

# Youth Protection Roundtable



youth protection roundtable newsletter nr. 8

february 2009

## news from the field

17.02.09 Every fourth young user puts personal information online

10.02.09 First European agreement of Social Networks - a Step Forward to child safety online Safer Internet Day

28.01.09 French Ministry of education and cultural affairs defends Internet blocking

28.01.09 Childrens voices: "I have nothing to hide"

## YPRT editorial

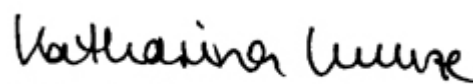
Dear Readers,

the Internet provides huge opportunities to improve life for all users. Especially children and young people are well acquainted with its appliances and can benefit from its use tremendously, but they are also vulnerable.

The Youth Protection Roundtable has developed guidelines to improve youth protection online. The Guidelines help to understand the risks of the online world and to localise the areas where they are most likely to occur. They also provide guidance for the decision how to deal most appropriately with online risks and threats to young people. Knowledge about the effectiveness of supportive technologies for youth protection online is as important for users and responsible adults in the case of minors as getting acquainted with children's online habits and learning about educational measures for improving digital literacy.

At the Final Conference of the project on April 3, 2009 in Berlin, the YPRT Guidelines will be presented to the public. High-level representatives from of the European Parliament, the European Commission, the UNESCO, from welfare organisations and companies around Europe will discuss the guidelines and YPRT members will introduce examples for implementation. The conference will be accompanied by an exhibition of good practise examples of technical and educational approaches to youth protection.

Please be kindly invited to take part in this outstanding event and register free of charge at [www.yprt.eu/registration](http://www.yprt.eu/registration).

  
Katharina Kunze, project manager

Bundesarbeitsgemeinschaft



der Freien  
Wohlfahrtspflege



Univerza  
Ljubljana  
Faculty  
of Social Sciences



JOHANNISCHES SOZIALWERK E.V.

jugendschutz.net





## YPRT report

### Who keeps the gate?

The CIRCAMP project, short for COSPOL<sup>1</sup> Internet related Child Abusive Material Project has chosen its wording carefully. Instead of the more common word 'child pornography' they use the term 'child sexual abuse material' or 'child abusive material' thus emphasising the various ugly faces of maltreatment of children.

As a targeted project CIRCAMP is funded within the Safer Internet Programme with the purpose to enhance law enforcement agencies' analysis of illegal material. CIRCAMP has developed the CSAADF - Child Sexual Abuse Anti Distribution Filter by initiation of Norway in the year 2004. Thirteen countries - Norway, UK, Denmark, Belgium, France, Finland, Ireland, Italy, Malta, Poland, Sweden, Netherlands and Spain are organised in the CIRCAMP project, operated by Norway, eight of them (N, S, DK, Fi, NI, CH, Nz, I) make use of the CSAADF to block websites.

In participating countries, police services receive complaints from the public through hotlines in relation to websites displaying child sexual abuse material. Based on these complaints and investigations, a list of websites containing child abuse material is provided to participating Internet Service Providers by National Police Services. The domain based filtering leads to displaying a STOP page on the computer or mobile device of an Internet user accessing a web site with child abuse content. The system is perceived as a preventive measure not aimed at initiating an investigation against the user, nor to replace traditional investigations into child sexual abuse on the Internet.

Europol describes the following primary aims of the filtering:

- To prevent the re-victimisation of those children who are or have been the victim of abuse
- To prevent accidental access to this illegal and harmful content by the public
- To prevent deliberate access to child abuse material on the Internet
- To reduce the customer base of these illegal websites with the assistance of participating Internet Service Providers (ISP)

In Germany the Ministry of Family Affairs has recently started campaigning for Germany to become partner in the CIRCAMP network.

The major Internet Service Providers covering 95% of Internet traffic are expected to voluntarily sign a contract committing themselves to filtering, based on an URL list operated by the Federal Criminal Police Office, legal regulation might follow the voluntary agreement.

While advocacies for the CIRCAMP system point out the positive impact of reducing access to illegal child abusive material, critical opponents call it censorship and worry about the right to freedom of speech. Also it is mentioned in the debate that filtering on ISP level would open Pandora's box and lead to unlimited demand for filtering on other purpose than child abusive material, f. e. copyright infringement. Other stakeholders mention the need to prosecute persistently the production of child abusive material instead of mere blocking of access to such material. They claim also that most child abusive material is exchanged via peer-to-peer networks or Internet Relay Chats (IRC) and not stored on web servers and thus cannot be blocked effectively by domain name based filtering. Experts also assume that domain based filtering is not very useful to combat the commercial dealing with child abusive material, because for technically skilled users it is easy to circumvent the blocking mechanisms. Finally there are concerns about the correctness of the URLs and about the feasibility to keep the list as secret as necessary. This point is underlined by the publication of two lists from Denmark and Thailand on Wikileaks, although these lists were identified as out-of-date. Several studies support the thesis that domain based filtering is in conflict with other legal regulations and infringes especially the secrecy of telecommunications.

In view of the [YPRT survey results](#) it has to be mentioned that the European experts judged the police as a less relevant gatekeeper with regard to youth protection online. The current debate emphasises once more the need to agree on joint efforts for youth protection. Neither police nor service and content providers will be able to solve the problem alone. Eventually only a collaborative environment ensuring the principle of legal certainty will strengthen the efforts of each single stakeholder to improve youth protection online.

[1] *COSPOL stands for Comprehensive, Operational, Strategic Planning for the Police.*

## research in the field

### Study to male and female behaviour in the social network studiVZ

Altogether ten students of "Media Studies" Film & Television Academy (HFF) "Konrad Wolf" Potsdam-Babelsberg in Germany and their leader Dr. Elisabeth Prommer performed a study about the topic: "Real life extension" in Web-based social networks: The gendered construction of self among student. Their thesis was that the use of web-based social networks is an instrument of constructing new self-identities and not only a way to built up close relationships. For the research the group of students used results of online-interviews they sent to other students of the German city Potsdam. Responses came from 1.210 young students and 1021 of them were registered by studiVZ.

### Change in awareness about data protection

Only half of the Internet users read the data protection policies of their service providers, the TNS Infratest study on behalf of the German Digital Institute and Microsoft Germany revealed. 1014 Internet users were surveyed. The Non-Readers were asked about the reasons for not reading the data protection policies, and it was stated that it takes too long. 13% have not thought about reading them up to now, 14% do not read them principally because they distrust those. The data protection regulations have to be abbreviated and to be make better understandable, so Tom Köhler from Microsoft Germany.

### Privacy Features of European eID Card Specifications

As an authentication token and personal data source, a national eID card is a gateway to personal information. Any unwanted disclosure of personal information as a result of the publishing or use of the card constitutes a violation of the citizen's privacy rights. Apart from considerations of fundamental rights, this is also a serious obstacle to the adoption of eID card schemes and to their cross-border interoperability.

## events in the field

### 02.03.09 - 03.03.09 Democratic Education in a New Europe

Berlin-Brandenburgische Akademie der Wissenschaften (Berlin-Brandenburg Academy of Sciences and Humanities) Jägerstraße 22/23  
10117 Berlin  
Germany

### 02.03.09 Violence and cyber-bullying on Web 2.0

Altes Rathaus, Karmarschstraße 42, Hannover, Germany

### 04.03.09 - 05.03.09 Annual Conference of the Federal Department for Media Harmful to Young Persons

Werk II - Kulturfabrik Leipzig e.V.  
Kochstr. 132  
04277 Leipzig  
Germany

### 11.03.09 - 12.03.09 10. Gautinger Internet-Treffen

Germeringer Straße 30  
82131 Gauting  
Germany

### 20.03.09 - 22.03.09 Ways of Implementing the EU Directives on Violence against Women, Children and Youth: Good Practices and Recommendations

Ljubljana, Slovenia

### 11.06.09 EU Kids Online Conference

London School of Economics, London, UK

## contact information

Stiftung Digitale Chancen  
Fasanenstraße 3  
10623 Berlin  
Tel.: 030-437277-30; -40/Fax: 030-437277 39  
E-Mail: [kunze@ypert.eu](mailto:kunze@ypert.eu)