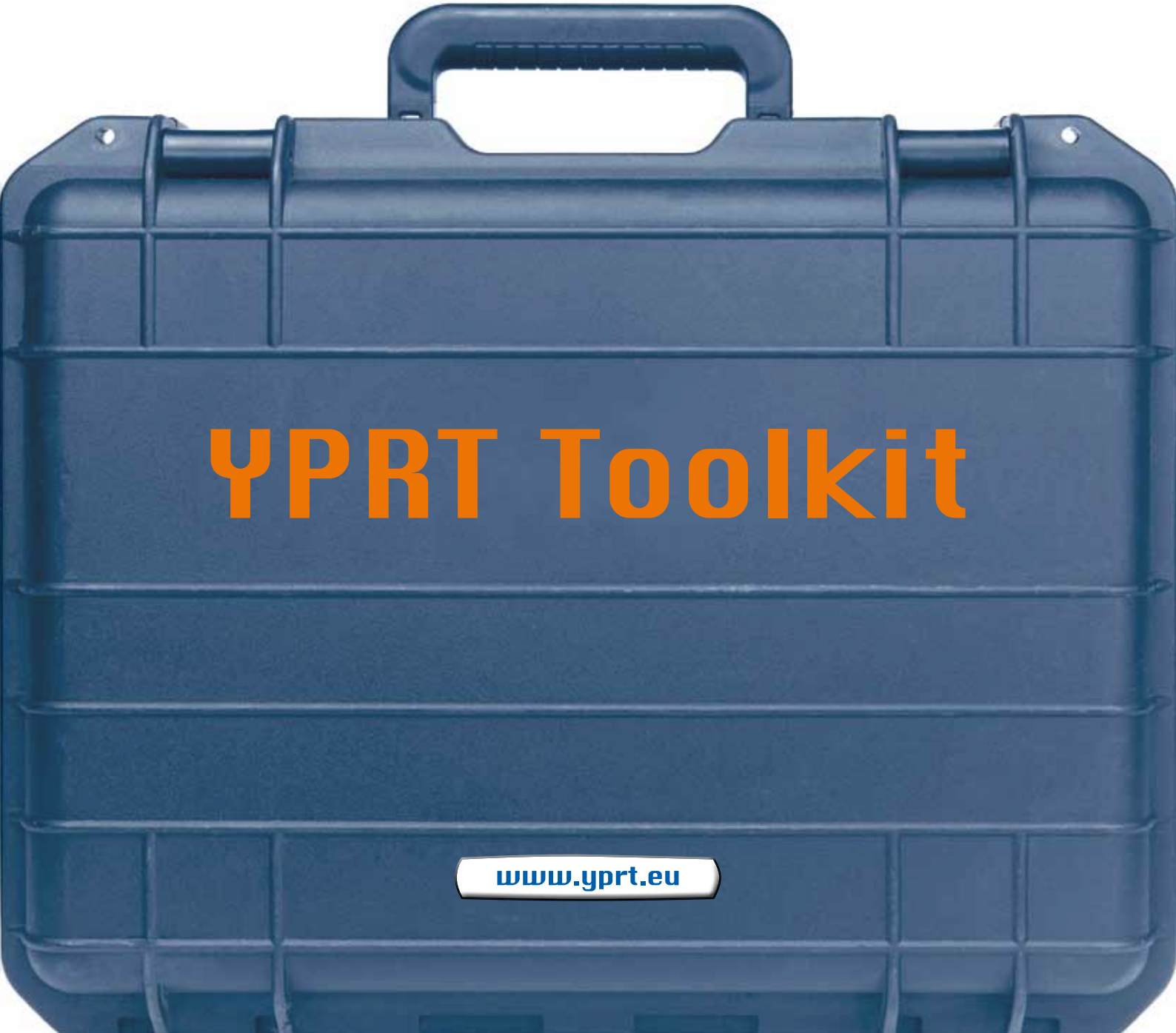
Youth Protection Roundtable



YPRT Toolkit

www.yprt.eu

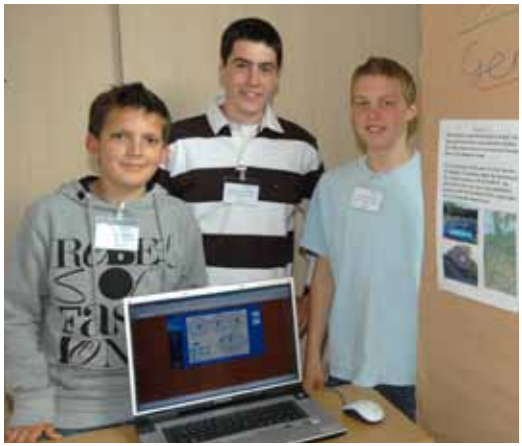
Index

Introduction to the YPRT Toolkit

This toolkit was developed by the Youth Protection Roundtable within the framework of the Safer Internet Programme of the European Commission.

The Youth Protection Roundtable was established in 2006, bringing together technical specialists and children's welfare experts with the purpose to develop the optimal mix of effective technology-enhanced strategies on the one hand and education-based strategies on the other hand to enable youths – and responsible adults in the case of minors – for a safe and secure use of the Internet. The 32 members from 13 European countries collaborated for 30 months convening for four meetings. To give the youth's voice a good hearing the so called Young Roundtable was established by the Youth Protection Roundtable.

Based on the project's findings and the insights to young people's online habits, the YPRT has elaborated this catalogue of ideas and suggestions to improve youth protection online.



Adopt, Adapt, Improve

The YPRT adopts this slogan coined by the Duke of Windsor when he introduced the idea of a Round Table in British Clublife back in 1927. He invited young men from different professions to discuss established practise in the light of new developments and to gain understanding of different views. This is what the YPRT has performed in face-to-face communication. Now, everybody who adopts the ideas and suggestions of the Toolkit, adapts them to his portfolio and tries to improve them is invited to join the virtual YPRT and to share his experience with other people perhaps differently minded at www.yprt.eu

Herbert Kubicek,
Scientific Director of Stiftung Digitale Chancen

Foreword

Taking part in the Information Society is essential for citizens of all age groups. The Internet provides huge opportunities to improve life for all users. It has positive effects on education, the working world and economic growth. Especially children and young people are well acquainted with its appliances and can benefit from its use tremendously, but they are also vulnerable. Risks and threats are coming along with this positive development, often parallel to those already existing in the offline world.

In order to solve the problem, technological measures can help. But however good they might get, it is never recommended to rely on technical tools completely. The best way to help children staying safe is to empower and educate them to avoid or deal with the risks. In delivering this objective, technologies can play a useful or supportive role, especially where younger children are concerned.

Therefore, the Youth Protection Roundtable in respect of

- the United Nations Convention on the Rights of the Child signed 1989
- Article 10 of the European Convention on Human Rights guaranteeing for the fundamental right to freedom of expression and to receive and impart information and ideas without interference by public authorities and regardless of frontiers;
- the Declaration on human rights and the rule of law in the information society, adopted by the Committee of Ministers on 13 May 2005, according to which member states should maintain and enhance legal and practical measures to prevent state and private censorship;
- the Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003;
- Recommendation Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment;
- Recommendation Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet;

- Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (Adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies);

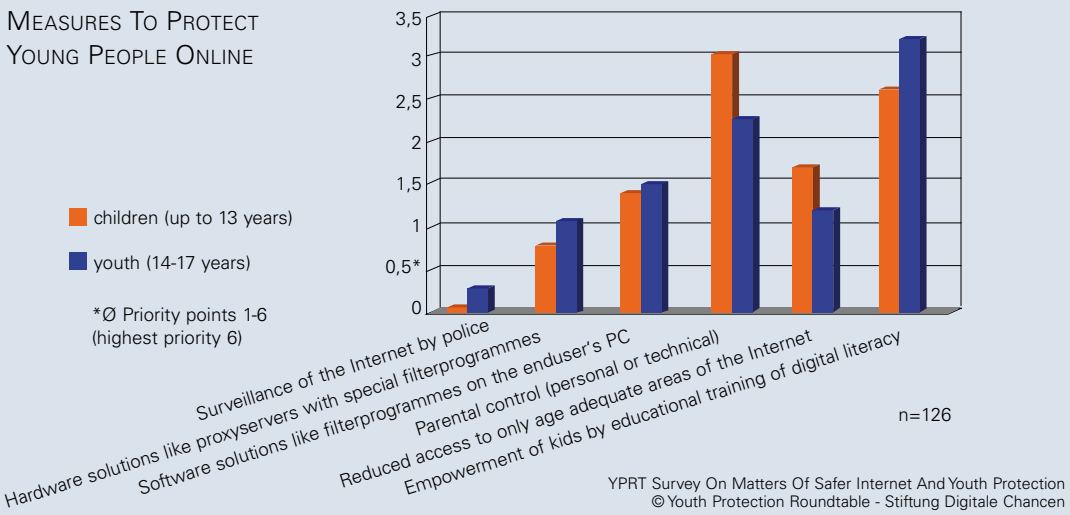
has developed a compilation of ideas and suggestions

- **for technical developments in respect of educational issues and**

- **for the use of filter technologies and educational measures in public and private areas.**

The YPRT Toolkit is a catalogue of non-binding references for the improvement of youth protection online, certainly not to be understood as obligatory.

The YPRT Toolkit shall support the various stakeholders involved in the processes of service and content provision, hardware and software development, parents' counselling, children's education, multipliers' training, and political decision making.



YPRT Survey On Matters Of Safer Internet And Youth Protection

The suggestions for technical developments in respect of educational issues

- inform providers and developers of the risks children and young people may encounter when using their online services, (Chapter A)
- give an overview on supportive technologies for youth protection currently available, (Chapter B)
- describe measures to bring supportive technologies into effect efficiently (e.g. that end-user based filters should be effective but also easy to use by persons in charge of minors) (Chapter C1-C4) and
- describe general conditions of youth protection (i. e. provide reference to national and international frameworks and legislation)

in order to achieve that technicians are able to pre-estimate the possible effects of newly developed end-user based technologies on children and youths.

The product-neutral suggestions for the use of filter technologies and educational measures in public and private areas

- inform pedagogical multipliers (teachers and carers) about the relation between particular online applications or products and related risks, (Chapter A)
- describe appropriate supportive technologies (Chapter B) and
- describe where additional educational measures are needed to enhance their potential for youth protection. (Chapter C2-C7)

The Youth Protection Roundtable made a great job starting a cross-sector dialogue putting together technical specialist, children's welfare specialist and Safer Internet project managers. The result of the effort of a collective work is valuable for people trying to empower and educate children based on the practical experience. The outcome of the project is valuable as a practical tool for implementation in real practice.

Ing. Pavel Vichtera, Saferinternet CZ project coordinator

A · Risks children and young people may encounter when using online services

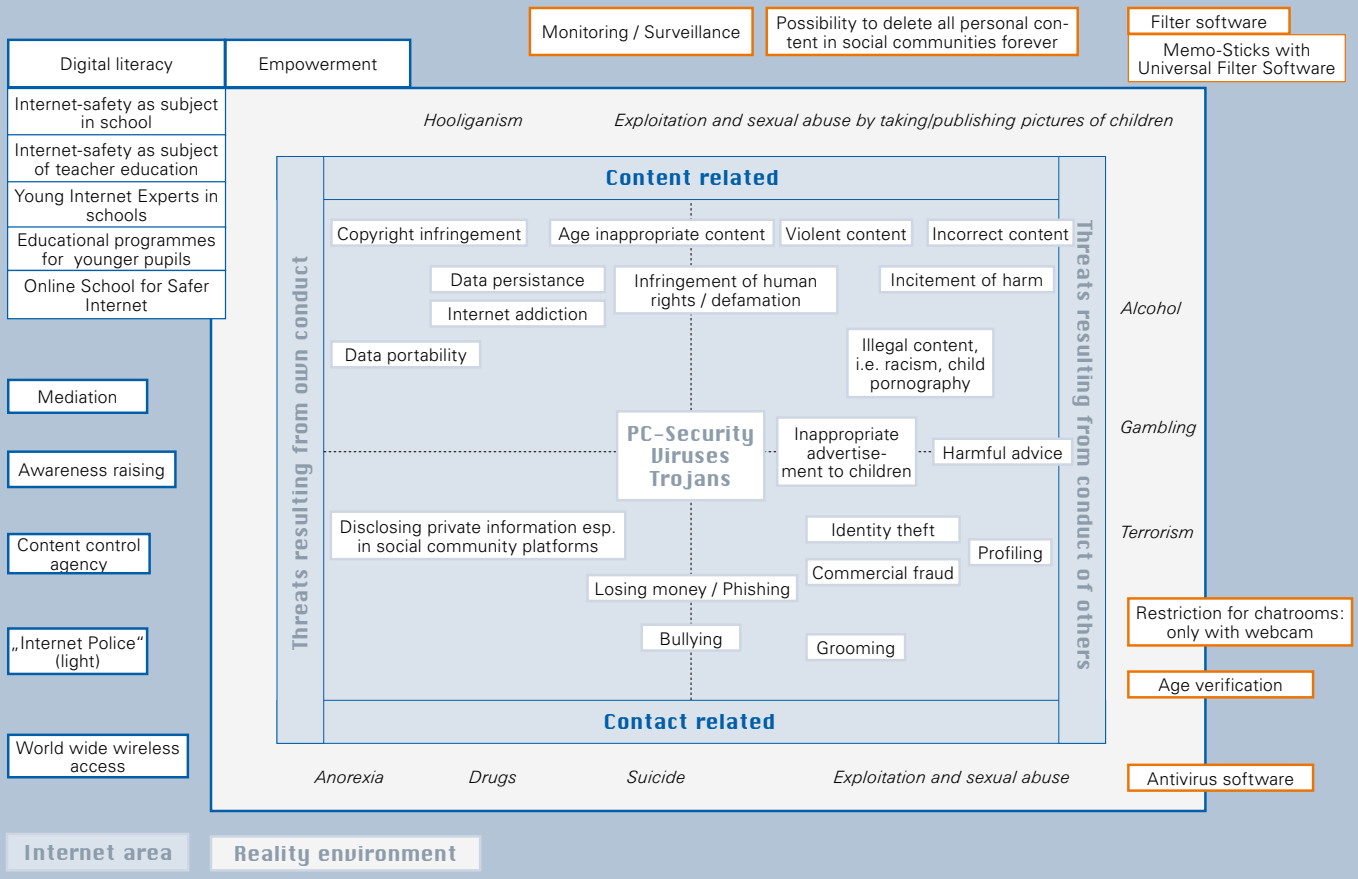
The Youth Protection Roundtable members have identified several risks and threats as relevant with regard to youth protection on the Internet. Although not all risks are of concern for all age groups, it is important to address all of them appropriately.

The risks were grouped along two dimensions, into those risks related to online content and those risks related to online contact. In both areas, some risks result from the users' own conduct, while other risks result from the conduct of other users. The location of some of the risks depends on whether one takes the perspective of the consumer of content or the producer of content, especially when it comes to user-generated content. This underlines the need of permeability between the areas of the Matrix. Furthermore it turns out that some risks are of relevance only to specific age groups of users and therefore can only be addressed by measures tailored to the user group's specific needs. According to these four dimensions relevant risks can be mapped.

My organisation particularly works with those people, who come from disadvantaged or disaffected backgrounds, so we were particularly interested in those young people, who don´t have all the other privileges some people have and maybe don´t get the same support and help in terms of dealings with the problems of Internet safety.

John Fisher, Citizens Online

Matrix of risks and threats



A 1 Risks related to online content

With regard to online content it is important to differentiate between illegal content and harmful content. There is no general European agreement on what is meant to be illegal, harmful or inappropriate content. Nevertheless some types of content, such as child pornography are outlawed nearly all over the world.

A 1.1 Age inappropriate content

The Internet provides a wealth of content for all groups of users. Mainstream interests are served as well as special interest groups. Nevertheless not all content should be accessible for children and youths. So it has to be carefully decided which content is appropriate to which age group. Special attention should be given to content that is not illegal in general but might harm younger users. Facing age inappropriate content like adult pornography might especially harm younger children when exposed to it unintentionally. The risk of facing age inappropriate content can result from the user's own conduct when searching for it deliberately as well as stumbling across it without intending to. Content that is not appropriate for all age groups might be provided for commercial reasons but can also be generated by the users themselves. Access to the former might be restricted to closed user groups only, while user generated content is mostly publicly available and needs therefore special attention. Since nowadays a high percentage of children and youths have a mobile phone with multimedia functionalities and access to the Internet at their fingertips, it must also be considered that they might access age inappropriate content when being on their own and not having an adult for guidance at their side. Mobile devices also enable children to produce their own digital content in any life situation thus contributing to the increasing number of user generated content.

A 1.2 Violent content

Violent content is another kind of age inappropriate content. The effect violent content has on the viewer largely depends on the age of the viewer, his or her habits of consuming Internet content and the social environment. Especially younger children should be protected from stumbling across violent content. It should also be prevented that they deliberately try to access content they are not allowed to see or buy on other media or in shops. An additional focus should be put on user generated content, particularly because children and youths might be producers and publishers of violent content not being aware of the harm this content could do to others.

Youth protection in the (online) media and the self regulatory approach play an important role in the work of eco for more than ten years, particularly by running a hotline to fight illegal content and content harmful to minors as well as being INHOPE (funding) member and being involved in several other activities in regard to youth protection and self regulation e.g. being point of presence for ICRADeutschland/fosi.

Alexandra Koch, eco Verband der deutschen Internetwirtschaft

A 1.3 Illegal content, i.e. racism, child pornography

The type of content classified as illegal, depends foremost on national law albeit some type of content is outlawed in most countries. Nevertheless illegal content is available and can be accessed unintentionally but also deliberately by children and youths. Attention should also be paid to children and youths as victims of illegal content, e.g. by taking and publishing child abuse pictures or videos.

A 1.4 Incorrect content

The risk to face incorrect content, f. e. within Wikipedia or as an advertisement of fake products is primarily related to the conduct of other users and is multiplied by the increasing number of Web 2.0 appliances where the correctness is at the most controlled by the users themselves but not by an editor. Biased content, i.e. content deliberately designed to transport a certain message, might also be taken for true by inexperienced young users.

A 1.5 Incitement of harm

There are many sites on the web inciting users to harm themselves, e.g. websites promoting suicide, anorexia or sectarianism. With Web 2.0 and the increasing possibilities to publish a user's own content, the risk of being exposed to content inciting harm is growing. In particular children and youths are in many cases not able to make a realistic assessment of the risks arising from following the instructions given in such websites.

A 1.6 Infringement of human rights / defamation

In the anonymity of the web, propaganda against certain population groups or individuals can easily be widespread. In addition one can presume that people act differently online where they must not face the reaction of their counterparts or victims directly and therefore are not immediately confronted with the consequences of their conduct. Thus the risk of infringement of human rights and being victim of defamation is much more likely to happen online than in reality. In addition, defamatory content is harmful to children and young people whose opinion might be influenced by misleading information.

A 1.7 Inappropriate advertisement and marketing to children

Inappropriate advertisement means the risks of receiving or being exposed to advertisement for products and/or services that are inappropriate to children like cosmetic surgery. The more users give away private information, i.e. name, age or gender, the more likely they are to receive advertisement or to be asked to participate in lotteries. Since children are in many cases not aware of the consequences of typing their names into forms and boxes on the web, they are profoundly at risk. Considering the high penetration rate of mobile phones among children and youths attention should also be paid to this additional channel for the dissemination of advertisement.

A 1.8 Data persistence

Content once published on the web can spread rapidly around the world. Especially children and youths are not aware of the short-term and long-term consequences and often publish texts and pictures they do not want to be publicly available later. Since it is impossible to delete this information totally later on, the risk of data persistence is in particular relevant to imprudent younger people.

A 1.9 Data portability

Data deliberately stored on a server or a platform can easily be transferred to innumerable other servers. People who are not aware of that fact might easily lose their privacy. Even if younger people are likely to know a lot about the technical possibilities of the web, admittedly most of them do not have the ability to roughly estimate the consequences when their private data are mingled with other data about their own person.

A 1.10 Copyright infringement

Copyright infringement is a risk mostly related to the conduct of the users themselves. Irrespective of the fact whether the copyright of others is infringed deliberately or undeliberately, the infringement is an economical fraud for the holder and puts the violator in risk of penalty.

A 2 Risks related to online contact

A 2.1 Harmful advice

Forums, blogs or other contact related areas of the Internet provide a platform for the exchange of advice between users. This could be valuable assistance but might also ease getting in touch with inappropriate or even more risky advisors. The risk of receiving harmful advice for children and youths occurs more often in social community platforms or other Web 2.0 appliances than on regular websites.

A 2.2 Internet addiction

As people spend more time online, the risk of getting addicted to the use of the Internet is growing. In particular young people are at risks of not being able to switch off the computer. Therefore this risk is first and foremost related to one's own conduct.

A 2.3 Identity theft

Getting hold of and making intentionally use of other peoples' electronic identity (e.g. user name and password) with the purpose to cause commercial or other fraud to this person and to benefit thereof is called identity theft. Identity theft is a growing risk as the number of virtual identities is increasing with the number of people being online and in particular using personalised services.

A 2.4 Losing money / Phishing

Phishing means the process of harvesting bank details, in particular PINs and TANs, with the purpose to ransack other people's bank account. Younger people are more likely not to recognise a fake website and give away their bank details.

A 2.5 Commercial fraud

Commercial fraud happens when sellers pretend to sell goods or services, which after payment either do not show the promised attributes or are not delivered at all. It can also result from identity theft and from phishing. Another source of commercial fraud can be the selling of digital services, e.g. a ring tone, at an unreasonable and unfair price often bound to a permanent subscription to the service that was not intended by the buyer. Children and youths are in the majority of cases not aware of the consequences of such contracts concluded online.

A 2.6 Grooming

Paedophiles use the Internet as a means to contact children and young people concealing their adult identity. They often build their strategy on children's longing for friendship and familiarity. All areas of the Web providing platforms for personal contact and exchange are likely to provide a basis for grooming attacks. As mentioned before the mobile phone as an additional device to contact others and to access e. g. social community platforms should be taken into strong consideration especially because children look at their mobile phone as a particular part of their private life and are mostly on their own when using it. Thus the risk of being a victim of a grooming attack and then following a dangerous invitation is increased largely.

"Child on the Web" campaign, 2004, by Nobody's Children Foundation and VA Strategic Communications Agency

A 2.7 Bullying

Various types of bullying seem to be always part of young people's life. Bullying one another is certainly simplified by the Internet due to the anonymity the medium provides. Children and young people risk both being victim of bullying and being offender. Hence bullying is related to one's own conduct as well as to the conduct of others. Even though publishing content like defaming pictures can be part of bullying, the phenomenon is foremost related to online contact. As mentioned before multifunctional mobile phones are often the device in use for taking pictures with the intention to bully and then upload the pictures to the Internet or send them via MMS to others. In view of the high penetration rate among children and youths the mobile phone equipped with a digital camera is likely to make bullying easier.

A 2.8 Disclosing private information

Setting up a profile on a social community platform invites the user to disclose private information with the intent to present oneself to the community. Also in chat rooms and forums users may disclose private data to others, such as their address or telephone number. In particular young people are not able to foresee the consequences of publishing their private data. They are often not aware that a chat room is not a private but a public area.

A 2.9 Profiling

With the increasing number of profiles a person publishes on different platforms, the risk increases that personal data published on one platform are merged with those published on others or given away elsewhere, f.e. in polling or raffles. Thus profiles are created that allow to directly address the person with potentially unwanted content, services and advertisement. Profiling can be accomplished from the website where the personal data are displayed publicly, but more dangerous when profiles of users or parts of these are harvested from the database behind the website and sold out from the platform provider to third parties.

B · Overview on supportive technologies for youth protection available so far

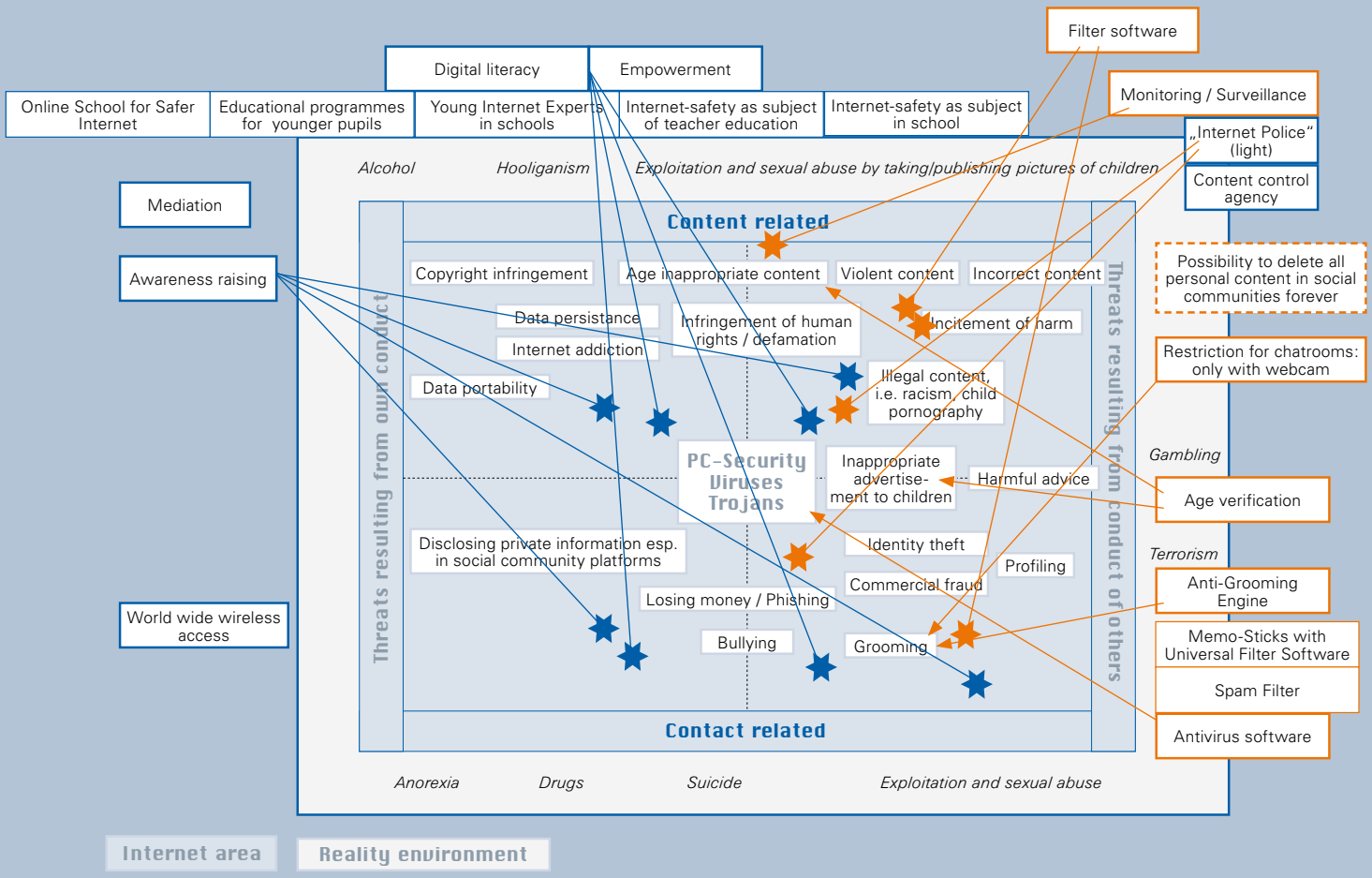
There are several technical tools available to address the risks and threats that might arise from the use of the Internet by children and youths. The YPRT has assessed recent research and findings in regards to the effectiveness of these tools. Also the YPRT members have assessed the following technical tools and estimated their effectiveness based on their own expertise. This was done in two steps of estimation, discussion and validation leading to a high degree of consensus.[1]

As a result, the YPRT members concluded that all technical tools need to be complemented by additional measures, i.e. empowerment through digital literacy, to be truly effective. Technical tools were therefore called supportive technologies for online youth protection in this toolkit.

The following version of the Matrix of risks and threats aims to demonstrate in which areas those technologies can be effective and thus support the efforts for youth protection on the Internet.

1 - Editorial note: The following section is based on the YPRT members' second estimation of effectiveness of tools, which was done during the discussions at the 4th Roundtable Meeting.

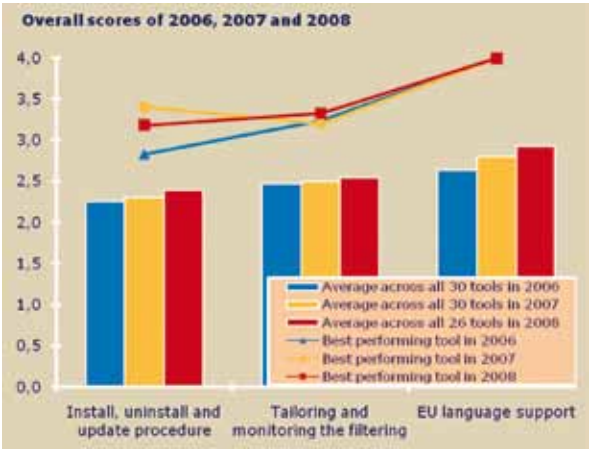
Matrix of risks and threats



B 1 Filter software

B 1.1 Description of filter software and its workflow

Filter software is an electronic facility that allows Internet data to be selected and sorted out. With regard to youth protection, filter software can protect children and young people from stumbling over or deliberately accessing harmful, illegal or inappropriate online content. It should be kept in mind that young people are very experienced technically and many filters can easily be circumvented. Filter programmes use either lists of rated content or analyse the content of web sites by semantic and statistical methods and work as a programme or module on an end-user device, on a central Internet access point like a proxy server or at the provider. Content can be rated by editorial classification (black and white lists), automatic classification (Keyword-Blocking) and content ratings checked by an independent agency, e.g. NICAM as administrator of PEGI or by the content provider himself, e.g. ICRA labelling. Most of the filter programmes integrate different content classification methods.[2]



The convenience of filtering solutions has improved between 2006 and 2008

© Deloitte 2008

2 - Source: http://www.lusi.lu/index.php?id=16&L=1

According to SIP Benchmark[3], filtering can be done at several levels. Filter software could be installed at the following places: at the end-user's PC, at a local server, at the Internet Service Provider, and elsewhere on the Internet, i.e. proxy-server based Internet filtering service. The technologies of the filter software include:

- Block a request to a URL that is listed in a vendor-provided blacklist (local blacklist check) or that is blacklisted on a vendor's or provider's site (remote blacklist check)
- Block a request to a URL that is not listed in a vendor-provided white list (local or remote white list check)
- Block a request to a URL that contains one or more keywords blacklisted by the user
- Block content that contains one or more keywords blacklisted by the user
- Erase pieces of content that resemble keywords blacklisted by the child carer
- Block a request to a URL with an ICRA label that is blacklisted by the user (remote ICRA check)
- Block a page that contains an ICRA label that is blacklisted by the user (local ICRA check)
- Disable specific applications (possibly during specified time intervals)
- Disable specific applications outside a time slot specified by the user
- Disable specific ports

The Family Online Safety Institute (FOSI) is an International, non-profit membership organisation that works to make the online world safer for kids and their families by identifying and promoting best practice, tools and methods in the field of online safety, that also respect free expression. Promoting better youth media protection is one of the core components of our strategy and through initiatives like the Youth Protection Roundtable we can share the thinking of our membership with the wider stakeholder community.

David Miles, European Director of the Family Online Safety Institute. March 2009

In order to achieve effective filtering rates, several technologies need to be combined.

It has to be taken into account that several side effects might come along with the process of filtering, not only in regard of freedom of expression and unintended censorship, but also with the problem of false positives and the negative impact on the infrastructure and the quality of services.

3 - Source Deloitte: http://www.sip-bench.eu/Reports2007/SIP%20Bench%202007%20-%20Synthesis%20Report.pdf

B 1.2 Effectiveness of filter software

Filter software is seen as a tool to solve many problems. In regard to the various risks listed in section A it becomes evident that the more concrete a type of content or a type of online conduct can be defined the more likely it is to be detected by filter software. Filter software therefore is less effective for less concretely definable content and online conduct.

Filter software is estimated to block about half of all websites with *age inappropriate* and *violent content*. With regard to *illegal content* filter software reaches a slightly higher degree of effectiveness. This is due to the fact that it can be more clearly defined what is illegal, and therefore illegal content can be more easily detected than other types of content and online conduct. In contrast to the same reason – definition of content – filter software must fail with regard to *incorrect content* for which effectiveness is seen as fairly low.

This is reinforced by the results filter software gains in regard to *inappropriate advertisement to children* and *incitement of harm*. Both types of content can be defined and therefore detected by filter software as content to be blocked in around one-third of all cases. It is more challenging to detect *harmful advice* often given in direct contact between users which leads to the estimation that filter software can affect only one out of seven cases of this risk. Also the online conduct of *grooming* can not be sufficiently detected by filter software; the experts anticipated detection in one out of five cases.

The risk of *disclosing private information*, which is also more likely to happen in the contact related areas of the Internet, can be addressed by filter software in only one out of ten cases according the experts' opinion.

Risks related to the own conduct of the user like *copyright infringement* and *Internet addiction* as well as those risks related to the conduct of other users like *identity theft* and *bullying* can be addressed by filter software only to a small degree. Also it was estimated that filter software can detect only one out of ten cases of *infringement of human rights and defamation*, which is related to both own conduct and conduct of others.

To the experts' opinion filter software can address a sixth part of cases of *commercial fraud* and *phishing*, but it tends to lower effectiveness for the risk of *profiling* and nearly no effectiveness in regard to risks like *data portability* and *data persistence*.

B 2 Monitoring and Surveillance

© Technogroup IT-Service GmbH

B 2.1 Description of monitoring and surveillance and its workflow

A monitoring system is based on software that monitors content and user's activity on the Internet and reports the results to a responsible person. It is an instrument to systematically search online content for a subsequent categorisation[4], e. g. into harmful or harmless content. Monitoring means to poll or check systems and services in an online environment automatically[5] with a filter mechanism and – to achieve more sensible and qualified results – followed by the review of the results by an expert who decides whether the content has to be filtered or taken down or not. Usually the review process is carried out with a random sampling of the scanned content. A monitoring system enables to review e. g. chat sessions, blog entries or the uploading and exchange of pictures. Technically it can be installed on the level of the Internet Service Provider (ISP) or the operator of an online service. In some cases monitoring and surveillance procedures are installed to review content before it is published online, while other monitoring procedures are based on the notice-and-take down approach, where online content is taken down after detection[6]. In regard to online communication, this approach can lead to the deletion or deactivation of users' profiles as soon as a violation of the code of conduct is reported or detected.

B 2.2 Effectiveness of monitoring and surveillance

By means of monitoring and surveillance the content of the Internet and the communication via the Internet can be reviewed to a certain extent. This might happen on various stages of the content storage and hosting as well as access providing process. In general monitoring and surveillance gain higher effectiveness than filter software alone. This result is based on the assumption that monitoring and surveillance both build the decision, whether online content should be taken down or not and online conduct should be filtered or not, on additional human review.

Thus monitoring and surveillance gain highest effectiveness in regard to *age inappropriate content* with more than half of all cases. The effectiveness for *violent content* and *illegal content* and also for *incitement of harm* is judged only slightly lower with two-fifth of all cases.

4 - Source: Wikipedia http://de.wikipedia.org/wiki/Webmonitoring
5 - Source: SiteScope193.138.212.37/SiteScope/docs/SiteScopeTerms.htm
6 - For example, the PEGI Online Safety Code makes it mandatory to have an effective alert system in place to be authorised to carry the PEGI online label.

Monitoring and surveillance were estimated to detect at least every third case of *harmful advice, infringement of human rights/defamation, inappropriate advertisement to children* and *grooming*.

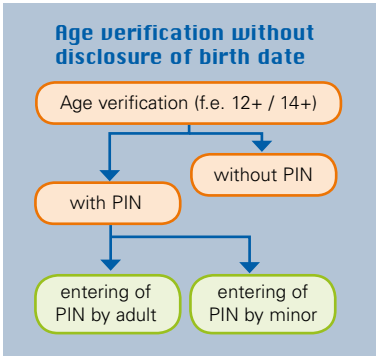
While it is assumed that monitoring and surveillance can achieve the detection of more than every fourth *phishing* attack, and also more than every third *bullying* attack, its effectiveness against *incorrect content, copyright infringement, commercial fraud, identity theft* and *disclosing of private information* is seen to be around each fifth case. The chance to address the risks of and *Internet addiction* by monitoring and surveillance is seen as fairly low with only one out of six cases.

Again monitoring and surveillance score a little bit higher than filter software for *data persistence, data portability* and *profiling*, nevertheless the degree of effectiveness for the three of them is less than one out of ten cases.

B 3 Age verification

B 3.1 Description of age verification and its workflow

Various systems are used to verify the age of users of online services and to ensure that only appropriate content and services are provided to specific age groups. Age verification can take place outside the Internet, based on a one-time personal face-to-face authorisation. That means after the personal identification and age verification the user gets his access information, e.g. password or PIN. These are usually also meant for paying functionalities thus it shall be ensured that the owner takes care of any misuse to avoid loss of money. Advanced systems of identification and age verification are based on the concept of the togetherness of a token (card or stick) and knowledge (PIN or password). Only the person that has both at his command can verify to be the legitimate owner of the identity and thus can prove to belong to a particular age group.



This type of technical age verification allows for a high degree of effectiveness, nevertheless it requires specific technical equipment (i. e. a card reader) and also corresponding legal regulations.

Currently legislation in many European countries allows age verification of adults to restrict access to adult content for minors. There are only a few concepts for age verification of minors like the kids card in Belgium that are able to technically ensure to a reasonable degree that only minors have access to special Internet areas, i. e. chat rooms for children.

The relevance of many of the risks and threats depends on the age of the user. Therefore age verification plays an important role in regard to restrict access of minors to specific content or to platforms providing contact opportunities.

B 3.2 Effectiveness of age verification

As described before, age verification is a tool meant for restricting access to specific content or areas of the web. So it does not come as a surprise that age verification gains higher effectiveness in regard to *age inappropriate content* (nearly half of all cases) and *violent content* than in regard to other risks. In regard to *illegal content* and *inappropriate advertisement* to children it is judged that age verification can detect each fourth to fifth case.

It is assumed that age verification could get in the way of one out of seven *grooming* attacks, which gives evidence of a fairly low effectiveness against that risk.

Also *incitement of harm* cannot be addressed properly by this supportive technology. Age verification gains low effectiveness against risks like *harmful advice, phishing* and *commercial fraud*, while it is judged as nearly ineffective against all other risks.

B 4 Other technical tools

B 4.1 Description of other tools, their workflow and effectiveness in regard to specific risks

Like age verification there are some other tools addressing special areas of risk.

Time control can be used to restrict the usage of a computer to a fixed span of time by switching off the machine automatically after that time. Automatic time control is not primarily developed to fight *Internet addiction* but it can be useful for that purpose. The experts judged that Time Control can address each second case of Internet addiction.

Automatic authentication processes are usually based on human authentication factors i. e. something the person owns like an identity card, something the persons knows like a PIN or password and something the person is or does like a fingerprint. Authentication processes that need to meet high security demands are often based on asymmetric cryptography like the digital signature. To the experts' opinion automatic authentication processes can avert more than one-third of cases of *identity theft*.

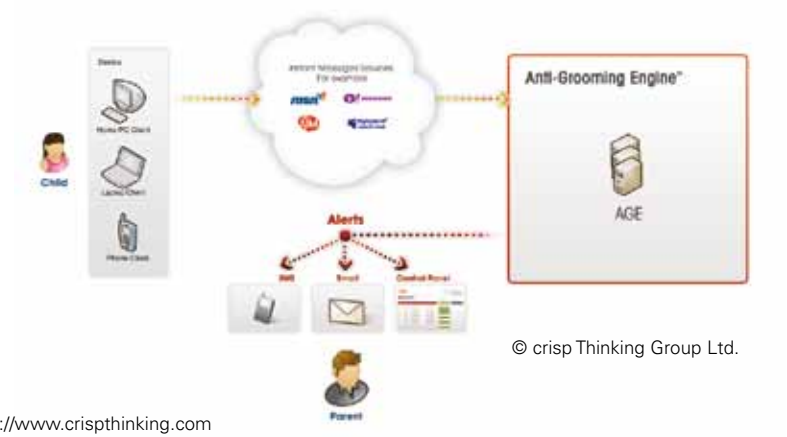
Anti-phishing software is a special type of filter software meant to detect *phishing* attacks and to inhibit them. The effectiveness is judged unequally: while some experts see a high degree of effectiveness between two-thirds of all cases, others do not believe that it can reach more than one quarter.

Digital watermark technology[7] might be a solution to prevent *copyright infringement*. Watermark technology means the implementation of a piece of code into digital content. To detect where the content is located, reduplicated and distributed, in addition a monitoring tool is needed targeted to the recognition of the watermark. It is assumed that one out of four copyright infringements could be prevented by watermark technology.

7 - Source: http://www.copyrightinfo.eu/

Data persistence and *data portability* are not a priori to be seen as a risk. Both are of value in case that it is necessary to ensure that data are unaltered and can be ported to another system. Nevertheless, data persistence and data portability can cause problems to the users. Not everybody wants all personal data retrievably stored forever. As described above, nearly all known technical tools are failing in regard to the risks of 'unwanted' data persistence and data portability. *Encoding* can be a tool to prevent unwanted portability of data. Encoding is the process of transforming information from one format into another. Before the encoded data can be ported to another system and f. e. merged with other data, they must be decoded. Thus encoding can help to prevent unwanted porting of data in around half of all cases, according to the experts' opinion. Generally setting an *expiration date* for all user generated content can slightly reduce the risk of data persistence in one quarter of all cases; also an irremovable tag with an expiry date might improve the avoiding of unwanted data persistence. An invariably available *option to delete* personal data can help to minimise the risk of unwanted reduplication in one out of five cases.

A so-called *Anti-Grooming Engine*[8] is a tool combining several methods to detect unusual conduct and thus prevent *grooming* attacks against children in chat rooms. The engine works from a database containing profiles of usual conduct of real-life groomers and real-life girls and boys. These profiles are built on an analysis of the communication in regard to vocabulary, punctuation, sentence length, typing speed and aggression level. The profiles are regularly updated, and thus the engine shall be able to differentiate between good relationships and bad ones. If there is evidence of a bad relationship, an alert is sent to a responsible adult via SMS, email or a control panel on the PC. This tool is judged to be effective in around two-fifth of all cases, which means that it is likely to be as effective against grooming as monitoring and surveillance.



8 - Source: http://www.crispthinking.com

C · Improvement of youth protection on the Internet

The suggestions to improve youth protection on the Internet identified by the YPRT are related to the following aspects:

- Measures to bring supportive technologies into effect efficiently
- Educational measures to be combined with supportive technologies, tailored to different age groups
- General conditions of youth protection

The Toolkit developed by the Youth Protection Roundtable shall support the various stakeholders involved in the processes of service and content provision, hardware and software development, parents' counselling, children's education, multipliers' training, and political decision making, they are of the nature of suggestions and are certainly not to be understood as obligatory.

The proposed measures are clustered to the following principles each of them addressing varying stakeholders.

C 1 Improvement of supportive technologies and infrastructures

Supportive technologies and infrastructures, f. e. filter software, databases, and systems of identification and verification, available so far do not always unfold their full potential for youth protection. It is therefore necessary to enhance their value technically, but also by co-operation between the various stakeholders involved in the process, like service providers, hardware manufacturers and software developers, research units and regulatory authorities. The Youth Protection Roundtable encourages exploiting the potential of supportive technologies and also of infrastructures by technically enhancing single solutions and by the optimisation of collaboration of different supportive technologies. The Youth Protection Roundtable also encourages establishing procedures for co-operation and sharing of resources between the stakeholders involved. The YPRT encourages those stakeholders to consider the following improvements:

C 1.1 Regular up-date of blacklists and white lists

C 1.2 Implementation of already existing lists approved by national authorities and implemented in the respective country, f. e. the so-called BPJM-Module in Germany (n. b. to avoid misuse those lists shall never be available to the public)

C 1.3 Promotion of interoperability of classification systems

C 1.4 Promotion of user-based classification of content stored in a database to be shared by any stakeholder interested to use it for 'good' purpose

C 1.5 Ensure that filtering activities are reported correctly in log files

C 1.6 Improvement of the usability of log files (software supported analysis of log files)

C 1.7 Promotion and improvement of learning software / artificial intelligence

C 1.8 Improvement of robustness of filter software regarding browsers

C 1.9 Ensure that supportive technologies work properly regardless of the device in use to access the Internet (PC, mobile phone, game console, etc)

C 2 Improvement of usability of filter software

The effectiveness of filter software is largely affected by the ability of the users to install, configure and adapt the system to their own needs and social environment. The Youth Protection Roundtable suggests improving the usability of filter software by examination of the technical pre-conditions and settings of their usage and also by explicitly taking into account comprehensibility and transparency of the filtering process and decision.

C 2.1 Pre-installation of filter software on the hardware in use to access the Internet (PC, game console or mobile device) or coming along with the service (preferably switched on by default i. e. opt-out instead of opt-in)

C 2.2 Avoidance of conflicts with other software (e. g. anti-virus software)

C 2.3 Prevention of circumvention of filter software on the end-user device (e. g. prevent bypassing of filters by misspelling, by using other languages, and prevent bypassing by use of alternative infrastructure and networks)

C 2.4 Meeting the expectations of parents in regard to installation and update procedures

C 2.5 Provision for comprehensible user dialogue and guidance with regard to the user's age

C 2.6 Ensure that the filtering decision is completely transparent and comprehensible for the user with regard to the user's age

In times of Web 2.0, the responsibility of the providers grows to develop their services in order to minimise the risks for children and young people. At the same time it is important to provide tools with parents and educators for protecting children and young people from harmful content and inappropriate contacts. Supportive technologies, like filtersoftware for youth protection have to be improved to relieve parents and ease the process of empowering their children by teaching media literacy.

Mark Bootz, jugendschutz.net

C 2.7 Provision of information about the filtering processes, in detail

- **C 2.7.1** that filtering procedures are implemented
- **C 2.7.2** on which basis the filter software does work (e. g. blacklist or white list of URLs or of words)
- **C 2.7.3** about the criteria for filtering
- **C 2.7.4** why a specific content has been filtered
- **C 2.7.5** about the estimated effectiveness of filter software in regard to the various types of content and communication
- **C 2.7.6** how content blocking and filtering can be overruled
- **C 2.7.7** where complaints about unjustified blocking of content can be reported

C 2.8 Provision of easy to use tailoring mechanisms for filter software and information to the users how they can adapt the filter to their own or their children's needs

C 2.9 Provision for the option to import and export filter policies to ease the sharing of policies for parents and teachers

C 2.10 Observance of the demand for consistency, transparency and comprehensibility in regard to the filtering procedures – avoid esp. inconsistency of filtering results

Almost 30% of the reports received by our Internet safety Helpline concerns cyberbullying cases. Over the last two years in Poland we have been focusing our efforts on encouraging a more responsible use of new technologies by young people. Parents seldom talk to their children about how they are using Internet and mobile phone and often do not realize that their child may as likely cyberbully as be a target of cyberbullying. Through nationwide educational campaigns we are trying to raise awareness that family and school have an important role to play in prevention and responding to cyberbullying incidents.

Agnieszka Wrzesień, Nobody's Children Foundation

C 3 Improvement of Internet appliances - technological basics and implementation of supportive widgets to help users to protect themselves

Media literacy is the key to ensure the safe use of Internet appliances. Nevertheless the educational efforts can be supported by technology, thus ensuring that codes of practice for the users are continuously kept in mind and especially unsafe or inappropriate action is avoided. In consideration of technical feasibility the Youth Protection Roundtable proposes to improve the safety of Internet appliances through the implementation of supportive widgets to help users to protect themselves.

C 3.1 Default setting of profiles on private (opt-in instead of opt-out)

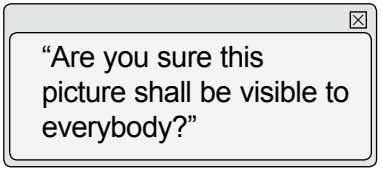
C 3.2 Provision of support to the users for password management, (i.e. master question, reminder, software password sitter)

C 3.3 Provision of the possibility to remove tags from own content and from content generated by others tagging to my profile

C 3.4 Implementation of a report button on sites with user-generated content where conflicts and harmful content might occur, delivering the reports preferably to already existing hotlines and helplines

C 3.5 Pop-Up or mouse-over effect with warning notes in regard to disclosure of private information

C 3.6 Pop-Up or mouse-over effect with warning notes in regard to infringement of human rights / defamation, f. e. when uploading pictures



C 3.7 Automatic deletion of content after date of expiry set by the user

C 3.8 Provision of a delete button on all sites with user-generated private data, allowing the user to delete his own data (knowing well that content that was once published can not be deleted totally)

C 3.9 Enabling the tagging of user-generated content in regard to an expiry date to ensure that content is deleted wherever it has been duplicated or moved

C 3.10 Provision of technical support to avert unwanted re-duplication of text and pictures published online

C 3.11 Provision of the possibility for the user to remove GPS data from pictures before uploading in order to avoid unintentional disclosure of location data

C 3.12 Ensure that passive localisation services by use of GPS data by third parties are accomplishable only with permission of the owner

C 3.13 Provision of explicit information about the status of communication areas (public or private)

C 3.14 Provision of word filtering for direct communication between users (forums, ecards), where children are addressed directly

C 3.15 Provision of the option for parents to monitor the usage of their children in regard to time, content and communication with respect of children's privacy

C 3.16 Provision of the possibility to encrypt personal data within the application

C 3.17 Footprint for data of users who have already objected to the storage and use of their data, to ensure that these data are not retrieved and stored again from another source

C 3.18 Text description for advertisement banners readable for word lists of filters

C 3.19 Involvement of the community in the process of development and implementation of safety tools and policies

C 4 Agreement on policies for providers and operators

The Youth Protection Roundtable motivates content providers and operators to consider the implementation of policies to ensure the safe use by children and young people. These policies should be developed subject to their services and implemented in accordance with their financial, technical and organisational capabilities.

C 4.1 Policy and procedures to follow user reports, esp. definition of times for reaction, or take down where appropriate

C 4.2 Policy in regard to easy tracking and handling of user complaints

C 4.3 Policy in regard to human moderation for all areas of the platform providing for direct communication with other users

C 4.4 Policy in regard to the promotion of help sites (e. g. when someone searches for anorexia, help sites should be the first results in the list)

C 4.5 Policy in regard to co-operation with welfare and help organisations

C 4.6 Policy in regard to co-operation between hotlines, law enforcement and providers

C 4.7 Policy in regard to storage, multiplication, and circulation of user data

C 4.8 Policy in regard to advertisement

C 4.9 Agreement on independent or internal monitoring of the above mentioned policies

© Pixelio

Adiconsum is engaged in youth media protection supporting and protecting rights and interests of the young users of the Net through the carrying out of awareness raising campaigns among youngsters, parents and teachers on the responsible and safe use of Internet and new online technologies; the drawing up of several brochures, guides and tools for pupils and adults on online safety; a steady dialogue and exchange of views with institutions, ICT companies and all other key stakeholders that directly or indirectly impact young people's appropriate use of technological tools, reminding each of them of their specific responsibilities in this area.

Paola Pendenza, Adiconsum

C 5 Digital literacy

The Youth Protection Roundtable supports the improvement of digital literacy of children and youths themselves and also of parents and persons in charge of minors. Digital literacy means knowledge about digital media and supportive technologies for youth protection and the ability to benefit from both. Empowerment is deemed the number one protection shield for children and youths in the Information Age. The Youth Protection Roundtable encourages supporting educational measures for the improvement of digital literacy with regard to all technical devices for Internet access and all supportive technologies.

To protect children from harmful and inappropriate content, besides technical tools digital literacy and empowerment is very important. Children can benefit from the huge opportunities the Internet provides only when they know how to chat safely how to protect their own data and when knowing websites that are age appropriate and interesting. Internet-ABC tends to empower children, parents and educators to explore the Internet and avoid risks.

Mechthild Appelhoff, Internet-ABC

C 5.1 Improvement of digital literacy with regard to all technical devices for Internet access (special attention to newly developing areas, at present i.e. mobile access)

C 5.2 Improvement of digital literacy with regard to supportive technologies and the use of supportive widgets

C 5.3 Improvement of digital literacy with regard to reporting of illegal, harmful or unwanted content and harassing conduct to hotlines and helplines

C 5.4 Improvement of digital literacy with regard to critical reflection of content

C 5.5 Improvement of digital literacy with regard to privacy and data protection

C 5.6 Set-up of an online school for safer Internet (website and online learning tools) in strong co-operation with already existing online offers

C 5.7 Training for young Internet experts in schools and institutions for social youth work

C 5.8 Internet safety as a subject in school and moreover cross-over subjects implementation of Internet safety aspects

C 5.9 Set-up of mediation processes to take care for bullying victims and violators

C 5.10 Provide education for digital citizenship, i.e. to make use of the technology in an autonomous and responsible way

C 5.11 Internet safety as a subject in teacher and social youth worker education

C 5.12 Provide training for mediators and moderators

C 5.13 Provide 'headmaster training', for those working at schools or other professionals working with children and youths

C 5.14 Enable headmasters to set up a safety concept at their school and to implement the requirements of security, privacy, data protection and digital literacy in all working processes

C 5.15 Develop and implement house rules regarding the use of digital media in educational institutions and Public Internet Access Points involving young people in the process of development

C 5.16 Provide appropriate material for the improvement of digital literacy in strong co-operation with already existing offers

C 5.17 Motivate children and young people to engage in safer Internet matters, i. e. by competitions, etc. and involve them in the development of material

The internet safety awareness work has been of great importance to The Mannerheim League for Child Welfare. In order to bridge the digital divide between generations, MLL pursues to foster the dialogue between generations. An important aspect of the approach is to familiarise adults with new forms of online and mobile methods of communication used by young people and to increase the understanding of the possible risks and negative effects they may induce. Thus, we have used young people as trainers to share their knowledge and experiences with parents and teachers.

Sanna Harakkamäki , The Mannerheim League for Child Welfare

C 6 Awareness raising

For the empowerment of citizens in the information age awareness raising is crucial. Sensitising for the risks and threats but also for the opportunities the Internet provides for shall come as a matter of course. The Youth Protection Roundtable members place special emphasis on positive impact of Internet usage on young peoples' development and commit themselves to strong efforts for a broader awareness in all groups of society regardless of age, gender and ethnicity.

C 6.1 Place special emphasis on positive impact of Internet usage on young peoples' development

frag FINN.de
Gecheckt! Das Netz für Kids.

C 6.2 Realisation of information and awareness raising days, such as Safer Internet Day involving young people

C 6.3 Provision of printed and online material targeted to

- children and youths
- adults in charge of minors
- persons with migratory backgrounds
- Internet service providers
- content providers
- providers of social community platforms

C 6.4 Initiation of awareness campaigns involving young people

C 6.5 Raising awareness for the option to report to hotlines and helplines

C 6.6 Raising awareness for education for digital citizenship

C 7 Research

Research builds the basis for the development of technical tools and educational strategies. Therefore the Youth Protection Roundtable encourages supporting, promoting and taking into consideration current research for all Internet safety activities.

C 7.1 Support for quantitative and qualitative studies about children's and young people's online behaviour

C 7.2 Promotion of available research and support for pan-European exchange of researchers in the area of media appropriation by children and youths

C 7.3 Support studies on media adaptation of children and young people

C 7.4 Formative evaluation of digital media use

Because of media convergence, youth media protection will continue to gain in importance in the future. We believe that self regulation of companies is a key component in this respect, too. Over the last years, FSM together with their member companies have therefore developed various branch-specific codes of conduct in order to meet the specific needs of youth media protection.

Sabine Frank, FSM Secretary General

C 8 Legal regulation

Based on already existing law and taking into account the differences in national law and cultural environments the Youth Protection Roundtable proposes to harmonise and concretise existing law and regulations regarding the definition of illegal content and content harmful to children, data protection or rather in regard to regulation for the right to delete user generated content and profiles generated by the user.

C 8.1 Regulation for the right to delete content and profiles generated by the user

C 8.2 Regulation for the right to privacy

C 8.3 Regulation for the prosecution of online offenders

C 8.4 Harmonisation of legal definition of illegal content

D · Resources

Code for the ChatCheck Badge by the Association of Danish Internet Media (2007)

Comparing Children's Online Activities and Risks across Europe. A Preliminary Report Comparing Findings for Poland, Portugal and UK, June 2007

Crisp Thinking Group Ltd. (2005). Anti-Grooming Engine™. Retrieved January 21, 2009 from http://www.crispthinking.com/anti-grooming-engine.htm

ENISA - Children on virtual worlds – What parents should know, September 2008

ENISA - Photo Sharing, Wikis, Social Networks –Web 2.0 and Malware 2.0, EU Agency issues Position Paper on security for the next generation web, December 2008

ENISA Position Paper No.1: Security Issues and Recommendations for Online Social Networks, October 2007

ENISA - Technology-induced challenges in Privacy & Data Protection in Europe, October 2008

Euro Media Literacy: Charter for Media Literacy (2005)

EurActiv.com (2008). Web 2.0: New opportunities, new risks. Retrieved September 4, 2008 from http://www.euractiv.com/en/infosociety/web-20-new-opportunities-new-risks/article-171600

Eurobarometer (2006). Eurobarometer on Safer Internet: quantitative surveys 2005-2006. Retrieved January 27, 2009 from http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

Eurobarometer (2007). Eurobarometer on Safer Internet for Children: qualitative study 2007. Retrieved January 21, 2009 from http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

Flash Eurobarometer survey (2008). Towards a Safer Use of the Internet for children in the EU - a parents' perspective. Retrieved January 27, 2009 from http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

Institute for Public Policy Research (ippr): Behind the Screen, the hidden life of youth online, March 2008-10-20

Internet Filters, a Public Policy Report by the Brennan Center for Justice, 2006

JFF – Institut für Medienpädagogik in Forschung und Praxis. Untersuchung der Akzeptanz des Jugendmedienschutzes aus der Perspektive von Eltern, Jugendlichen und pädagogischen Fachkräften. Eigenständige Teilstudie des JFF zur Analyse des Jugendmedienschutzsystems, München, August 2007

Luxembourg Safer Internet Helpline Project 2006, para.1, Definition von Filtersoftware [Electronic version]. Retrieved January 21, 2009 from http://www.lusi.lu/index.php?id=16&L=1

Media Literacy – An Alternative to censorship by the Free Expression Policy Project, 2003

Mercury Interactive Corporation (2004). SiteScope User's Guide, Version 7.9.5.0. para. 14, Monitoring. Retrieved January 21, 2009 from http://mon15ny450.doubleclick.net/SiteScope/docs/SiteScopeTerms.htm

Niedersächsische Landesmedienanstalt. Helmut Volpers (Hrsg.). Funktionsweise des Internets und sein Gefährdungspotenzial für Kinder und Jugendliche. Ein Handbuch zur Medienkompetenzvermittlung. NLM-Band 17, 2004

Ofcom. Social Networking. A quantitative and qualitative research report into attitudes, behaviours and use, April 2008

Paris Agenda or 12 Recommendations for Media Education, Paris, UNESCO, 21-22 June 2007

Photopatrol (2007). Mehr Schutz und Erfolg für Ihre Bilder durch digitale Signaturen. Retrieved January 21, 2009 from http://www.photopatrol.eu/fileadmin/templates/Hilfe_Texte/Informationen_ueber_Photopatrol_Download_-_V.1.pdf

Protecting Children Using the Internet – Opinion by the European and Social Committee, May 2008

Public consultation of the European Commission in regard to Age Verification, Cross Media Rating and Classification, Online Social Networking, July 2008

Recommendation CM/Rec (2008) 6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (May 2008)

Resolution on Children's Online Privacy (30th International Conference of Data Protection and Privacy Commissioners – Strasbourg), October 17, 2008

Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners – Strasbourg), October 17, 2008

Safer Children in a Digital World – The report of the Byron Review, March 2008

Schulen ans Netz e.V. IT works. Jugendmedienschutz Filterlösungen im schulischen Umfeld, Bonn 2005

SIP Benchmark Synthesis Report 2007 Edition by Deloitte Enterprise Risk Services, December 2007

SIP Benchmark Synthesis Report 2008 Edition by Deloitte Enterprise Risk Services, November 2008

Good practice guidance for the providers of social networking and other user interactive services 2008, March 2008

Good Practice Guidance for Moderation of Interactive Services for Children, December 2005

Good practice guidance for search service providers and advice to the public on how to search safely, December 2005

Good Practice Models and Guidance for the Internet Industry On: Chat Services, Instant Messaging, Web-based Services, January 2003

United Nations Convention on the Rights of the Child signed 1989

Universität Leipzig. Medienkonvergenz Monitoring Report 2008, Jugendliche in konvergierenden Medienwelten

Wikipedia Encyclopaedia (2009). Webmonitoring. Retrieved January 21, 2009 from http://de.wikipedia.org/wiki/Webmonitoring

E · Inventory of self-regulation

E 1 Organisations of self-regulation in Europe

Name of organisation	type of organisation	geographical scope	content-related scope	URL
Austrian E-Commerce Trust Mark	Association	Austria	web	http://www.guetezeichen.at/
Internet Ombudsmann	Association	Austria	web	http://www.ombudsmann.at/
Asociace provozovatelů mobilních sítí	Association of Mobile Network Operators	Czech Republic	mobile	http://www.apms.cz/Default.aspx?ModuleId=379&ID=156
Sdružení pro internetovou reklamu v ČR, z.s.p.o. (SPIR)	Association of Internet advertising	Czech Republic	web	http://www.spir.cz
Association of eCommerce	Association	Czech Republic	web	http://www.certifikovany-obchod.cz/o-apek-certifikaci
Media Council for Children and Young People	Association	Denmark	movies	http://www.medieraadet.dk/
European Internet Coregulation Network	Association	Europe	web	http://network.foruminternet.org/
Interactive Software Federation of Europe (ISFE)	Association of Companies	Europe	interactive software	http://www.isfe-eu.org/
Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.	Association of Companies	Germany	web	www.fsm.de
Freiwillige Selbstkontrolle Fernsehen e.V.	Association of Companies	Germany	TV	www.fsf.de
Spitzenorganisation der Filmwirtschaft e.V.	Association of Companies	Germany	movies	www.spio.de
Unterhaltungssoftware Selbstkontrolle	Association of Companies	Germany	interactive software	www.usk.de
Deutscher Presserat	Association of Companies	Germany	all media	http://www.presserat.de/
Deutscher Werberat	Association of Companies	Germany	advertisement	http://www.werberat.de/
Freiwillige Selbstkontrolle Telefonmehrwertdienste e.V.	Association of Companies	Germany		http://www.fst-ev.org/
Beschwerdestelle / Deutschland sicher im Netz	Working group of Association of Companies	Germany	web	http://www.eco.de/servlet/PB/menu/1020202_l1/index.html

Name of organisation	type of organisation	geographical scope	content-related scope	URL
ICRA Deutschland	Association of Companies	Germany	web	http://www.eco.de/servlet/PB/menu/1211767_l1/index.html
Kommission für Jugendmedienschutz	Authority	Germany	all media	http://www.kjm-online.de/public/kjm/
Bundesprüfstelle für jugendgefährdende Medien	Federal Authority	Germany	all media	http://www.bundespruefstelle.de/
Freiwillige Selbstkontrolle der Chatbetreiber	Association of Companies	Germany	web	http://www.fsm.de/de/Chat
Automaten-Selbst-Kontrolle (ASK)	Association	Germany	interactive software	http://www.automaten-selbstkontrolle.de
Arbeitsgemeinschaft der Landesmedienanstalten (ALM)	Association	Germany	all media	http://www.alm.de
Greek Self-Regulating Organisation for Internet Content - SAFENET	NGO	Greece	web	http://www.safenet.org.gr/
National Committee of Users (CNU)	Association	Italy	all media	http://www.agcom.it/cnu/
ADUC - Associazione per i Diritti degli Utenti e Consumatori	Association for the Rights of Consumers	Italy	all media	http://www.aduc.it/
Netherlands Institute for the Classification of Audio-visual Media	Association of Companies	Netherlands	all media	http://www.kijkwijzer.nl/
ECP.NL	Public-private not for profit organisation	Netherlands		http://www.ecp.nl/
Stichting Reclame Code (SRC)	Advertising Code Foundation	Netherlands	advertisement	http://www.reclamecode.nl/
Rada Reklamy (Advertising Council)	Polish Advertising Industry	Poland	advertisement	http://www.radareklamy.org
hotline Spletno oko	Non-profit project (Internet)	Slovenia	web	https://www.spletno-oko.si/
Slovenian Consumers' Association	Non-profit organisation (Consumers' rights using Internet, mobile phones and computers)	Slovenia	all media	http://www.zps.si/
APEK (Post and Electronic Communications Agency of the Republic of Slovenia)	Independent Regulatory Body (electronic communications and postal market)	Slovenia	all media	http://www.apek.si/

Name of organisation	type of organisation	geographical scope	content-related scope	URL
Association Vita Activa	Association	Slovenia	all media	http://www.drustvo-vitaactiva.si/401.html
Slovenian Advertising Chamber	Non-profit association of legal and physical persons (companies and individuals) regulation of media advertising	Slovenia	advertisement	http://www.soz.si/
Asociación Española de Distribuidores y Editores de Software de Entretenimiento	Spanish Association of Editors and Wholesalers of Entertainment Software	Spain	interactive software	http://www.adese.es
Asociación para la Autoregulación de la Comunicación Comercial "Autocontrol".	Spanish advertising self-regulation organisation	Spain	advertisement	http://www.autocontrol.es/
Agencia de Calidad de Internet	Internet Quality Agency	Spain	web	http://www.iqua.net
Internet Watch Foundation	Charity	UK	web	http://www.iwf.org.uk/
OFCOM - Office of Communication	Public regulation Authority	UK	all media	http://www.ofcom.org.uk/about/csg/ofcom_board/code/
Home Office Task Force on Child Protection on the Internet	Task Force	UK	web	http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce
Family Online Safety Institute	Association	UK	web	http://www.fosi.org/icra

E 2 Instruments of self-regulation in Europe

Name of instrument	type of document	geographical scope	content-related scope	URL
Spam code of conduct of ISPA	Code of Conduct	Austria	web	http://www.ispa.at/downloads/COC_spam_english.pdf
Journalists' Code of Conduct	Code of Conduct	Cyprus	journalistic ethics	http://www.mmc2000.net/docs/leggi/CYPRUS.pdf
Kodex Etického Nákupu Vodafonu	Code of ethical purchase	Czech Republic	mobile	http://www.vodafone.cz/pdf/kodex_cz.pdf
Etický kodex o užívání veřejných informačních služeb pro šíření sázkových služeb	Code of Conduct	Czech Republic	gambling	http://web01.sazka.cz/LoterieAHry/docDetail.aspx?docid=19015601&doctype=ART&&cpi=1&highlight=etick_%20kodex
Evropská Asociace Státních Loterií A Toto Společností	Code of Conduct	Czech Republic	web	http://www.sazka.cz/o-nas/vice-o-sazka/zakony/kodex.php
Code for the ChatCheck Badge	Code of Conduct	Denmark	web	http://www.fdim.dk/?pageid=52
European Framework for Safer Mobile Use by Younger Teenagers and Children	Framework	Europe	mobile	http://www.gsmworld.com/gsmeurope/documents/eur.pdf
Rec. on measures to promote the freedom of expression and information with regard to Internet filters	Recommendations	Europe	web	http://www.coe.int/
Journalists' Code of Conduct	Code of Conduct	Europe	all media	http://www.presswise.org.uk
ISPA Code of Conduct	Code of Conduct	Europe	journalistic ethics	http://www.ispa.org.za/code/code_of_conduct.shtml
Code of Conduct for search engines / Verhaltenssubkodex für Suchmaschinenanbieter der FSM	Sub - Code of Conduct	Germany	web	http://www.fsm.de/en/SubCoC_Search_Engines
Code of Conduct of Mobile Phone Service Providers in Germany for the Protection of Minors Using Mobile Phones	Sub - Code of Conduct	Germany	mobile	http://www.fsm.de/en/Subcode_of_Conduct_mobile
Code of Conduct of Chat Providers in the FSM	Sub - Code of Conduct	Germany	web	http://www.fsm.de/inhalt.doc/Sub-Code_Chat.pdf
NICAMs regulations for film, DVD, TV and Mobile Operators	Sub - Statutes	Netherlands	all media	http://www.kijkwijzer.nl/
Richtlijn voor chatrooms	Guidelines	Netherlands	web	http://www.chatinfo.nl/
Dutch Advertising Code	Code	Netherlands	advertisement	http://www.reclamecodecommissie.nl/bijlagen/dutch_advertising_code.pdf

Name of instrument	type of document	geographical scope	content-related scope	URL
Code of Ethics in Advertising	Code of Conduct	Poland	advertisement	http://www.radareklamy.pl/img_in//PLIKI/Kodeks%20Etyki%20Reklamy%20Eng.pdf
Slovenian Code of Advertising Practice	Code of Conduct	Slovenia	advertisement	http://www.soz.si/oglasevalsko_razsodisce/slovenski_oglasevalski_kodeks/
Internet Service Providers' Association Code of Conduct	Code of Conduct	South Africa	web	http://www.ispa.org.za/code/code_of_conduct.shtml
Convenio Marco De Colaboración Para La Promoción Del Uso Seguro De Internet Por La Infancia Y La Juventud	Agreement	Spain	web	not digitally available
Código de autorregulación de la publicidad de alimentos dirigida a menores, prevención de la obesidad y salud	Food advertising for children and obesity prevention self-regulation code	Spain	advertisement	http://www.fiab.es/datos/1/PAOS_1676.pdf
Código de conducta de la industria europea del software interactivo relativo a la clasificación por edades, el etiquetado, la promoción y la publicidad de productos de software interactivo.	Code of Conduct	Spain	interactive software	http://www.adese.es/web/criterios_autoregulacion.asp
Código de Conducta Publicitaria	Code of Conduct	Spain	journalistic ethics	http://www.autocontrol.es/pdfs/Cod_conducta_publicitaria.pdf
Código Ético de Comercio Electrónico y Publicidad Interactiva	Code of Conduct	Spain	web	http://www.confianzaonline.org/codigoetico/codigoetico.php
Código Deontológico para Publicidad Infantil de la Asociación Española de Fabricantes de Juguetes, y Unión de Consumidores de España	Consumers Code of Ethics	Spain	advertisement	http://www.aefj.es/template.php?id=91
Código de Autorregulación sobre contenidos televisivos e infancia.	Self-regulation code on TV content for children	Spain	TV	http://www.tvinfancia.es/Textos/CodigoAutorregulacion/Codigo.htm

Name of instrument	type of document	geographical scope	content-related scope	URL
Convenio de Autorregulación para promover el buen uso de Internet en España	Self-regulation code for the promotion of an appropriate use of Internet in Spain	Spain	web	http://www.aui.es/../biblio/documentos/legislacion/proteccion_menores/convenio/tex_conv.htm
Código deontológico de la Agencia de Calidad de Internet	Internet Quality Agency Code of Ethics	Spain	web	http://www.iqua.net/Codigos_de_conducta/Codigo_de_conducta/?go=WWiW6aWP3cIUyUj7fiM3LUP2TC+M0m3NphIdSA2vOCaqmvpV3BPkG0o8
Convenio Marco De Colaboración Para La Seguridad Del Menor	Committment	Spain		
Code of Practice for the self-regulation of new forms of content on mobiles	Code of Practice	UK	mobile	http://www.mobilebroadbandgroup.com/content-code.pdf
Self-regulatory Code for the responsible selling of mobile telephony	Code of Practice	UK	mobile	http://www.mobilebroadbandgroup.com/documents/mbg_cop_sm_250707_f.pdf
Industry Code of Practice for the use of mobile phone technology to provide passive location services in the UK	Code of Practice	UK	mobile	http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf
Good Practice Guidance for the Moderation of Interactive Services for Children	Guidelines	UK	web	http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation-document-final.pdf?view=Binary
Good practice guidance for search service providers and advice to the public on how to search safely	Guidelines	UK	web	http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/search-and-advice-public.pdf?view=Binary
Promoting Internet Safety Through Public Awareness Campaigns Guidance for Using Real Life Examples Involving Children or Young People	Guidelines	UK	web	http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/RealLifeExamples.pdf?view=Binary
Good Practice Models and Guidance for the Internet Industry On: Chat Services, Instant Messaging, Web-based Services	Guidelines	UK	web	http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf?view=Binary
Television Advertising of Food and Drink Products to Children"	Code	UK	advertisement	http://www.ofcom.org.uk/consult/condocs/foodads_new/statement/

Name of instrument	type of document	geographical scope	content-related scope	URL
BCAP Spread Betting Advertising Rules and BCAP Radio Advertising Code	Code	UK	advertisement	http://www.cap.org.uk/NR/rdonlyres/6C6CECA6-CCCB-44B7-A146-460D2726BC48/0/BCAPSpreadBettingRadioAdvertisingRules.pdf
BCAP Rules on the Scheduling of Advertising	Rules	UK	advertisement	http://www.asa.org.uk/NR/rdonlyres/7F763788-6A51-4A73-B35B-C60346FD5F6C/0/BCAPRulesontheSchedulingofTelevisionAdvertisements_20080108.pdf
Advertising Standards Code for Text Services	Code	UK		http://www.asa.org.uk/NR/rdonlyres/3B4358E5-85CC-40EE-A2DD-EE883BBABB6E/0/BCAPCodeforTextServices_20080108.pdf
BCAP Guidance to Broadcasters on the Regulation of Interactive Television Services	Guidelines	UK	TV	http://www.asa.org.uk/NR/rdonlyres/D41345A2-31B5-4149-879B-69A08A64879C/0/BCAP_Guidance_on_Interactive_TV.pdf
BCAP Advertising Guidance Notes	Notes to Guidlines	UK	advertisement	http://www.clearcast.co.uk/clearcast/notes_of_guidance/Appendix+3+Guidelines+for+Superimposed+Text+from+BCAP+Guidance+on+Text+and+Subtitling+in+Television.htm
Good practice guidance for the providers of social networking and other user interactive services 2008	Guidance	UK	web	http://police.homeoffice.gov.uk/
Editors' Code of Practice	Code of Practice	UK	journalistic ethics	http://www.pcc.org.uk/
CAP and BCAP Gambling Advertising Rules and BCAP Spread Betting Rules	Rules	UK	web	http://www.cap.org.uk/NR/rdonlyres/8C9D2140-EE00-424F-9E67-CE1914B3DA71/0/FINALCAPBCAPGamblingRules.pdf

F · Inventory of legal regulation in Europe

EU Member States	Youth Protection / Youth Media Protection	Source
Austria	Pornografiegesetz	http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR12058546/NOR12058546.pdf
	9 different youth protection laws (including youth media protection) of the Federal States	http://www.bmwfj.gv.at/BMWA/Schwerpunkte/Jugend/Jugendschutz/default.htm
	Anti-Stalkinggesetz § 107a Strafgesetzbuch. Tatbestand der "beharrlichen Verfolgung"	http://www.ris.bka.gv.at/GeltendeFassung.wxe?QueryID=Bundesnormen&Gesetzesnummer=10002296
Belgium	Belgian Penal Code Articles 380 till 383	http://www.stopchildporno.be/index.php?pid=13
Bulgaria	Child protection Act from 03.04.2003	http://www.sacp.government.bg/index_en.htm
Cyprus		http://www.lexadin.nl/wlg/legis/nofr/eur/lxwecyp.htm
Czech Republic	Act No. 359/1999 Coll., on the socio-legal protection of children, as amended (Act No. 501/2004 Coll., comes into effect 1.1.2006)	http://www.czso.cz/csu/cizinci.nsf/engo/gender_odkazy-links_with_legislative
	Act No. 94/1963 on family	http://mujweb.cz/www/vaske/rodina.htm
	Act No. 108/2006 on social services	http://www.ilo.org/dyn/natlex/natlex_browse.details?p_lang=en&p_country=CZE&p_classification=15.05&p_origin=COUNTRY&p_sortby=SORTBY_COUNTRY
	Act No. 218/2003 on legal responsibility of youth and judicature in cases of youth	http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN012622.pdf
	Act No. 140/1961 Criminal law § 205a „Receiving of child pornography" § 205b „Misuse of children for pornography production"	http://web.mvcr.cz/archiv2008/prevence/priority/kszd/english.html
	Act No. 500/2004 Administrative law	http://www.nssoud.cz/default.aspx?cls=art&art_id=1
Denmark	The Marketing Practices Act No. 1389 of 21. December 2005, latest amended in 2007	http://www.forbrug.dk/english/dco/lawsandacts/marketing-practises-act/
	Radio and Television Broadcasting Act No. 338 of 11 April 2007	http://www.kum.dk/sw4507.asp
Estonia	Youth Work Act	http://www.hm.ee/index.php?148615
	Juvenile Sanctions Act	http://www.hm.ee/index.php?149399
	Hobby Schools Act	http://www.hm.ee/index.php?149396
Finland	Child Welfare Act from 05.08.1983	http://www.finlex.fi/pdf/saadkaan/E9830683.PDF
	Act on the Classification of Audiovisual Programmes (L 775/2000) from 25.08.2000	http://www.vet.fi/english/lait_kuvaohjelmien_tarkastaminen.php
	Finish Government's Child and Youth Policy Programme 2007–2011 (Finish Ministry of Education)	http://www.minedu.fi/OPM/Julkaisut/2007/Lapsija_nuorisopolitiikan_kehittamisohjelma_2007-2011?lang=en
France	Penal code	http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm
	separate bills regarding youth protection for different media. No specific regulation for youth media protection	http://www.legifrance.gouv.fr/

EU Member States	Youth Protection / Youth Media Protection	Source
Germany	Youth Protection Act (2002)	http://www.bmfsfj.de/bmfsfj/generator/Kategorien/Service/themenlotse,did=12862.html
	Interstate Treaty for the Protection of Minors from Harmful Content in the Media (2003)	http://www.bmfsfj.de/bmfsfj/generator/Kategorien/Service/themenlotse,did=12862.html
Greece	LAW NO. 1729 Combat against the spread of drugs, protection of youth and other provisions	http://www.unodc.org/enl/showDocument.do?documentUid=446&node=docs&country=GRE&cmd=add
	Penal Code	http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/CsaGreece.pdf
	separate bill for youth protection from the National Radio and TV Council	No source
	General information on legal regulation	http://www.kep.gov.gr/portal/page/portal/MyNewPortal?lng=us http://old.mfa.gr/english/greece/today/media/internet.html
Hungary	Act I of 1996 on Radio and Television Broadcasting (Media Act)	http://www.helsinki.hu/docs/Act%20I%20of%201996.pdf
Ireland	Criminal Justice Act 2008	http://www.bailii.org/cgi-bin/markup.cgi?doc=/ie/legis/num_act/2008/a0708.html&query=Youth+Media+Protection&method=all
Italy	Codice del consumo (D.lgs. 206/2005)	http://www.altalex.com/index.php?idstr=39&idnot=33366
	Gentiloni's decree (against online pedo-pornographic materials through a blocking filter on the basis of a national black list provided by LEA to ISP (Italian Ministry of Communication)	http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0707/it3.htm http://www.comunicazioni.it/361-381.html http://www.lexadin.nl/wlg/legis/nofr/eur/lxweita.htm
	Bill on video games	http://www.comunicazioni.it/binary/min_comunicazioni/news_eng/Parliamentary%20Bill%20on%20Regulations%20for%20the%20Protection%20of%20Children%20in%20Film%20Viewing%20and%20use%20of%20Videogames.pdf
	Personal Data Protection Code, Legislative Decree no. 196 dated 30 June 2003	http://www.garanteprivacy.it/garante/document?ID=1219452
	Legislative Decree No. 345 Of 4 August 1999 Implementing The Directive No. 94/33 EC On The Protection Of Young People At Work	http://www.ilo.org/dyn/natlex/docs/WEBTEXT/54507/65185/E99ITA01.htm
	bill 6 February 2006, n. 38 against pedo- pornography and child sex abuse (the bill affords also online aspect of these issues),	http://www.edri.org/edrigram/number5.1/italy_blocking
	bill 3 august 1998 n. 269 against child prostitution, child pornography and sexual tourism	
	bill 15 February 1996 n. 66 on sex violence against children	
Latvia	Children's Rights Protection Law	http://www.humanrights.lv/doc/latlik/bern.htm
	Advertising Law (20.12.1999)	http://www.kp.gov.lv/uploaded_files/ENG/E_likumR.pdf
	Youth Law	http://www.bm.gov.lv/eng/regulatory_enactment/regulatory_enactment/?doc=10753
Lithuania	Law On Fundamentals Of Protection Of The Rights Of The Child	http://www.litlex.lt/Litlex/Eng/Frames/Laws/Documents/359.HTM

EU Member States	Youth Protection / Youth Media Protection	Source
Luxembourg	Loi sur la liberté d'expression dans les medias(Juni 2004): Chapitre V/Section 5: De la protection des mineurs	http://www.legilux.public.lu/leg/textescoordonnes/compilation/recueil_lois_speciales/MEDIAS.pdf
Malta	Criminal Code	http://docs.justice.gov.mt/lom/legislation/english/leg/vol_1/chapt9.pdf
	Electronic Commerce Act: Article 25.1.i	http://www.lexadin.nl/wlg/legis/nofr/eur/lxwemal.htm
	Broadcasting Code for the Protection of Minors (Sept.2001) (350.05: subsidiary legislation on broadcasting act)	http://docs.justice.gov.mt/lom/Legislation/English/SubLeg/350/05.pdf
Netherlands	Dutch Media Act	http://www.lexadin.nl/wlg/legis/nofr/eur/arch/ned/mediaact.pdf
	The Media Decree	http://www.lexadin.nl/wlg/legis/nofr/eur/arch/ned/mediadecree.pdf
	Dutch Advertising Code: B: Code for advertising directed at children or young people (Article 5 and 6)	http://www.reclamecode.nl/bijlagen/dutch_advertising_code.pdf
	Criminal Code; Article 240a	http://www.thefuturegroup.org/youwillbecaught/law_Netherlands.html
Poland	Polish Penal Code 202	http://www.internationalresourcecentre.org/missingkids/servlet/PageServlet?LanguageCountry=en_X2&PageId=3428
		http://www.era.int/domains/corpus-juris/public_pdf/polish_penal_code2.pdf
Portugal		http://www.lexadin.nl/wlg/legis/nofr/eur/lxwepor.htm
Romania		http://www.lexadin.nl/wlg/legis/nofr/eur/lxwerom.htm
Slovakia		http://www.lexadin.nl/wlg/legis/nofr/eur/lxweslw.htm
Slovenia	Constitution of the Republic of Slovenia; Article 56	http://www.up-rs.si/up-rs/uprs-eng.nsf/dokumentiweb/063E5907BE5B679CC1256FB20037658C?OpenDocument
	Public Media Act	http://www.mk.gov.si/si/postopki/mediji/vpis_v_register_tujih_dopisnikov_in_dopisnistev/navodila_eng/?type=98
Spain	Ley Organica 1/1996 de 15/1/96	http://vlex.com/vid/ley-organica-codigo-penal-126987
Sweden	The Children's Ombudsman Act	http://www.bo.se/adfinity.aspx?pageid=86
United Kingdom	Protection of Children Act 1978 (England and Wales)	http://www.iwf.org.uk/police/page.22.htm
	Sex Offences Act 2003 (SOA 2003):	http://www.iwf.org.uk/police/page.22.htm
	Civic Government (Scotland) Act, 1982	http://www.iwf.org.uk/police/page.22.htm
	Obscene Publications Act 1959 & 1964	http://www.iwf.org.uk/police/page.22.htm
	Police and Justice Act 2006 (Section 39 and Schedule 11)	http://www.iwf.org.uk/police/page.22.htm
	Public Order Act 1986	http://www.iwf.org.uk/police/page.22.htm

European regulation

Youth Protection / Youth Media Protection	Source
Framework decision on combating the sexual exploitation of children and child pornography	http://europa.eu/scadplus/leg/en/lvb/l33138.htm
Green Paper: Protection of minors and human dignity in audiovisual and information services (from 1996)	http://europa.eu/scadplus/leg/en/lvb/l24030b.htm
Cybercrime Convention from 23.11.2001 (Council of Europe)	http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG
Stockholm Agenda for Action regarding child pornography from 1996	http://www.ilo.org/public/english/comp/child/standards/resolution/stockholm.htm
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual abuse, signed on the 25th October 2007	http://www.nspcc.org.uk/Inform/policyandpublicaffairs/Europe/Briefings/councilofeurope_wdf51232.pdf
Communication (COM (2000) 890): Creating a safer information society by improving the security of information infrastructures and combating computer-related crime	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:EN:HTML
Council Decision of 29 May 2000 to combat child pornography on the Internet.	http://europa.eu/scadplus/leg/en/lvb/l33116.htm
Joint action to combat trafficking in human beings and sexual exploitation of children	http://europa.eu/scadplus/leg/en/lvb/l33072.htm
Communication on Illegal and Harmful Content on the Internet (1996)	http://www.copacommission.org/meetings/hearing3/eu.test.pdf
UN Convention on the Rights of the Child	http://www.unicef.org/crc/
Charter of Fundamental Rights (2000)	http://europa.eu/scadplus/leg/en/lvb/l33501.htm
Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography	http://europa.eu/scadplus/leg/en/lvb/l33138.htm
Television without Frontiers Directive (03.10.1989)	http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1989/L/01989L0552-19970730-en.pdf
Audiovisual Media Services Directive (11 December 2007)	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007L0065:EN:NOT

Project co-ordinator

stiftung digitale-chancen

Please contact us

Stiftung Digitale Chancen
Managing Director
Jutta Croll
Fasanenstraße 3
10623 Berlin
Tel.: ++49-30-43727730
Fax: ++49-30-43727739
email: jcroll@digitale-chancen.de

Project Manager
Katharina Kunze
Fasanenstraße 3
10623 Berlin
Tel.: ++49-30-43727740
Fax: ++49-30-43727739
email: kunze@yprt.eu

Project within the Safer Internet Programme
of the European Commission

Funded by

Design and Layout: Barbara Kloth, Hamburg


ADICONSUM
associazione difesa consumatori e ambiente


Save the Children
Italia ONLUS


AOL


Bundesarbeitsgemeinschaft
der Freien
Wohlfahrtspflege


CitizensOnline


D.O.M.


die lobby für kinder


eco


Extreme
Media Solutions


Family
Online Safety
Institute


Le Forum des droits
sur l'internet


fsm


F-SECURE
BE SURE.


iSFE


internet abc
Das Portal für Kinder,
Eltern + Pädagogen
www.internet-abc.de


JOHANNISCHES SOZIALWERK E.V.


jugendschutz.net


klicksafe.de


MLL
MANNERHEIMIN
LASTENSUOJELULIITTO


NCH


NICAM


oiat


pegasus


protegeles
.com


Safer
internet.cz