed risks or further potentially dangerous forms of communication? Which are the best means and ways of addressing them?

One contributor expressed the sentiments running through many contributions, when they wrote that they do ‘not see communication per se as dangerous, but see it as an important element of children’s play, social development and identity construction.’ It is the risk behaviour that should be focused on. The advantage of general media education and promoting critical thinking is ‘that the method works for existing risks and threats as well as for issues that may be considered harmful in the future’.

Interactive gaming and its overlap with gambling, fraudulent services, material of a sectarian, xenophobic, bigot or hooligan nature, iTunes used as a bullying device, publishing personal data and pictures, suicide sites, encouragement of anorexia, the evolution of some social networking sites to ‘popularity contest’ sites, and identity theft were mentioned as current and future additional risks. Exposure to extreme ideological groups and ideas was identified as another risk, one specifying ‘online terrorists and criminals recruiting’.

Because of the nature of the question, there were many responses, each often focusing on a number of additional potential future risks.

Some of the responses talked about broader themes which have the potential for more long-term consideration. One stressed that there is a ‘negative effect that can arise from the use of on-line technologies for generating and maintaining emotional relationships’, pointing to often early and over-sexualised relationships that can occur. Another lamented the effects of such communication on language development and its resulting decline in offline written work and good spelling.

One response said that ‘seeking to identify the sort of services which users will be using in 2008 and beyond is probably a fruitless exercise.’ Another felt that the question was ‘technology-led’ and proposed research to discover the actual experiences of children.

3.3. Which role could education have in empowering children to deal appropriately with harmful and illegal user-generated content? Should such issues be integrated into school curricula? If so, which would be the best ways of doing so?

There was a broad consensus that awareness campaigns should be addressing school children, and that these issues should form an integral part of educational curricula. Guidelines for

teachers are necessary. Children need to be made aware that there is a code of ethics associated with communicating.

Many stated that education on dealing with harmful and illegal user-generated content should be included in citizenship or media literacy classes. Such content should be repeated and updated, and taught in an age-appropriate manner, and indeed be approached right across the curriculum.

Educators should be role models who can be approached and who can discuss with children situations that they may or might have encountered.

Several respondents pointed to the gap between school education and the reality of using the media at home; this needs to be addressed.

One minority view expressed was that ‘computer teachers’ should be responsible for relevant lessons and seminars; another believed that it is important to ‘focus on the topic, not so much on the media’.

3.4	Should the media take an active part in the awareness-raising in this sphere and in what way?
-----	---

Here, many respondents pointed to answers to Questions 2.3 and 2.5 in particular.

There was a broad consensus that ‘the media’ should take an active part – but there was a wide divergence concerning the actual meaning of ‘media’, and on the ways in which the media could play an active part in awareness raising.

‘Traditional media’ like TV and radio, cinema shows, newspapers, chat shows, and current affairs programmes were mentioned alongside on-line communication providers. Media is clearly a much fragmented stakeholder group and this needs to be reflected in multi-stakeholder partnerships, so as not to over-rely on a particular media sector.

Methods and approaches to awareness raising reflected this fragmentation, with a multitude of suggestions made. There was emphasis on using different media so as to reach different target audiences.

As regards children and young people as target audiences, dissemination of safety messages should target them where they are in terms of communication methods, as well as involve them in the production of such messages to make them relevant. Providers of on-line communication services were asked to run safety campaigns to warn children and young people of the risks they face when communicating on-line.

Parents and educators, on the other hand, were believed to benefit more from articles in newspapers as a possible vehicle for communicating this message to adults, alongside chat shows and current affairs programmes on radio and TV.

Several respondents proposed awareness raising methods addressing the whole family as multiple audiences, potentially through, for example, advertising campaigns providing messages for these audiences, including during children’s TV programmes and in cinemas. One contributor explicitly proposed the traditional ‘soap’ TV programmes to encompass storylines portraying key messages for both children and parents. Another suggested that public talks should be offered to parents, and information leaflets be distributed from schools to all their families.

3.5 A central element for the Safer Internet plus Programme in making Internet safer for children has been to support an international network of awareness nodes which promote public campaigns informing the public of the risks linked to the use of online technologies and on safeguard measures. In your opinion, is this the most appropriate way of dealing with communication risks and user-generated content beyond 2008? If so, please indicate in what ways this line of action can be strengthened.

There was broad and overwhelming support for the continuation of the international network of awareness nodes (INSAFE). More joined up thinking, however, was suggested, with greater multi-stakeholder involvement, and with more collaboration between schools, government departments, the media, charities and industry.

Again, many referred to earlier answers in Questionnaire 2. A number of ways of strengthening this work were suggested:

- focus on educating parents and teachers
- develop support networks to deal with online communication risks
- more direct regulation of service providers by governments
- increasing the budgets and securing support from national governments and industry
- ‘An understanding of impact is crucial’ – i.e. more effective measurements
- Mass media are crucial
- Share experiences and expertise via INSAFE network
- An ethical and safe culture among Internet users needs to be promoted internationally
- Higher Education Institutions should be part of this awareness work
- An international network of awareness nodes
- Have a common domain name
- Coordinate research more
- This network raises visibility
- Review what has worked so far
- Create minimum standards of platforms
- Develop stronger industry self-regulation codes and agreement of minimum standards
- Closer collaboration with government authorities

3.6 Development of efficient technologies can help to make the use of the online communication safer (e.g. monitoring social networking sites, age verification systems etc). Which are the subjects which should be addressed when supporting the development of technologies within this field?

Respondents came up with a long list of subjects to be addressed in developing communication technologies. Some stressed a more holistic approach, others mentioned particular issues:

- Creating a global websites-rating system
- Age verification was mentioned many times
- Measures have to be transparent to the users
- Parental, easy to use, controls
- Technological tools which inform parents and others when illegal or harmful content has been detected; such tools which automatically send a report to hotlines and law enforcement agencies
- How the use of such communications invades the privacy of children
- How information can be traced and eradicated from the public domain
- Technological support combined with human moderation
- Media literacy

- Electronic identity – who has checked your website or web space, tracking, verification

3.7 Research on sociological issues concerning use of online technologies, particularly how children themselves perceive risks, how offenders use online technologies to get into contact with children, the effects of grooming and bullying on children, as well as analysis of effective awareness-raising methods, can help to understand better how trends, behaviours and risks evolve in the society and to formulate awareness-raising initiatives in this field. Which are the subjects which should be addressed in these areas when conducting research?

An enormous variety of research subjects emerged. Here are just a few:

- New and emerging threats like addiction
- Use of new channels and tools for disseminating illegal and harmful content
- Emerging behavioural patterns from use of social networks; emotional behaviour
- Effects of exposure of intimacy to a wide online audience unknown to the young person
- Infringement of copy rights
- Who are the victims?
- Identifying and combating deceit
- Cyber-bullying
- Children grooming other children
- Unified European study
- Effects of harmful content
- Self-control mechanisms

3.8 The legal situation concerning grooming online differs across the EU Member States. Which are the issues which should be addressed when harmonising legal provisions across the Member States?

There was no clear preference regarding harmonising the legal situation concerning the tackling of grooming across EU Member states. Some believe that legal specialists should be addressing this issue. ‘We need a common understanding of what illegal is.’ ‘There may be merit in the harmonisation of the law around grooming to facilitate implementation of enforcement measures across Europe.’ Emphasis should be on sharing good practice.

A number of respondents, including from government and industry bodies, proposed self-regulation, as well as prevention measures such as law enforcement operations (e.g. sting, and group sting) alongside awareness raising targeted to different groups.

There was a proposal to conduct a review of the effects of having a grooming offence in countries which have such legislation, and a comparative analysis of the legal situation in the EU Member States.

One respondent expressed the view that provision aimed at curbing grooming at pan-European level could ‘happily co-exist with a diversity of legal provisions’ at national level. Another argued for more ‘cooperation between Member States’.

‘The law needs to allow the stepping in before a child is hurt.’ ‘Grooming should be made an offence.’

Alongside grooming, it was suggested, the distribution of illegal ‘morphed’ images or ‘virtual child abuse’, and written ‘child pornography’ should be criminalised.

## 4 PART 2: REPORT FROM THE SAFER INTERNET FORUM 20-21 JUNE 2007

The 2007 Safer Internet Forum in Luxembourg was attended by around 125 participants from 29 countries, alongside more than 20 keynote speakers and nine staff team members from the European Commission service in charge of the *Safer Internet plus* programme (DG Information Society/Unit E6).

Participants came from national awareness nodes, hotlines, non-governmental organisations, academic institutions, various types of industry, law enforcement, governments from EU and Non-EU member states and other interest groups.

During the first day of the Forum meeting, three **Thematic Workshops** were held, each consisting of four main sessions spanning the whole day. Speakers' presentations are published on the website:

[http://ec.europa.eu/information\\_society/activities/sip/si\\_forum/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/si_forum/index_en.htm)

Each workshop had a dedicated rapporteur who later presented the key points and summaries on Day Two, alongside summary and preliminary conclusions of the online public consultation by the author of this report. To enable the workshop rapporteurs to reflect the variety and depth of floor contributions made, many participants generously completed a form summarising their interventions and observations. These provided additional valuable information<sup>10</sup>. Below, there is a summary of the main conclusions and recommendations formulated in each of the three workshops. The individual rapporteurs' full workshop reports are available will also be published on the *Safer Internet plus* website:

[http://ec.europa.eu/information\\_society/activities/sip/si\\_forum/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/si_forum/index_en.htm)

---

<sup>10</sup> For example, one government representative wrote: "I did not want to make any intervention, just learn about what is going on and where the main problems are." One senior media representative commented that there is a 'jungle of ideas' with many good initiatives, "but what is still missing is a clear view on what a 'safe Internet site' is, and a code of conduct".

## **4.1 Workshop 1 – Online-related sexual abuse of children, with a special focus on the process of grooming and the consequences for children**

Chair: **Richard Swetenham**, Safer Internet *plus*

Rapporteur: **Ionel Ghiassi Razavi Stancu**

Number of participants: 26

Countries represented: AT BE DE ES FI FR GB GR IE IT LU MT NL NO PL RO SE SI TR US

### **4.1.1 Themes and keynote speakers**

**Online-related sexual abuse of children** – introduction (Vernon Jones, Save the Children Europe/Denmark)

**How the issues are dealt with today** (Ethal Quayle, COPINE project, University of Cork)

**Identifying the needs for action: how should the issues be dealt with in the future?** (John Starnes, Norwegian National Criminal Investigation service)

**Solutions, relevant actors and their need for support** (Dawn Hold and Julie Hewitt, Children’s Service Practitioners from the E-Spy Project, NSPCC; John Carr, Chair of CHIS, UK).

### **4.1.2 Main conclusions**

- There was great optimism that the concerted efforts of stakeholders would continue to bring about positive and increasingly visible results in tackling online child sexual abuse. Very few points of disagreement were expressed, indicating a common vision and sense of urgency. The speed and effectiveness of counteracting mechanisms could be strengthened by sharing good and successful practice. Greater involvement by a more extensive range of stakeholders was considered essential.
- Types and methods of online child sexual abuse continue to broaden, with images no longer the sole kind of material. This reflects the diversification of activities of sexual abusers based on evolving technologies with the potential for grooming children via many devices.
- There is as yet no standardised meaning of the term ‘grooming’, especially where the abuse is ‘non-contact’. The UK definition is being used successfully by law enforcement there.
- Rapidly evolving and converging technologies bring with them new types of online behaviour and forms of risk/risk-seeking by children and young people. The increase in self-generated material is leading to the publication of more and arguably more aggressively presented personal information.
- A comprehensive approach continues to be favoured, with a stress on seeking combined solutions through: (a) improved education and awareness (b) better technology e.g. for age verification, improving and extending blocking measures, and (c) hotlines and awareness campaigns working more closely together.
- Gaps in legislation regarding issues such as online images and other forms of representations of child abuse, and counter-action in cases of physical sexual abuse following the online grooming, or a lack of understanding of existing legislation, can restrict actions by police and other stakeholders. While legislation in some countries is changing, process is slower in others; standardised legislation on some issues might be possible and desirable.
- Participants registered a strong concern that measures regarding online child abuse should not detract from other necessary actions such as against bullying, racism and discrimination.
- The mass media, at least in some nations, appear to have a reduced interest in online child abuse matters while continuing to portray dangers in one-sided ways (e.g. ‘stranger danger’).

### 4.1.3 Recommendations

#### ***Recommendations for actions***

The workshop proposed a range of actions at four different levels:

**Political level.** There were demands for the Council of Europe to make a statement on the sexual exploitation of children, and for the EC to move the tackling of child sexual abuse higher up the European political agenda, to encourage governments to be informed on the subjects of online grooming and collaborate with each other and take necessary actions.

**Education and awareness.** Education and awareness campaigns in the media should go hand in hand, and empower children and adults themselves to be able to take and disseminate preventive and educational measures.

**Stakeholders.** The EC was asked to strengthen stakeholder cooperation, e.g. by promoting and financially supporting joint projects as models of good practice, facilitating further professional networking and training (including for mass media workers), and supporting the work of NGOs. Practical measures proposed included: buying the copyright to materials dealing with online related sexual exploitation/abuse of children, and making them freely available to stakeholders; seeking the collaboration for enhanced use of blocking systems by ISPs at European level, with legislative support where necessary; and creating a general list of websites disseminating online child abuse material, again with the aim of facilitating blocking at the European level.

**Technology.** There should be support for the development of software to trace, analyse and block websites disseminating online child abuse material, and to support the development and use of tighter age identification systems. The EC was also asked to participate in developing websites with good and attractive content for children as a positive preventive measure.

#### ***Recommendations for research***

Five areas for research were identified, incl. psycho-social, quantitative and technical aspects.

**Offenders and grooming behaviour** – moving from accessing images of child abuse to grooming; typology/profiling online sexual abusers; which types of websites attract both children and sexual predators; qualitative research.

**Children** – the psycho-social impact on children of online situations, ranging from accessing offensive images to being abused, including young people's own perceptions; the relationship between young people's sexuality and online grooming; profiling of risk-taking online behaviour by different groups of children; reasons for not disclosing abuse; and children's understanding of content globalisation and its ongoing availability on the internet.

**Family, parenting, personal histories** – how attitudes towards strangers have changed between different generations; the relationship between the quality of parenting and grooming; and the (emerging) link between depression and grooming, in both abuser and abused.

**Facts and figures:** gathering robust statistics (nationally and Europe-wide) on online sexual abuse and grooming; comparative research e.g. on relevant legislation.

**Technical and procedural aspects** – e.g. children's use of technology such as web cameras and cell phones; technologies and procedures for victim identification and offenders' age verification; online undercover operation in chatrooms but avoiding the charge of 'entrapment'.

- In addition, there was a request to consider how online sexual abuse and ways of combating it are viewed from alternative perspectives including by civil liberty organisations.

## **4.2 Workshop 2 – Awareness-raising: Assessing the need for awareness-raising towards different target groups and increasing the effectiveness of such activities**

Chair: **Manuela Martra**, Safer Internet *plus*

Rapporteur:- **Prof. Wolfgang Kleinwaechter**

Number of participants: 44

Countries represented: AT AU BE BG DE ES FI FR GB GR IE LU LV MT NO PL PT RU TR

### **4.2.1 Themes and keynote speakers**

**Children’s use of online technologies** (Sonia Livingstone, LSE)

**Consequences for awareness-raising and how to reach the goal** (Janice Richardson, coordinator of INSAFE, the European network of Safer Internet Awareness Nodes co-funded by the Safer Internet programme)

**The role of awareness-raising in creating a safer online environment in the future** (Steven Carrick-Davies, Childnet International; Sandrine Gobert, communication agency Ligaris: The Help campaign; Johnny Lindqvist, Friends.se; Egbert Melten, Ogilvy; Joachim Kind, Klicksafe.de)

**Identifying the actors and actions** (Tanja Sterk, SAFE-SI, Slovenian awareness node; Peter Behrens, Klicksafe.de, German awareness node)

### **4.2.2 Main conclusions**

- There is no risk-free internet. The first priority to improve safety on the internet for children is to increase education and awareness about its downsides: children have to learn how to deal with risks; actions and campaigns need to target specific age groups.
- The level of media education, internet literacy, and awareness about threats and risks linked to internet use differ substantially between European countries, as do parental attitudes to controlling children’s online experiences. Tailored awareness raising approaches are needed to target different audiences.
- Technological developments – especially new generations of mobile end devices for communication and mobile broadband internet access – are leading to new global forms of social networking. User generated content networks are becoming integrated into the culture of young people; children’s capacity to be creative and innovative and discover new cyberspace territory in productive and constructive ways can be strengthened.
- The relationship between offline and online worlds is not yet well understood, for example the differences and similarities between offline and cyber bullying.
- Education systems and teachers play an important role in educating on internet use and its risks. Schools have done a good job so far, but education authorities, in particular ministries, could be more active as they appear currently to be mainly occupied with access and technical security and less with the educational and awareness issue.
- A combination of education and awareness raising measures, working in schools and with a wide range of media, enables children to deal with negative aspects in self confident and responsible ways. Innovative methods are needed to reflect the real and virtual spaces which children and young people inhabit, using their evolving languages to reach them.
- Institutions like schools, libraries, media, youth organisations, industry and regulators which deal directly or indirectly with children and have special responsibilities for the creation of frameworks for children’s internet use, are also target audiences for campaigns.

- Many stakeholder groups expressed a demand for content filtering mechanisms, including in languages other than English. Russian law permits filtering in four categories of illegal and harmful content.
- Large-scale public awareness campaigns (the EC's anti-tobacco or the Swedish anti-bullying campaigns etc) provide important lessons e.g. on how to reach young people, and measuring impact. Learning can also be facilitated at European level by sharing the growing range of good, innovative practices emerging from different countries.
- Multi-stakeholder partnerships can be highly effective. Successful collaboration is illustrated e.g. by a German TV clip produced with sponsorship of a private industry partner; it is a tool now being shared effectively across Europe.

#### 4.2.3 Recommendations

1. Further **research** on the safer internet should be more qualitative and comparative; issues such as the following need to be addressed:
  - What are the most urgent research gaps?
  - Which risks are a priority for further research? How can we develop more refined analyses of issues such as levels of danger?
  - How to identify the most vulnerable target groups
  - When risks turn into harm, what specifically are the harmful consequences?
  - How important is the broader context for the consequences of online communication?
  - How to research communication patterns among children themselves, and between children and adults, in particular parents and teachers
  - How to measure the level of trust in trans-generational communication
  - The differences in use between age groups, and between what users do and say they do online.
2. **Awareness-raising strategies** to reflect the 'children's agenda', not that of adults.
3. Awareness campaigns and programs to be developed for **specific target groups**, possibly based on a five-step approach: Knowledge (be aware), Approval (support for new behaviour), Intention (convince target of new behaviour), Practice (put new behaviour into practice), and Advocacy (encourage other to do the same).
4. Awareness nodes to build closer relationships with the press, radio and television.
5. **Good practices** from different countries to be shared more effectively across Europe.
6. Safer Internet Day to be public, highly visible events with dedicated awareness materials.
7. Teachers to combine education on internet use with developing an understanding of its risks, with appropriate support and training to fulfil this task.
8. To improve the understanding of the relationship between online and offline worlds with regard to risk.
9. To improve our understanding of the implications and consequences of the Web 2.0
10. To expand and broaden multi-stakeholder partnerships, including industry, whilst maintaining the independence and ethics of awareness nodes.
11. To engage and support parents by developing/improving their communication skills based on their existing knowledge, sensitising them to children's ideas, needs and aspirations.

### **4.3 Workshop 3 – The impact and consequences of convergence of online technologies**

Chair: **Evangelia Markidou**, Safer Internet *plus*

Rapporteur:- **Kenneth Bone**

Number of participants: 55

Countries represented: BE BG CA CY CZ DE DK ES FI FR GB IE IT LU MT NL PL SE TR US

#### **4.3.1 Themes and keynote speakers**

**New technologies – new uses? Status and emerging trends and technological developments**  
(Pekka Heikkinen, NOKIA)

**New technologies – new risks to children?** (Zoe Hilton, NSPCC; Chris Vleugels, Free University Brussels )

**Ahead of the future: possibilities for reducing and dealing with the risks** (Anne Clarke, ETSI)

**Identifying actors and actions: Research into risks** (Sonia Livingstone, EuKidsOnline, London School of Economics), **Social Networking Sites** (Rachel O'Connell, Bebo)

#### **4.3.2 Main conclusions**

- Technology convergence will continue as a business driven requirement, with rapid changes and developments, requiring of stakeholders an equally fast response and collaboration in providing new safety options.
- Content has evolved into standardised formats, providing digital convergence of content for consumption through various delivery methods. Mobile devices give access to a variety of audio-visual content and functionality.
- Children need to participate directly for stakeholders to be able to keep up with technological change and use. The Commission is considering ways of involving and is already consulting children.
- Convergence of technologies means children have more access points and therefore potentially also more access to support.
- To prevent adult material being accessed by children, effective age verification systems need to be deployed. A common agreement is needed on standardised, efficient and effective application of such methods by all relevant stakeholders.
- A combination of hardware and software methods, and awareness raising and education, can counter the threat of accessing ‘non-advisable content’.
- Users increasingly supply extensive personal profiles to public areas in order to personalise content, thus compromising privacy.
- Parents, held responsible for ensuring safety through technology, would benefit from easier application methodologies for security features. Many are unaware or unable to use access control tools and safe filters.
- Automated tools and manual monitoring are used by some service providers to monitor content; other industry representatives argue that large information flows make manual monitoring impossible. Both stress that awareness and education remain key to effective online security.
- One problem identified was that carriers being immune from responsibility and prosecution, means that they may not be putting enough effort into tackling the problem.
- A developing cross-industry group initiative is about to agree on a standard set of principles and values, resulting in the development of a common ‘trust mark’ for content.

- There is a debate over whether measures by industry stakeholders reflect an ‘enforcement of self regulation’; some recognise that stakeholders cannot be ‘forced to self-regulate’. Clear guidelines, standards and incentives for stakeholders to participate are needed. Industry and association representatives agreed that self-regulation only works where there is leadership.

### **4.3.3 Recommendations**

1. Identified research needs:
  - more data on types of child abuse incidents, methods and rates, to address the current knowledge gaps. All stakeholders to contribute existing research material, especially on access through mobile devices as opposed to so called fixed internet.
  - on children’s own reaction to regulations (filtering) and how they bypass restrictions.
  - on risk evolving into actual harm to children, how to track online incidents and how these impact or complement incidents of abuse through traditional methods.
  - Research to be structured into: Content: the child as recipient; Contact: the child as participant, and Conduct: the child as actor.
  - to help identify which children are vulnerable, with the help of social workers, psychologists, and specialists.
2. A distinction should be made between age groups when child audiences are targeted.
3. Current legislation does not allow the ‘interception’ of data. Manufacturers are to consider researching a hardware methodology for this.
4. The Commission’s new call for proposals should focus on parental under-use of access control and filtering systems.
5. The Commission can provide support in these areas: sharing information, disseminating available items, and promoting policies; and providing co-ordination between all those making a significant contribution; focused political leadership; and further support in existing fields where the Commission is active (e.g. hotlines, umbrella organizations).

## 5 Annex I – Contributors to the online consultation

List of contributors to the public online consultation (in alphabetical order); all original responses (by individuals and organisations) may be viewed and downloaded from the website [http://ec.europa.eu/information\\_society/activities/sip/public\\_consultation/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm).

1. 3 GROUP
2. ADICONSUM - ASSOCIAZIONE DIFESA CONSUMATORI E AMBIENTE
3. ADULLACT – ALLART PHILIPPE
4. ADULLACT - CHRISTOPHER MANN
5. AFA
6. AGENZIJA APPOGG
7. ANCHOR YOUTH CENTRE
8. ANEC
9. AOL
10. BITKOM
11. BOCATEL INVENT GMBH
12. BRITISH TELECOM
13. BULGARIAN HOTLINE
14. BUNDESKANZLERAMT
15. CCPAS - CHURCHES CHILD PROTECTION ADVISORY SERVICE
16. CEEP - EUROPEAN CENTRE OF ENTERPRISES WITH PUBLIC PARTICIPATION AND OF ENTERPRISES OF GENERAL ECONOMIC INTEREST
17. CEOP - CHILD EXPLOITATION AND ONLINE PROTECTION CENTRE
18. CHAMOIX JEAN-PIERRE
19. CHILD FOCUS
20. CHILDNET INTERNATIONAL
21. CHIS - UK CHILDREN'S CHARITIES' COALITION ON INTERNET SAFETY
22. CYBERETHICS - CYPRUS SAFER INTERNET AWARENESS NODE
23. CRIOC - RESEARCH AND INFORMATION CENTRE OF THE BELGIAN CONSUMER ORGANIZATIONS
24. DIGITALE CHANCEN
25. DZIEDZIC BEATA, PHD & GODEJORD PER ARNE
26. E.KAT.O. - HELLENIC CONSUMER ORGANIZATION
27. ELUAU MIRIAM
28. ETSI TCHF - TECHNICAL COMMITTEE OF EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
29. EU KIDS ONLINE
30. EUROISPA - EUROPEAN INTERNET SERVICES PROVIDERS ASSOCIATION
31. EUROPEAN SCHOOLNET
32. EXTREME MEDIA SOLUTIONS LTD.
33. FESNEAU
34. FOX INTERACTIVE MEDIA
35. FRANCE TELECOM GROUP
36. FSM - FREIWILLIGE SELBSTKONTROLLE MULTIMEDIA-DIENSTEANBIETER (VOLUNTARY SELF-MONITORING OF MULTIMEDIA SERVICE PROVIDERS)
37. FTC - U.S. FEDERAL TRADE COMMISSION
38. GREEN LEAGUE (FINLAND)
39. GSM EUROPE
40. HENNO JACQUES
41. HOME OFFICE - DEPARTMENT OF TRADE AND INDUSTRY
42. HOPWOOD KARL
43. INHOPE - INTERNET HOTLINE PROVIDERS
44. INTERNATIONAL INSTITUTE OF COMMUNICATIONS
45. INTERNET ADVISORY BOARD IRELAND
46. IPOS UNESCO IFAP (RUSSIA)
47. ISFE - THE INTERACTIVE SOFTWARE FEDERATION OF EUROPE
48. ISPA - THE INTERNET SERVICES PROVIDERS' ASSOCIATION (AUSTRIA)
49. ISPA – THE INTERNETSERVICES PROVIDERS' ASSOCIATION (UNITED KINGDOM)

50. ISPAI
51. IVD - INTERESSENVERBAND DES VIDEO- UND MEDIENFACHHANDELS IN DEUTSCHLAND
52. IWF - INTERNET WATCH FOUNDATION
53. JUGENDSCHUTZ.NET
54. KENT COUNTY COUNCIL
55. KEPKA - CONSUMERS' PROTECTION CENTRE
56. KJM - KOMMISSION FÜR JUGENDMEDIENSCHUTZ DER LANDESMEDIENANSTALTEN
57. KLICKSAFE.DE - GERMAN AWARENESS NODE
58. LAW SOCIETY OF SCOTLAND
59. LE FORUM DES DROITS SUR L'INTERNET
60. LIVERPOOL LAW SCHOOL
61. LIVINGSTONE SONIA AND MILLWOOD HARGRAVE ANDREA
62. LÖFFLER WILHELM
63. MEDIERÅDET FOR BØRN OG UNGE - DENMARK
64. MEDIERÅDET / SWEDISH MEDIA COUNCIL
65. MEDIAS 1992
66. MICROSOFT
67. N.E.O.I. (YOUNG EUROPEANS ACTIVE & ORGANISED - GREEK NGO)
68. NORTHERN HOTLINE
69. OCU (ORGANIZACIÓN DE CONSUMIDORES Z USUARIOS)
70. OFCOM - OFFICE OF COMMUNICATIONS
71. OUTERMEDIA GMBH
72. OVEA
73. PANEUROPEAN FRIENDS FOUNDATION
74. POLISH COMBINED NODE: NOBODY'S CHILDREN FOUNDATION & NASK
75. PROTEGELES
76. ROYAL COLLEGE OF NURSING
77. SAFERINTERNET.CZ
78. SAFETY WORLD WIDE WEB FOUNDATION ONLUS
79. SAFEWEB: THE CYPRUS HOTLINE
80. SAVE THE CHILDREN ITALIA ONLUS
81. SAVE THE CHILDREN NORWAY
82. STOPLINE
83. TELEFÓNICA
84. TELIA-SONERA
85. THUS PLC
86. T-MOBILE INTERNATIONAL
87. UNIVERSITÉ DES SCIENCES SOCIALES TOULOUSE I
88. VIEIRA NELSON
89. VISA EUROPE
90. VODAFONE GROUP
91. YAHOO! EUROPE

(91 responses; 2 further were non-public)

## 6 Annex II – Experts and rapporteurs

NB: Key speakers' presentations referred to will be available on [http://ec.europa.eu/information\\_society/activities/sip/si\\_forum/forum\\_june\\_2007/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/si_forum/forum_june_2007/index_en.htm)

### ***Workshop 1: Online-related sexual abuse of children, with a special focus on the process of grooming and the consequences for children***

**Vernon Jones**, MA, is a qualified social worker. He worked in child protection for several British local authorities with a specialisation in children who have been subjected to sexual abuse. He later went on to undertake assessment and therapeutic work with adolescent and adult males who had been convicted or were suspected of sexually abusing children. In 1997 he moved to Denmark where he worked as a social worker before joining Red Barnet, Save the Children Denmark in 2000. He has been responsible for developing programmes, has researched and practiced in protection of children from all forms of sexual abuse and exploitation, particularly concerning online-related issues. He is currently working within the Danish government task force on combating sexual abuse of children by Danish travelling sex offenders.

**Dr. Ethel Quayle** is a lecturer in the Department of Applied Psychology, University College Cork and a researcher and project director with the COPINE project. She trained as a clinical psychologist with a special interest in sexual offending and has focused for the last ten years on victimisation of children through Internet abuse images. Recent research has led to the development of a self-help website for offenders and the development of guidelines for working with young people who engage in problematic sexual behaviour in relation to the new technologies. She is co-author of "Child Pornography: An Internet Crime" (2003), "Only Pictures? Therapeutic Approaches with Internet offenders" (2006) and "Viewing Child Pornography on the Internet. Understanding the offence, managing the offender, helping the victims" (2005) and has published articles in academic and professional journals. The collaborative work on therapeutic approaches to Internet offenders, supported by funding from the EU Daphne Programme, has been adapted by the Home Office, UK. This has also led to the establishment of an accredited programme dedicated to this group. She is a member of the Home Office (UK) Internet Task Force.

**John Staale Starnes**, Police Superintendent, is in charge of the Child Sexual Exploitation Unit within the National Criminal Investigation Service (NCIS) in Norway. He has been engaged in investigations of child sexual abuse since 1993, and has also been seconded to the Interpol General Secretariat to support the international effort combating commercial exploitation of children. Currently Mr. Starnes is chairing the Interpol Commercial Exploitation and Trafficking in Children theme group, and also represents Norway as driver of the European Chief of Police task force initiative CIRCAMP (Cospol Internet Related Child Abusive Material Project) aimed at fighting commercial sexual exploitation of children.

**Dawn Holt** qualified as a social worker (CQSW) in 1988. She worked for Local Authority Social Services, Children and Families until 1997, the last 7 years as a senior practitioner dealing with complex child protection cases. Whilst working for Social Services she obtained a Masters Degree in Child Protection and the Advanced Award in Social Work. Ms Holt joined the NSPCC in 1997 as a Children's Services Practitioner for the West Yorkshire Specialist Investigation Service undertaking investigations and assessments where allegations and/or concerns had been raised involving professionals or those in positions of trust. During this time

she spent 5 years working jointly with the Police on a large scale historic abuse enquiry and as part of the enquiry set up an independent counselling service for victims/witnesses. Ms Holt was seconded to Project E-Spy at its conception in April 2005, focussing on influencing and developing the project as a model of good practice for working together to protect and prevent the abuse of children and young people via the Internet.

**Julie Hewitt** graduated from Leeds University in 1993 with an Honours Degree in Social Policy, before obtaining a Diploma in Social Work from Manchester University in 1996 and a Social Work Masters Degree in 2002. She worked as a Local Authority child protection social worker for 5 years before joining the NSPCC's Specialist Investigation Service covering the North West of England 7 years ago. This team specialised in undertaking independent child protection inquiries into allegations against professionals and people in a position of trust with children, and in cases involving multiple victims and/or perpetrators. Since November 2005 she has been seconded to Project Espy which is a joint venture between the NSPCC and Greater Manchester Police to develop and offer a holistic approach in the Abusive Images Investigation Unit.

**John Carr** John Carr is Secretary of the UK's Children's Charities' Coalition on Internet Safety. The focus of much of his work is on the "digital divide", seeking to ensure all children and young people can benefit from the opportunities presented by the new technologies. He has been Internet columnist for *Prospect* magazine and has written about the Internet for many renowned journals, both in the UK and overseas. In 2003 Mr Carr was named as one of the UK's 50 most influential people in the new media industries by *New Media Age*. In May, 2006, he was named by the *New Statesman* as one of 50 "Modern Heroes" related to helping to make the Internet safer for children. He was a member of the Board established to develop the UK's new national centre for online child protection, CEOP, he is a member of the Home Secretary's Internet Task Force and has been Board Member and Director of Internet Watch Foundation, the UK hotline. Mr Carr has presented to and been consulted by Governments, inter-governmental agencies, NGOs and technology companies all over the world and was a member of the European Commission's High Level Group developing the European Framework for Safer Mobile Use by Younger Teenagers and Children which was signed in February 2007.

## ***Workshop 2: Awareness-raising: Assessing the need for awareness-raising towards different target groups and increasing the effectiveness of such activities***

**Sonia Livingstone** holds a bachelor degree in psychology and a PhD in Social Psychology from Oxford University. She joined the LSE in 1990 and is Professor of Social Psychology in the Department of Media and Communications. She is author of eight books, and has published widely on the subject of media audiences, focusing on audience reception of diverse television genres. Her recent work concerns children, young people and the Internet, as part of a broader interest in the domestic, familial and educational contexts of new media access and use.

**Janice Richardson** has worked as a teacher, teacher-trainer, university lecturer and consultant respectively in Australia, France, Luxembourg and Belgium. She is the author of two books and many articles on the pedagogical use of ICT and the development of information literacy. In 2002, she led an editorial team at the Council of Europe to create an online Internet literacy manual. Ms Richardson moved to Brussels in 2004 to work with European Schoolnet, an umbrella organisation that runs educational portals and develops learning for schools, teachers and pupils. There she is the project manager of Insafe, the European Safer Internet network mandated by the European Commission to coordinate Internet safety awareness raising initiatives across Europe and beyond.

**Stephen Carrick-Davies** is since 2003 the Chief Executive Officer of Childnet International, a not-for profit organisation based in the UK and established in 1995. Childnet works with a wide range of young people and partners throughout the world in its mission to “help make the Internet a great and safe place for children.” He has worked at Childnet since 1998 and has during this time led the development of award-winning Internet education and awareness projects such as Childnet’s “Kidsmart”, “Jenny’s Story” and “Chatdanger” resources as well as the Childnet Awards and Academy programmes which reward young people who are developing outstanding Internet projects which directly benefit other children. Mr Carrick-Davies represents Childnet on a number of important bodies including The UK Government’s Home Office Task Force on Child Protection on the Internet and The British Educational Communications Technology Safe Use of the Internet Policy Group and Technology Committee. He is also on the Advisory Board of FOSI – the Family Online Safety Institute based in Washington DC. He has an honours degree from the University of London in Education and Communications, has 3 children and lives in South London.

**Sandrine Gobert** started her professional career in 1994 at Trilogie Consultants, an independent consultancy assisting US and European IT firms with their launch on the referent markets. She then joined Orlando, one of the first French web agencies linked to an IT financial holding (HOF) where she tackled Internet and merchant applications as a communication project manager. From 1997 to 2001, Sandrine piloted interactive projects for key institutional accounts like PricewaterhouseCoopers, Steelcase Strafor, Lotus, France Telecom or Renault as a consulting director at the agency.com network and TBWA group. From 2002 onward, she headed missions within TBWA Consulting & Design, the global design TBWA France agency, developing major brand identity programs, of which TGV and Corail visual and brand identity territories are a good example. She joined e-Topics, the interactive pole of the Ligaris group, in January 2007 as an Interactive expert and Account Director.

**Johnny Lindqvist** works as a lecturer at the organisation Friends in Sweden. He has been a lecturer for 6 years and visited over 200 schools all over Sweden. For the past 1,5 years he worked only with cyberbullying and questions regarding children's use of the Internet. Friends focus on preventative actions and educate both teachers and students in how to prevent bullying.

Before coming to Friends, Johnny Lindqvist worked as a teacher in a theatre for children and grown ups, as well as an actor and director with focus on children's theatre.

**Egbert Melten** is a Management Supervisor, Ogilvy & Mather advertising agency, Frankfurt. After his graduation at the Academy for Marketing Communication in Frankfurt, Egbert Melten started his career in advertising in 1982 at McCann-Erickson as a customer consultant. He has worked with branding of companies like Lingner & Fischer (nowadays Sara Lee), Eckes, Camel and Nestlé. Since 1995 Egbert Melten is at Ogilvy & Mather in Frankfurt as Management Supervisor and was in charge of different international and national brands, including Unilever (Lätta, becel, Du darfst), Nestlé (Vittel, LC1), Rotkaeppchen-Mumm wineries and brands of the Radeberger Group. Furthermore, Egbert Melten is active in the nature protection organisation WWF Germany, the LZG (Central Authority for Health Promotion) and the LMK (Central Authority for Media and Communication Rhineland-Palatinate).

**Joachim Kind** is a Head of Communication, Media and Communication Authority (LMK) Ludwigshafen since 2006 and spokesman for klicksafe.de, the German awareness node. In 2001-2005 he was a Managing Director in the Commission on Digital Access of the Director's Conference of German Media Authorities (DLM), Berlin. Since 1998 until 2001 he was a Spokesman Media Authority for Broadcasting (LPR) Ludwigshafen. In 1994-1998 he was a Head of Public Relations, European Law Foundation (ERA) Trier / Brussels. He has also been engaged in managing and scientific jobs in the academic world. Mr Kind holds a PhD in Communication and Linguistics, M.A. in English, French and Italian Linguistics and Literature, Certificate in Media and Mass Communication and Certificate in European Law. He also has been an intern at European Commission in Brussels, European Parliament, Strasbourg, United Nations Headquarter, New York, Varta South East Asia, Singapore.

**Tanja Sterk** is a research assistant at Faculty of Social Sciences, University of Ljubljana. In 2002 she graduated in Political Sciences – International Relations. She worked on international projects (EU 6<sup>th</sup> Framework IST projects) connected with information society (EPSINET, eUser, eInclusion). She coordinates the existing Slovenian Awareness Node SAFE-SI and has been working on the Awareness project since its launch in Slovenia in March 2005. In 2006 she was also involved in the process of establishing Slovenian hotline “Spletno oko”.

**Peter Behrens** has education in political science, German literature and education. From 1984 he was working as a scientific assistant at the University of Trier, in a project concerning private broadcasting. From 1988 he worked as a project coordinator in Company market and media research. From 1990 he dealt with protection of minors, research, Press- and public relations for the Central Authority for Media and Communication (LMK), Rhineland-Palatinate. From 2001 he is its head of department for media literacy/public access channels. His other tasks include: project coordinator “klicksafe.de”, directorate of Foundation Media Literacy Forum Southwest (MKFS), directorate of Media Education Research Association Southwest, directorate of Institute education public access channels (BZBM), Insafe Steering Committee member.

### ***Workshop 3: The impact and consequences of convergence of online technologies***

**Pekka Heikkinen** has a degree from the Technical University of Helsinki. He joined Nokia in 1999 and works currently for the Standardization and Industry Relations. His focus is on regulatory policy issues related to equipment and services. Mr Heikkinen is a chair of EICTA (European ICT and Consumer Electronics Industry Association) Mobile Terminal Group. Before joining Nokia he worked for Finnet, a telecommunications operator group, and before that for Alcatel and ITT.

**Zoë Hilton** (Dr) is a Policy Advisor for Safeguarding and Children's Rights at the NSPCC. Since joining the NSPCC in 2005, she has focussed upon child sexual abuse and safeguarding of vulnerable children. She has recently become the organisation's policy expert on a number of child protection related issues including on-line and other electronic media. Prior to joining the NSPCC, she researched and lectured in social policy at the Heriot-Watt University, where she also completed her PhD in Sociology and Criminology.

**Chris Vleugels** holds a Master Degree in Sociology from the Catholic University Leuven with specialization in Theoretical Sociology and Sociology of Culture and Education. He is a junior researcher at the research centre SMIT (Studies on Media, Information and Telecommunication), Free University Brussels where he is involved in the TIRO project (Teens and ICT: Risks and Opportunities). Within this project he combines his interests in qualitative research, sociology of youth and processes of socialization by conducting a qualitative field research on the use of ICT by teenagers. Other partners involved in this Belgian research project are the University of Antwerp (UA), Cellule Interfacultaire de Technology Assessment (CITA, University of Namur) and the Research Centre in Informatics and Law (CRID, University of Namur).

**Anne M Clarke** is one of Europe's leading experts on the impact of ICT on young children. For the past 6 years, she has been leading ETSI's work in defining the issues in this important area, and developing guidelines for the industry. As a result, young children are now seen as a significant sector of the European Information Society and other standards organisations are adopting ETSI's approach. For many years, Ms Clarke was part of the research staff of the Human Factors Department of Loughborough University, leading a number of international human factors research programmes funded by the European Commission, including advanced communications projects and a series of international conferences and projects looking at the longer term future of technology development. Ms Clarke is now an independent consultant to the telecommunications sector on human factors issues. Her work with ETSI, supported by Telefonica, has led to a number of publications and conference presentations on the impact of ICT on very young children. She currently leads ETSI Childaware Project, which aims to encourage ICT product and service providers to be aware of young child users. This project will define new guidelines for service providers whose services are used by young children. She is currently also a member of the permanent steering committee of the Human Factors in Telecommunications biennial series of conferences.

**Sonia Livingstone:** See CV under workshop 2

**Dr Rachel O'Connell's** experience includes more than 7 years of involvement in researching how various end-users use new and emerging technologies - and she has gone on to use this evidence base in the development of programmes designed to educate and empower children, young people and adults in various capacities (e.g. parents, teachers, social workers etc) with the tools, knowledge and skills to navigate the internet safely.

She has also been a key contributor to policy development with respect to Internet related issues in the UK, and most recently she has chaired the Public Awareness Group of the Home Secretary's Internet Task Force on Child Protection. In her capacity as chair of the Public Awareness Group Rachel facilitated a partnership approach between representatives from across the mobile and fixed internet industry, child welfare organisations, government, parent and teachers organisation to develop a web based programme of education on internet safety (see [www.internetsafetyzone.com](http://www.internetsafetyzone.com)).

In addition to holding a seat on the Internet Strategy Group at the Department for Education & Skills (DfES) in the UK, she has co-ordinated pan-European projects designed to address internet safety related issues, funded by the European Commission. Dr O'Connell has also been an advisor to the Council of Europe's, specialist media and communications policy group and has recently co-authored a book which addresses issues around human rights in the digital era.

### **CV of Dr Ute Navidi (overall rapporteur)**

Dr Ute Navidi was assigned by the European Commission – DG Information Society the following tasks:

- analysing the contributions received in response to the online public consultation on "Safer Internet and online technologies for children"
- acting as overall rapporteur for the 2007 Safer Internet Forum held in Luxembourg on 20-21 June 2007.

Navidi is a long-standing independent international expert for the European Commission's Safer Internet, Safer Internet *plus*, and Hotline programmes, and has worked on different evaluations, reviews, site visits to various European countries and as rapporteur.

She has a professional background in child welfare NGOs, including policy and practice regarding disabled children. As former UK Head of Policy at the children's charity ChildLine, she is knowledgeable about child sexual abuse, including about children who abuse other children, bullying, cyber-bullying, forms of violence, gender differences, substance abuse, and many other child-related issues. Currently Director of the children's charity London Play, she is leading an organisation that promotes and supports children and young people's outdoor play and leisure activities as a right under the UN Convention on the Rights of the Child, and combats discriminations based on racism, socio-economic circumstances, poverty, gender and age. She is the International Play Association's national representative (England Wales Northern Ireland) and IPA Vice President (elect) for the European region. She was the UK researcher/writer for a six-nation EU Research project on age discrimination of children in Europe's judicial systems.

Navidi has extensive and in-depth expertise regarding children's use of the internet and new communication technologies, mobiles phones, chat rooms, representations of child abuse, the grooming process, law enforcement methods, and awareness raising including media literacy and campaigns. This expertise was recognised by the Home Office which invited her to join the UK Government's Internet Task Force on Child Safety on the Internet where she was also involved in key sub-groups, including on developing industry guidelines and public awareness campaigns. She is a founder member of CHIS, the children's charities coalition on internet safety, former member of the Stop It Now! steering group, and spoke at an international experts' conference on mobile technologies and child protection in Japan. She advised the BBC on a

number of media campaigns and long-term scenario forecasting, and acted as consultant and advisor on several series of children's books (mainly for 6-16 year olds). She continues to have a high profile as public speaker and media spokesperson, in the UK and internationally, and writes, edits and researches for a wide range of media.

Ph.D. Birkbeck College, University of London (1996) 'Identity and racism in post-reunification Germany'; B.Sc. City University, London (Sociology and Economics, 1978); Diploma in Translation (DipTrans); Post-Graduate Professional Certificate in Management (Voluntary and Not-for-profit sectors) Open University Business School.

## ***CVs of workshop rapporteurs***

### **Ionel Ghiassi Razavi Stancu**

He received his license in Psychology from the State University of Bucharest. He worked in Romania, Macedonia, Kosovo, Albania with various national and international organisations such as Unicef, Save the Children, Center for Crisis Psychology, International Medical Corps. In 2003 - 2004 he acted as a Psychologist in 'Blue Iris' Clinic (Romania); in 2005 - 2006 he was Programme and Services Director in the Estuar Foundation (Romania) in the mental health sector.

His fields of specialisation cover domestic violence and child abuse, the work with abandoned and street children, refugees and migrants, the counselling of teenagers and young couples but also interventions in cases of post-traumatic stress disorders and psychogeriatrics related issues. His experience includes group and individual post-trauma counselling, trainings and consultancy, research, development of psycho-social training programmes, programme coordination, supervision and implementation of projects.

### **Prof. Wolfgang Kleinwächter, University of Aarhus**

Wolfgang Kleinwaechter is a Professor for International Communication Policy and Regulation at the Department for Media and Information Sciences of the University of Aarhus / Denmark.

He studied Communication, International Law and International Relations at the University of Leipzig. His Academic Teaching Experiences includes University of Leipzig, University of Tampere, American University, Washington, D.C and University of Oerebro.

He has been involved in Internet Governance issues since 1997 and participated in various capacities in all ICANN meetings since its first meeting in Singapore (1999). He was a member of ICANN Membership Information Task Force and was elected as member of the Steering Committee of At Large. In 2004 he was appointed by UN Secretary General Kofi Annan as a member of the UN Working Group on Internet Governance (WGIG). In 2006 he was appointed as "Special Adviser" to the Chair of the UN Internet Governance Forum (IGF).

He is a member of the International Council of the "International Association for Media and Communication Research" (IAMCR) and served as the president of the IAMCR Law Section between 1988 and 1998. He is the Co-Founder and Member of the Board of the Media City Leipzig e.V., Leipzig, Germany and of the ICANN Studienkreis.

He was Member of the Programme Committee for INET 2002, Internet Society, Washington D.C. and a Key-Note Speaker, Panelist, Moderator and Rapporteur of numerous international conferences on the Information Society, Information Law and Internet Governance.

His research work includes more than 100 international publications, including 5 books, on issues of Broadcasting Legislation, Global Information Society, Internet Governance and WSIS.

### **Kenneth Bone**

Kenneth Bone is the Principal of Seasus, a Malta based Internet Technology and Multimedia service provider.

He founded Seasus in 1998, while still reading a B.Sc. IT degree at the University of Malta. Since then, Seasus has matured into one of the local leaders in the industry and is now providing its services in several countries including the UK, US, Sweden, Norway, Italy, Holland and France.

In addition to his commitments at Seasus, Kenneth has also been invited as contributor at various conferences and served as a consultant to several boards and organisations, including the Organisation for Economic Co-operation and Development (OECD) in Paris.

Since 2005, he exclusively represented Malta as ICT expert in the United Nations framework of the World Summit Award 2005, a global initiative for selecting and promoting the best in e-Content and creativity.