Challenges and Risks to Children from Internet Content

- Age-inappropriate content: 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 users themselves. Access to the former might be restricted to closed user-groups only, while user-generated content is mostly publicly available and therefore needs special attention. Since today many children and young people have a mobile phone with multimedia functionalities and access to the Internet at their fingertips, it must be considered that they might access age-inappropriate content when 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 volume of user-generated content.

- Illegal content (i.e. racism and child pornography): The type of content classified as illegal depends foremost on national laws, although some type of content is outlawed in most countries. Nevertheless, illegal content is available and can be accessed unintentionally or deliberately by children and young people. Attention should also be paid to children and young people as potential victims of illegal content, e.g. by taking and publishing pictures or videos of child abuse.

- Lack of verification of content: Given that content available through the Internet is often not verified by an independent source, it is important that young people learn to read content with a critical eye and not take everything that is said at face value. User-generated content, characteristic of the Web 2.0 environment, can often be partial, biased or inaccurate. Younger users need to be aware of the dangers of simply believing anything they read online.

- 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 user's own content, the risk of being exposed to content inciting harm is growing. In particular children and young people are in many cases not able to make a realistic assessment of the risks arising from following the instructions given in such websites.

- 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 when they do not have to face 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 a victim of defamation is much more likely online than in reality. Also, defamatory content is harmful to children and young people whose opinion might be influenced by misleading information.

- Inappropriate advertisement and marketing to children: Inappropriate advertisement means the risks of receiving or being exposed to advertising 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 advertisements or be asked to participate in lotteries. Since children are in many cases unaware 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 young people, attention should also be paid to this additional channel for the dissemination of advertisement.

- Privacy: Once published on the web, content can spread rapidly around the world and remain in existence indefinitely. Users, and in particular children and young people, are often unaware of the short-and long-term consequences of publishing texts and pictures they may not want to make available publicly later. Data stored on a server or a platform can be easily accessed by others and people may not be aware of how unprotected their personal data can be. It is important when using the Internet that people fully understand the environment they are working in.

- Copyright infringement: Copyright infringement is a risk mostly related to the conduct of users themselves. Irrespective of whether a copyright has been infringed deliberately or accidentally, the infringement is seen as fraud by the holder and puts the violator at risk of penalty.

- Harmful advice: Forums, blogs and other contact-related areas of the Internet provide a platform for the exchange of information and advice between users. This can be valuable assistance but can also facilitate contact with inappropriate or even more harmful advisors. The risk of receiving harmful advice, in particular for children and young people, is greater in social community platforms or other Web 2.0 applications than on regular websites.

- Identity theft: Getting hold of, and making use of, other people's electronic identity (e.g. user name and password) with the intent to commit commercial or other fraud and to benefit from it is called identity theft. Identity theft is a growing risk as the number of virtual identities is increasing with the number of people online and particularly those using personalized services.

- Money theft/phishing: Phishing refers to the process of harvesting bank details, in particular personal identification numbers (PINs) and transaction authentication numbers (TANs), with the intent to ransack other people's bank accounts. Young people are more likely to not recognize a fake website and to give away their bank details.

- 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 phishing. Another source of commercial fraud can be the sale 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. In the majority of cases, users (and in particular young people and children) are unaware of the consequences of such contracts concluded online.

- Grooming: Grooming refers to paedophiles using the Internet as a means to contact children and young people while concealing their adult identity. They often build their strategy on children's longing for friendship and familiarity. All areas of the Internet that provide 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 social networks) should be taken into strong consideration here, especially as children look at their mobile phone as a particular part of their private life and are mostly on their own when using it. Thus, with the increase of mobile communication technologies and social networks, the risk of falling prey to a grooming attack and then accepting a dangerous invitation has become much greater.

- Bullying: Various types of bullying seem always to be part of people’s lives. Bullying one another is certainly simplified by the Internet due to the anonymity provided by the medium. Children and young people in particular risk being both victims of bullying and offenders. Hence bullying is related to one’s own conduct as well as to the conduct of others. Even though publishing content like defamatory pictures can be part of bullying, the phenomenon is chiefly related to online contact. As mentioned before, multifunctional mobile phones are often used for taking pictures with the intention of bullying and then uploading the pictures to the Internet or sending them via multimedia messaging (MMS) to others. Since many children and young people have a mobile phone equipped with a digital camera, bullying is becoming easier.

- Disclosing private information: When setting up a profile on a social community platform, users are invited to disclose private information to present themselves to the community. Also in chat rooms and forums users may disclose private data to others, such as their address or telephone number. Young people in particular, are unable to foresee the consequences of publishing their private data. They are often unaware that a chat room is not a private but a public area.

- Profiling: With the increasing number of profiles a person can publish on different platforms, there is a greater risk that personal data published on one platform will be merged with data published on other platforms or given away elsewhere (e.g. in polling or raffles). Thus profiles are created that make it possible to directly address the person with potentially unwanted content, services and advertisements. Profiling can be carried out from the website when personal data are displayed publicly, but a more dangerous practice is when profiles of users (or their partial profiles) are harvested from the database behind the website and sold by the platform provider to third parties.