What the IGF requires is IGF a brief write up on

1) The actors involved in the field; various initiatives that people can connect with, and contacts for further information:

2) A brief substantive summary and the main issues that were identified:

and

3) Conclusions and further comments.

(Apart from summarizing the talk of each of the panelists, a "brief substantive summary of the main issues identified" has to be part of this report)

Workshop 106: The mobile Internet in developing economies - child safety dimensions

Original Title: "Children in the Age of Mobile Access: The promises of Internet co-examined with the increasing challenges to Child Safety"
Date/Time: Wednesday 18 November 2009. 14:30-17:30 (note change of time)
Location: Room 5: Shinx, IGF, Sharm el Sheikh

Moderator

Olivier Crépin-Leblond - ISOC England - ocl@gih.com

Workshop Organizers

John Carr, The European Commission, Safer Internet programme - john.carr49@btinternet.com
Anjan Bose, ECPAT International
Sivasubramanian Muthusamy, ISOC India Chennai. - isolatedn@gmail.com

Panel Speakers (in order)

Gitte Stald - Associate Professor, IT University of Copenhagen
Jonne Soininen - Head of Internet Affairs, Nokia Siemens Networks
Rudi Vansnick - Chair, ISOC Belgium
Anjan Bose - ICT Officer, ECPAT International
Ruben Rodriguez - President, INHOPE, The International Association of Internet Hotlines

A recording of this session is available on:
http://www.un.org/webcast/igf/ondemand.asp?mediaID=ws091118-sphinx-pm1

Panel speakers each had about 15-20 minutes to make their presentation, followed by a discussion, with no effective limit on the number of questions from the audience, in order to generate as much involvement from the audience as possible. Some panelists used a deck of slides, whilst others reported verbally.

It was noted that this session was the result of the merger of several proposals, and that the title of the overall session had been changed. The range of presentations reflected this.
Whilst the first three speakers spoke about the dangers of children accessing internet content, the last two speakers concentrated their efforts on the use of new Internet technologies in the context of sexual exploitation of children through the generation of pedophile content, particularly in developing economies.

Gitte Stald - stald@itu.dk

The mobile Internet takes the Internet to a new level of portability. Use of the Mobile Internet is now increasing at a faster rate than standard Internet connectivity using computers. In this field, technology in developing countries is only two years behind technology in developed countries. Whilst most Internet access in the developed world takes place using computers, the developing world is likely to access the Internet using mobile devices. Thsi is due to infrastructure reasons and cost, and means that most children in the developing world will likely access the Internet through a mobile device.

Jonne Soininen - jonne.soininen@nsn.com

Nokia has studied the Internet use on mobile phones and over mobile networks for a long time. Obviously, Nokia has studied also substantially how to keep children safe on-line, and what are the issues that are faced by children and their parents when thinking about the Internet.
The issue of child safety online is no simple matter. This is trapped between multiple gaps that complicate the matters. These are the generation gap, technology gap, and different cultural gaps. As the parent-child relationship should be based on trust, and only works well when trust exists, when the trust deteriorates the whole normal upbringing is at risk. This is especially noticeable in connection with the Internet. Parents may not have the ability to help their children to understand the risks of the Internet. Despite the risks of the Internet, there are many very positive new things coming from the Internet that were not possible before. These can also help to deal with issues, which could not be dealt properly before the ability to have digital options to discuss issues that children feel they cannot discuss with their own parents.
Nokia has been studying different approaches to deal with the child safety issues. With an issue as complex as child safety, it is clear that there is no "silver bullet", and definitely technology solutions - in form of filtering or other means - cannot answer the question alone. The complexities and the different sides of the issue are just not possible to teach for a machine or software to handle adequately. In addition, many of the technical solutions can be circumvented. As the children are mostly more technically skilled than their parents, the parents may not even notice that the technical safeguards have been lifted. Thus, the parents cannot push the responsibility of being a parent onto any technology.
Nokia believes that the right approach of keeping children safe is to educate the parents, and also the children about the capabilities of the devices and the right way of using the Internet. Practically, different actions have been taken ranging from making the consumers fully aware of the capabilities and the potential of Nokia devices, to contributing to activities that teach the children how to constructively use the Internet. A practical example of the later is the "Hiiripiiri" (www.hiiripiiri.fi) project, which has generated educational material provided to teachers to teach for young children to be used in ICT, media and online safety education.
Nokia knows that building the needed trust is a challenging and difficult matter, where both the children and their parents have to learn. However, over time the trust will develop. Trust is like Rome, and it was not built in a day.

Rudi Vansnick - rudi.vansnick@isoc.be

Many parents are clueless and many find it very difficult to effectively engage in their children's on-line activity. The current assumption that end users are responsible for security has been seen by many as inefficient and unrealistic. With ICT use now being more mobile supervision from parents/carers is harder. Also young children will not disclose if something goes wrong.

Protecting children from accessing harmful or illegal content is only possible if parents are able to effectively use the appropriate technical solutions. The first step is good communication between children and their parents. In many cases we see that child victims are from social environments where knowledge and awareness of the dangers are non-existent. It seems as though getting tools and technical solutions to those parents is even more difficult than children accessing harmful and illegal content.
Knowing this, it is very clear that other actions should be considered in order to make every parent, or any other person having the responsibility to protect children, aware of the possible danger while having access to the WWW. We may not consider having fulfilled that task by just putting banners, buttons and whatsoever information on a (web)page.
The *Safe Chat* project for instance has proved children will try to avoid being controlled and will use the non-safe access to that chat room. Moreover, the offender will also try to get access to the Safe chat environment.

Young children have a lifetime to use a particular brand and the reputation of those providing services is crucial not just to parents but to children who one day will grow and have children of their own. Companies have an opportunity to give parents more choice and see safety as a unique selling point. Parents will choose products that they see as safe.
Furthermore many service and mobile providers are global players and operate in less well developed areas where there is an absence of media literacy, and child protection standards, so it is especially important to recognise what help young children need in this context.. This reflects the fact that this is very much a Corporate Social responsibility.

3Cs

- contact
- content
- commercial agreements

3Gs

- gaming
- gambling
- girls

Electronic baby sit.
Schools have the possibility to install special software being some kind of electronic babysitting. Net nanny and Cyberpatrol are good samples. However no standard definition of usage has been done by government or by any official body.

Conclusions.

There is widespread support for some form of standardization for internet filtering tools among consumer organizations and other organizations involved in internet safety issues in Europe. Test results from internet content filter projects have shown considerable variation in the technical capability of the products and in the performance of other variables such as ease of use, security and

over blocking. There are no standard test protocols or agreed processes for evaluating this software.

Each test project has devised its own test method and evaluation system. According to stakeholders

consulted, standardization would:

- help consumers avoid the worst products more easily;
- help raise awareness of filters in countries where they are hardly used;
- help non-governmental organizations give advice to families about how best to use the internet safely; and,
- give consumers added confidence.

Anjan Bose - anjanb@ecpat.net

The mobile phone industry like other technical developments has to undergo research and development for development of their products. In practice, every bit of innovation is tried out for possible failures and design changes
are made in advance to make the product successful. Similar approach should be taken for impact on the lives of children, particularly when they are a significant users of mobile devices worldwide. Applications developed
for mobile phones should take care in advance about the possible child protection issues and in this regard, collaboration with specialized child protection agencies who are experienced on the issues that brings risk to children
on-line, should be in place. Development of features and standards such as customized buttons on the mobile phones (that can be set by the service providers) for reporting easily to dedicated hotlines is one feature that can be easily added. Moreover, mobile service providers should have content filtering in place to make sure that already blacklisted sites (provided by the respective law enforcement of that country) are not accessible through the mobile phones.

What happens when the mobile phone is used for uploading illegal content? With travelling child sex offenders, who may exploit a child at a destination country may also record the scene of the offence, very conveniently on his/her mobile phone and then upload them to sites on-line with a few clicks. With the advent of 3G networks (even in less developed countries and developing countries in the East Asia Pacific for example) and emerging 4G mobile networks, that are going to provide broadband access through wireless, the implications on child protection is huge. Unless the users are registered for the service and the on-line transactions are logged, it will create an environment which perpetrators can take advantage of for exploiting children. Countries should have mechanisms in place, whereby an integrated system of reporting, take down of content and at the same time support and rehabilitation services for the victims should be in place. In many countries, reporting incidents directly to a national hotline through the cell phone has not yet been set up. With the growing popularity of the mobile Internet, it is essential that this channel should also be added for existing hotlines.

Clearly, what is illegal somewhere is sometimes legal elsewhere, so how do we tackle this? In some countries, there are no laws or definitions about child pornography and often this is misused, not only by producing images but also hosting content in such jurisdictions.

Educating children and young people is of course of paramount importance to protect them from exploitation online. But every stakeholder in the society must play their part and assume responsibility to make sure that the framework for protection is in place. Mobile network providers can also come up with interesting and innovative ideas such as downloadable ring tones, animations etc. that alerts and creates awareness amongst young people, use SMS broadcast for promoting events on online safety,

pass on useful safety tips and at the same time alert people against the criminal nature of the offences of sexual exploitation against children on-line and the seriousness of such crimes.

Ruben Rodriguez - rrodriguez@icmec.org

Hotlines can be created to report illegal content, but in areas of the world where there is no legislation, what can a hotline do?
Further progress is required worldwide to harmonize the legislation against child pornography in many countries.
Industry is in a unique position to help the development in emerging countries, all countries are embracing electronic infrastructure development, why not
lead in the efforts to harmonize legislation to safeguard the use of their services? Many models are already being implemented, these examples should be
highlighted to emerging countries as best practices.

Clearly, the increasing use of mobile phones to consult and upload Internet content is making the problem even more pressing.

The mission of the INHOPE Association is to support and enhance the performance of Internet Hotlines around the World, ensuring swift action is taken in responding to reports of illegal content to make the Internet a safer place

Action Points

- Proposal for a session which deals specifically with the Internet generation gap and the education of parents who then need to educate their children about the Internet.