



## **Comments of the Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, FSM e.V. (Voluntary Self-Monitoring of Multimedia Service Providers)**

### **Introduction**

The Voluntary Self-Monitoring of Multimedia Service Providers (FSM) is a registered association founded in 1997 by e-commerce alliances and companies. The members of the FSM share the opinion of the Federal Government and the Federal States that also the economy has to act in order to prevent the diffusion of content considered illegal and harmful to minors within the online-media. The FSM was founded for that reason.

The members of the FSM are e-commerce alliances and companies as well as mobile phone operators/companies. Under the umbrella of the FSM, the affiliated companies strive to further strengthen and ameliorate youth protection in Germany.

Together with eco, the registered association of German internet enterprises, the FSM is operating a hotline within the INHOPE-network and strives to communicate a responsible handling of online-media to the user of online services. Since many years, the FSM takes an active part in working within the Safer Internet Program. The FSM, eco and other stakeholders involved with projects supported by the Safer Internet Project are closely linked together. German hotlines and awareness nodes have established a joint advisory board in order to coordinate the efforts and to make cooperation more effective. The FSM is also part of the thematic network of the Youth Protection Round Table, which is also supported by the Safer Internet Program.

# **Questionnaire 1**

## **Fighting illegal content**

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

The problem of illegal content being accessible via the Internet will not vanish in the near future; therefore the pro-active fight will need to continue as well beyond the year 2008. The near past has rather shown that the amount of illegal content is on the rise. Accordingly, the average figures of reports being issued to the FSM-Hotline has been growing. Even though the FSM-Hotline only covers the domain of youth media protection, questions regarding other kind of illegal content or activity (fraud, copyright infringement etc.) are also being addressed to the FSM. The overall development therefore underlines the need to uphold and even strengthen past efforts to fight illegal content on the internet.

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

In the domain of youth media protection, the most alarming issue is amount of reports concerning child pornography. Moreover, all content which is potentially harmful to minors and content which implies other elements of crime should be dealt with. To give some examples, according to German youth media protection law, e.g. the following content is unconditionally illegal:

- Propaganda material and symbols of unconstitutional organisations,
- Public incitement and lies about Auschwitz,
- Encouraging or instructing anyone to commit criminal offences,
- Depictions of violence,
- Pornography involving children, animals or violence,
- Erotic images of minors,
- War glorification content,
- Violations of human dignity,

### **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.**

In the fight against illegal content on the internet governments should strengthen self-regulation which is carried out by the industry (notice and takedown procedures) and hotlines, which inform law enforcement agencies about illegal content. Furthermore co-and self-regulation mechanisms have proven to be very effective in the area of youth protection on the internet.

The national governments should as well initiate measures of cooperation between the different stakeholders (especially between self regulatory bodies/hotlines and law enforcement agencies) and should seek international cooperation in this matter. The past has shown that inquiries to identify potential offenders, e.g. concerning the

diffusion of child pornography, require not only the support of the industry and NGOs, but as well a tight international framework. Crucial information is often held by companies who maintain the technical framework of the internet. They have to take part in the process of investigation by delivering relevant information. This process has to be conducted in accordance with the rule of law, taking into account important fundamental rights of privacy and data protection.

The flow of information between self regulatory bodies/hotlines, which obtain reports about potential breaches of the law, and law enforcement agencies has to be strengthened and supported.

For the internet is a decentralised technique, the stakeholders have to participate on a global scale. Internationally operating law enforcement agencies have to be supported in order to be able to do the workload. The network of civilian hotlines (INHOPE) plays an important part to support the work of the police on the national and international level, as hotlines can give validated hints to police forces regarding the source of criminal content. The co-operation of national hotlines within an international framework (INHOPE) renders possible that relevant information about criminal content is swiftly transmitted to the respective police force of the country of origin. Hotlines should therefore play an important role in the concept of fighting illegal content on the internet as well in the future.

Moreover, the tracking of online-content is impeded by the fact that registry information is often faked and criminal offenders remain anonymous. International measures and standards have to be developed in order to grant the accurate input of registry information.

**1.4A 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 civilian hotlines are a very effective measure to offer the public an opportunity to report illegal content. The hotlines then can give validated hints to the police forces. Figures of reports issued to the hotlines within the INHOPE-Network show that this opportunity is being used extensively. Given these facts, these hotlines must be upheld, strengthened and supported beyond 2008. The exchange of information within the INHOPE-Network is very vivid. In the last couple of years, the members of INHOPE have collected precious experience of how to address illegal content found on the web. Law enforcement agencies and hotlines should further strengthen cooperation by exchanging information in order to fight illegal content more effectively.

**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?**

Governments should endow law enforcement agencies and co-regulation bodies with the necessary resources in order to fight illegal content.

The industry has to support the investigative work of law enforcement agencies by promoting hotlines and swiftly issuing relevant information concerning the use of those technical resources of the internet which are controlled by the relevant company. In order to do so, it is necessary for the industry to have a clear legal framework under which conditions they can issue information to the police. This is not the case so far in some countries.

Only if law enforcement agencies, the industry, self- and co-regulation bodies and other NGOs work effectively together, the problem of illegal content can be successfully tackled.

**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?**

The reports issued to the FSM-Hotline in the past have shown that criminal offenders often host their websites in countries where law enforcement is not as effectively realised as in other countries. Moreover, the registry information of the relevant websites is often faked. The anonymity of the Internet is the main reason for the extensive diffusion of e.g. child pornography and the disability of law enforcement agencies to prosecute such offences. In the opinion of the FSM it would be an effective measure to ensure on an international level that the registry information is accurate.

The work within the INHOPE-framework has already shown that international cooperation of hotlines is an important issue to approach the problem of illegal content. By swift exchange of information, the hotlines deliver important hints to the police of the respective country. The hotlines operating within the INHOPE framework as well as their cooperation with police forces have to be further strengthened and extended.

**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?**

Technologies like user autonomous filtering systems and image recognition can be helpful tools in the fight against illegal content. They can also prevent the confrontation of juveniles with harmful content. However, technical tools can never be the sole solution, and they should be applied only in case they are useful and effective. Therefore, the FSM underlines that awareness raising measures and the teaching of media literacy are crucial in order to give parents the capacity to protect their children and to impede the diffusion of such content "via the conscience of the

user.” It is the conviction of the FSM that, at present, there is a lack of awareness among users of what is legal and what is not.

**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?**

By inspecting the ways of how offenders use the internet, measures can be conceived to fight these offences. Only if the means of offenders are fully understood, the effectiveness of possible counter measures can be evaluated in an appropriate way. Therefore, the experience gained by self-control bodies (hotlines) and law enforcement agencies, as regards application of technique and content, is precious information in order to find expedient ways to fight illegal content.

**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?**

In all EU Member States instruments exist, with which illegal content can be fought. A challenge surely is that there are also different definitions and understandings of illegal content. Nevertheless the FSM stands for the fact that one should discuss common definitions and also rough objectives on the European level. A harmonisation of political handling is not necessary however. Rather the cultural and social factors should not be ignored.

## **Questionnaire 2**

### **Fighting harmful content**

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.

**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.**

Given the rising number of reports issued to the FSM-Hotline, it is the conviction of the FSM that the fighting of harmful and illegal content is a crucial task, certainly as well beyond the year 2008. However not all potentially harmful content is illegal and requires fighting. Adult content offered by using access controls is legitimate and legal.

Dealing with potentially harmful content is a difficult task, bearing in mind that the classification of such content as illegal is very culture sensitive and therefore largely varies from country to country, considering also the different use of diverse age groups. Furthermore the means to effectively hinder the confrontation of minors with potentially harmful content or activity are very complex. Therefore it is very important to identify which type of content is potentially harmful to minors and requires access controls and further activities. These actions have to include the strengthening of media literacy of parents, teachers and minors. In the view of the FSM, the strengthening of media literacy is a key issue, for the internet can not be controlled fully by technical means, but by the aware, mindful and observant user. User autonomous filtering tools could be a supplement means to hinder harmful content, but they cannot substitute the teaching of a responsible and alert use of the internet.

**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.**

Again, all stakeholders have to work together in order to fight harmful content effectively. The industry has to further uphold and strengthen self-control mechanisms (notice and take-down procedures), which can react swiftly if harmful

content is sighted. The past has shown that hotlines are a successful measure to fight harmful content. Also, the flow of information between self-control bodies, hotlines and law enforcement agencies has to be strengthened.

The government should extensively promote the strengthening of media literacy. The responsible use of the internet and other new media has to be taught in school, but it seems that at present teachers as well as parents are not aware of the problems and important issues concerning the internet and other new media. New techniques like the internet or mobile communication will be omnipresent in the future lives of the children of today. It is thus imperative that the chances and the potential of these techniques as well as possible dangers are made an issue at schools.

Moreover, the industry and the media have to take responsibility within their scope of influence. Awareness raising campaigns and the support of self-control bodies are examples for actions that can and have already been taken by a considerable number of companies.

For the domain of search engines e.g., the FSM, the affiliated search engine providers and the German Agency for the Examination of Media for Young People have developed the so called BPJM-module. In a first step, internet content harmful to minors is indexed by the competent state authority in a constitutional procedure. In a second step, the indexed sites are implemented in the BPJM-module and used by the affiliated search engine providers. As a result, the indexed sites are not shown in the search results.

Additionally, together with the FSM and various companies, the German Government has recently started the project "A net for kids". With the financial support of the Government and the companies, the FSM will create a "Whitelist", a databank of websites suitable and adapted for kids, in order to provide a safe and interesting environment for kids to surf. The list is expected to contain several thousand websites, which can be implemented in youth protection software and operating systems.

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

The EU, national governments and the industry should initiate awareness raising campaigns in the media in order to educate and sensitise parents and juveniles for possible dangers associated with harmful content. The media has a crucial role when it comes to getting the attention of the population. Broadly based awareness raising campaigns could therefore contribute to the effective strengthening of media literacy.

### **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?**

As already mentioned, education should be integrated into school curricula as soon as possible. Schools in particular should act on pupils accordingly and educate

parents and guardians, who are often ignorant of the problems. Educationalists and experts have to work out resources and concepts for schools, internet and mobile phones should be integrated into classes. Teachers should address the important topics related to the internet in class, point out possible dangers and indicate appropriate solutions and ways to handle the problem.

A sound approach would be to elaborate specific aspects of the educational work at European level. European requirements for the member states to support schools and other public institutions in order to teach and convey the needed media literacy would effectively ameliorate protection of minors.

The FSM together with affiliated companies and the Children's Charity of Germany have successfully developed resources ("The internaut suitcase") for schools, addressing important issues of media-use.

**2.5A 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.**

In the view of the FSM, awareness raising is the key aspect in the fight against illegal and harmful content. Informing the public about risks and safeguard measures is thus of paramount importance and should be further strengthened and extended beyond 2008. Co-operation between the industry and other awareness nodes should be established, efforts should be bundled in order to boost the penetration of such measures. A high level of transparency is required as well as conveyance of consistent, simple, recognizable and uniform information.

**2.6 Efficient technologies can help to make the use of the Internet, mobile phones and game consoles safer for children to use (eg. 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?**

The implementation of filtering- or blocking-system on the access level (ISP) is problematic for legal reasons: in Germany, pre-censorship is forbidden by the constitution.

However, the application of different non-access-levelled youth protection programs by the user is possible and desirable. Promising filtering systems already exist for the internet, reading out preliminary labelled websites according to the labelling (e.g. ICRA/ICRA plus). International standards and criteria should be established, in order to allow a swift and effective development of such software. A thematic, uniform labelling of content similar to the Dutch KIJKWIJZER-system or the European PEGI-system would also help to increase the awareness and attention of parents. In

general, the use of clear-cut, easily perceivable symbols is desirable to reach the needed transparency for parents and children.

Additionally, in Germany the law demands so called age verification systems for certain content (e.g. pornography). The requirements for such systems to be in accordance with the law are very high and represent an apt measure to protect children from harmful content.

**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?**

It is important to clearly identify the virtual problems in a first step. In many cases, the media covers single cases in a one-sided, biased way. However, reliable research has shown that the issue of harmful content and the respective interplay of cause and effect are very complex issues, which have to be examined further. Without playing down the effects of harmful content, it must be stressed that grievances of society such as violence amongst juveniles are not singly caused by the media. Juveniles who deliberately consume harmful content might be a cause of other nuisances, but it is as well a symptom. Research in these areas has to be aware of the complex interrelations. The complexity of the situations also implies that solutions are rarely evident at first glance.

## **Questionnaire 3**

**User- generated content  
and online communication**

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.

**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)?**

As already stressed, awareness raising is a key issue to inform parents, teachers and children about possible risks. Such campaigns should be initiated by the government and supported by the industry. Additionally, media literacy has to be taught more extensively in schools (see above).

In the domain of user generated content, self control measures are the most promising way, for the amount of content is vast and growing and thus barely controllable through means of supervision.

**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?**

The internet will always generate new phenomena with characteristics without precedent. A good example is "Second Life", which has made the headlines recently because child pornographic content was uploaded and sexual acts conducted with child-avatars have been sighted. Therefore, the means of fighting such content also have to change accordingly. However, the need for awareness raising and teaching of media literacy is present irrespective of the manifestation of harmful content.

**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?**

As stressed at point 2.4, the integration of how to deal with harmful content, whether user-generated or not, is of paramount importance. Concerning user generated content, it is important to highlight that every individual plays an active role, for he or she can share his contents with all other users. Thus, every one has as well a responsibility for the introduced content, which implies certain social rules. These rules of behaviour must be promoted and taught in schools. Children must learn that e.g. the upload of extremely violent content cannot only be illegal, but can also harm others. The problem is that teachers are often ignorant of these problems. The government has to initiate measures in order to keep teachers and educationalists up to date.

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

See 2.3.

### **3.4 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.**

The arguments mentioned in 2.5 are also valid for user generated-content and communication risks. However, concerning user-generated content the operator of the platform should also take part in the awareness raising process by promoting social rules of behaviour and implementing self-control mechanisms.

### **3.5 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?**

For user generated content is always growing and changing, stiff technical solutions will not be successful. Monitoring social networking sites is desirable. However, while monitoring is realisable for e.g. chats, this might not be convertible in all cases, given the vast amount of communication and uploaded content on popular platforms. Thus, additionally other measures have to be put in place. Self-control mechanisms and social rules of conduct, which inform and integrate the users themselves to react to illegal and harmful content or grooming and bullying are a promising way to cover a larger amount of user generated content. Such mechanisms could be combined with platform internal "awards" or privileges for users who stand out for notifying unwanted content and incidents.

**3.6 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?**

For user generated content is a comparably recent development, the ways of how to control content are not yet fully clear. In a first step, research has to clearly identify the dangers. Web 2.0 platforms offer various ways for potential offenders to get the information they want. These ways have to be examined and according safeguard measures have to be conceived. As mentioned under 3.6., it seems that self-control mechanisms seem to be a good way to address the risks. Research should therefore as well concentrate on concepts of self-control.

**3.7 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?**

The creation of uniform standards and legal provision on an international level is desirable in order to facilitate law enforcement and prosecution. However, concerning e.g. grooming the major effort has to be made to prevent criminal offences which are set in motion by child grooming. Potential offenders of serious crimes as sexual abuse of children will not be stopped by regulations which forbid the establishing of contact or the deception of children in order to gain information. For this reason, on the European level it should be thought about how Member States can optimize their prosecution systems regarding grooming.

Children and juveniles have to be informed about the danger, so that their ingeniousness cannot be exploited. Operators of Web 2.0 platforms and chats have to clearly inform juvenile users about possible risks and provide social rules of behaviour (e.g. not to disclose private information). Additionally, teachers and parents as well have to be informed about the danger, so that they can provide the children with clear rules concerning the use of web 2.0 platforms or chats.

