Protecting Children in Cyberspace

Round table discussions
May 14th, 2009

Dr. Imad Hoballah
Commissioner and Board Member
Head of Telecommunications Technologies Unit
Telecommunications Regulatory Authority

The TRA is keen on promoting Internet parental protection and plans to make it a priority for 2009 – working with the HCC

Purpose of today's roundtable

- Raise **awareness** at all levels of the Lebanese society

    - Government and Telecommunications Regulatory Authority responsibilities

    - Parents responsibilities towards the access of their children to inappropriate websites

    - ISPs and Internet cafes responsibilities in dedicating areas for browsing for children

- Discuss the **technical tools** available for parental protection,

- Discuss the **Legal and Regulatory Framework** and its Enforcement regarding protecting children and youths in Cyberspace

- **The subject addresses more than Internet**

    This year, to mark World Telecommunication and Information Society Day, ITU Council adopted the theme, 'Protecting children in cyberspace'

    The theme of this year adopted by the TRA aims to ensure that children can safely access the Internet and its valuable resources without the fear of falling prey to unscrupulous predators in cyberspace

ITU has called upon all stakeholders to promote the adoption of policies and strategies that will protect children in cyberspace and promote their safe access to online resources

Republic of Lebanon
Telecommunications
Regulatory Authority

In order to address issues related to protecting children in cyberspace, ITU has called upon Member States to:

- **Create public awareness** on the issues related to protecting children in cyberspace and to identify policies, best practices, tools and resources for adaptation/use in their countries

- **Support ongoing work aimed at developing Guidelines** on protecting children online for policy makers and regulators

- **Identify risks and vulnerabilities** to children in cyberspace as the Internet and other online resources continue to expand

- **Build resource repositories** for common use

- **Promote capacity building** aimed at strengthening global response in protecting children as they venture into cyberspace

Some Initiatives around the World

Africa

- **African Information Security Association** (AISA) will organize a forum - "Protecting Children and Young People Online" on May 19, 2009
- **The National Working Group (NWG)** will be partnering with the Government of Uganda represented by the ICT Ministry to commemorate WTISD 2009 in Uganda with three activities: an ICT exhibition, a Youth ICT Forum, and a National Symposium on 15th May 2009
- The initiative of Sudan's **Youth National Training Center** is to celebrate WTISD by making technical presentations, workshops, and cultural nights
- **Hugtech Information Links** (HIL) is organizing on 17 May 2009 the *National Youth Summit on the Information Society : NAYSIS* at the Continuing Education Centre (CEC), University of Nigeria, Nsukka
- **i-Vission International** in partnership with The Commonwealth Club of the University of Douala will be organizing a seminar to empower the citizens on cyber criminality as a whole, and the ways through which children are exploited in the Cameroonian context

Arab Countries

- **Arab ICT Organization** will celebrate the day by organizing in partnership with ITU a conference under the theme "Protecting Children in Cyberspace" as well as an exhibition showing the latest technologies in the relevant field, 16 May 2009
- **The Suzanne Mubarak Women's international Peace movement** will avail the 1st Arab Family Safety Kit on line free of charge to Arabic speaking countries.
- **Information Technology Authority**, Oman will be visiting schools across the country with the aim of raising awareness of students. Posters, pamphlets, and students kits will be distributed in schools and awareness lectures will be conducted for students and teachers.

Some initiatives around the world (cont)

Europe and Asia

- **European Network and Information Security Association** (ENISA)is promoting a set of security posters aim at raising awareness of parents to enhance the safety of children using virtual worlds and the Internet
- **HiPiKids** is launching HiPiCUBE Kids' Internet Operating System in Beijing China focusing on operating a better Internet for children via a proprietary Kids Internet Operating System and Internet devices such as mobile phones, desktop computers, laptops, net books, MID or a SoC Flash drives
- *Internet Sans Creinte* the French national program to raise awareness of the online risks among young people which represents France in the European project *Safer Internet Plus* which gathers 26 countries from the European Union is promoting a special program for teenagers between the ages of 12 and 16
- *ODISHA TELECOM DEVELOPMENT FORUM* OTDF in India has proposed to observe and celebrate WTISD to create public awareness
- **Pakistan Fair & Exhibition Corporation** organizes from 17-19 May 2009 the Pakistan Telecom Expo and Conference (PTEC 2009) where it will calls upon all stakeholders (policy makers, regulators, operators and industry) to promote the adoption of policies and strategies that will protect children in cyberspace and promote their safe access to online resources

Best Practices Used Around the World

Child Online Protection Act (COPA) , USA

- **1996** - Communications Decency Act (CDA), part of the Telecommunications Act of 1996

- **1997** - Supreme Court ruled 9-0 in [Reno vs. American Civil Liberties Union](): CDA unconstitutional restriction on Internet

- **1998** - Congress passed, President Clinton signed into law Child Online Protection Act (COPA), the "sequel" to CDA. COPA establishes criminal penalties for commercial distribution of material harmful to minors.

- EPIC joined with ACLU and others in lawsuit to strike down the law

- **1999 -** federal district court in Philadelphia issued an injunction preventing the government from enforcing COPA

Challenges to the Child Online Protection Act (COPA)

- **May 13, 2002** - Supreme Court Maintains Ban on COPA Enforcement
- Court Strikes Down Censorship Law (Again)
- **June 29, 2004** - Supreme Court Maintains Block on Web Censorship Law
- **July 22, 2008** - In ACLU, EPIC Case, Federal Court Strikes Down Internet Censorship Law
- **January 21, 2009** - Supreme Court Refuses to Hear Internet Censorship Appeal

Australia

- Web Censorship plan heads towards a dead end
- An Opposition's communications spokesman obtained legal advice saying if Government is to pursue mandatory filtering regime "legislation of some sort will be required"
- A very strong case for blocking other legal content refused classification

European Parliament and Council

The Commission:

- Encourages cooperation and the sharing of experience and best practices between existing self and co-regulatory bodies, with a view to enabling all users, but especially parents, teachers and trainers, to report illegal content.
- Believes that self-regulation of the audiovisual sector is proving an effective additional measure, but it is not sufficient to protect minors from messages with harmful content.

The constant and fast development of new information and communications technologies makes it urgent for the Community to ensure full and adequate protection for citizens' interests

The EUROPEAN PARLIAMENT AND COUNCIL therefore recommends

- Take actions to enable minors to make responsible use of audiovisual and on-line information services by improving the level of awareness among parents, teachers and trainers

- Draw-up a code of conduct in cooperation with professionals and regulatory authorities at national and Community level

- Adopt a quality label for service providers, so that users can easily check whether or not a given provider subscribes to a code of conduct

- Examine the possibility of creating filters which would prevent information offending against human dignity from passing through the Internet

- Develop measures to increase the use of content labeling systems for material distributed over the Internet

- Explore the possibility of supporting the establishment of a generic second level domain name reserved for monitored sites committed to respecting minors and their rights, such as .KID.eu

Possible Actions for a Protected World

Media Literacy as one possible action

- Continuing education of teachers and trainers, in liaison with child protection associations

- Internet training aimed at children from a very early age, including sessions open to parents

- Integrated educational approach forming part of school curricula and media literacy programs

- National campaigns aimed at citizens, involving all communications media

- Distribution of information packs on possible risks of the Internet and setting up of hotlines to report complaints

Possible actions by the industries and the parties concerned for the benefit of minors

- Provide users with filtering system when they subscribe to an access provider
- Offer access to services intended for children/equipped with automatic filtering systems
- Introduce incentives to provide a regularly updated description of the available sites
- Post banners on search engines to the availability both of information about responsible use of the Internet and of telephone hotlines

Filters empower parents; otherwise, children are victimized by the surfeit of dangerous content. Main conference topics

The Internet: changing the way people live

Self-regulation of Internet content: towards a systematic, integrated and international appr**oach**

Internet industry: developing and implementing codes of conduct

Sharing responsibility: self-regulatory agencies enforcing codes of conduct

Governments: supporting and reinforcing self-regulation

Self-rating and filtering systems: empowering user choice

Internet filtering: ensuring youth protection and freedom of speech

Hotlines: communicating and evaluating content concerns

International cooperation: acting against content where it is located

The legal framework: limitations on liability

Law enforcement: cooperation and continuous training

A "learning system": education and constant evaluation

Possible Actions to Protect Minors Online

- Some categories of technologies
  a) Age verification, Identity Authentication, and Biometrics
  b) Filtering, Auditing and Text Analysis
- Technologies presents **privacy and security issues** that must be weighed against potential benefits
- Some technologies carry an economic cost and some require involvement by parents and teachers
- Relying on technologies may not protect most vulnerable minors
- Steps by the social network sites are helpful in mitigating some risks, but none is fail-safe
- Technology can play a helpful role and development of technologies will enhance protections for minors online and support institutions and individuals involved in protecting minors
- Supporting institutions and individuals working on the net are effective participants in the protection of minors

- **<u>There is no one technological solution or specific combination of technological solutions</u>** to the problem, but a combination of:
  - Technologies
    - Parental Oversight
      - Education
        - Social Services
          - Legal and Regulatory Framework and Law Enforcement
            - Sound Policies by Social Network Sites and Service Providers

- All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors

- Greater resources should be allocated to
    - **Schools, libraries, and other community organizations**: assist them in adopting risk management policies and in providing education about online safety issues
    - **Law enforcement** for training and developing technology tools, and to enhance community policing efforts around youth online safety
    - **Social services and mental health professionals who focus on minors and their families**, so that they can extend their expertise to online spaces and work with law enforcement and the Internet community to develop a unified approach for identifying at-risk youth and intervening before risky behavior results in danger
- **Greater resources also should be allocated for ongoing research** into the precise nature of online risks to minors, and how these risks shift over time and are (or are not) mitigated by interventions
- **Law enforcement should work with researchers** to help them gather data on registered sex offenders' use of Internet technologies,
- **Technology companies should provide researchers with appropriately anonymized data** for studying their practices

General Recommendations

- Establish a joint Public-Private Administration (PPA)
  - Develop a **National Strategy** for Cyber Security
  - Coordinate **Nationally** between government, public and private sectors
  - Create **National Incident Management** Capabilities
  - Promote a **National Culture** of Cyber Security (and awareness campaign)
    - Kick start a public children information and education campaign (media & schools)
    - Develop an awareness and education website specifically for children
  - **Secure government cyberspace**
  - Improve **regional and international coordination** and cooperation
- Possible Security Models/Templates
  - Comprehensive laws governing collection, use and dissemination of personal data
  - **Implement a newly-enacted requirement** that agencies include information security strategic objectives in their information technology procurement decision-making
  - **Specific rules for the different industries**, information types, & technologies
  - Introduce Internet child protection legislation

General Recommendations - Possible parental and social workers Measures

Parents must get actively involved

- **Educate themselves about the Internet** & ways children use it as well as about technology in general
- **Explore and evaluate the effectiveness of available technological tools** for their particular child and their family context, and adopt those tools as may be appropriate
- **Be engaged and involved** in their children's Internet use
- **Be conscious** of the common risks youth face to help their children understand & navigate the tech
- **Be attentive to at-risk minors** in their community and in their children's peer group;
- Recognize when they need to seek help from others
- Discuss safety aspects of Internet usage with children

- Take an active interest in your child's online activities

- Periodically check browsing history

- Avoid placing computers in secluded places

- Limit computer usage and amount of time spent online

- Install "nanny software" with filtering and monitoring capability

General Recommendations - Possible Regulatory Measures - TRA

- The TRA could specify **binding recommendations**, to ensure information security on telecommunications infrastructure, applicable to all providers
- Make sure that the telecommunications regulatory framework facilitates the establishment of **modern licensing** and the **adoption of E-Commerce, Cyber laws,** and Child Protection Laws
- **Licenses must be clear on requirements**
- Set **requirements on the service providers (**and on their resellers) to maintain network and services security standards (e.g., ISO/IEC 27K) and public safety
- Update **consumer protection** regulations to include Cyber Security and **Child Protection** requirements
- Develop **processes and procedures** with **enforcement** authorities

- **Apply what is required of every user/resellers**
- **Implement careful design** and plan the networks in close coordination with the TRA
- Adhere by the social responsibility to **educate customers**/end users about Cyber Threats/Security and about child protection
- **Sharing responsibility by developing** and implementing **codes of conduct** and **self-regulatory agencies enforcing those codes of conduct**
- Provide users with filtering system when they subscribe to an access provider
- Offer access to services intended for children/equipped with automatic filtering systems and provide a regularly updated description of the available sites
- Post banners on search engines to the availability both of information about responsible use of the Internet and of telephone hotlines
- Adopt Acceptable Use Policies or Terms of Service Agreements
- Promote safe Internet education and awareness
- Create parent/children education sections on their websites
- **Adhere to public order**, **public decency** and applied rules and regulations
- Monitor social networking sites, forums and chat rooms for sexual predators
- Cooperation between law enforcement & ISPs to shut down or block illegal activities
- Require public internet access to install "nanny filters"

- Offer filtered content upon customer request

- Offer subscriber bundled "nanny" software

- Implement careful design and plan the networks in close coordination with the TRA

- Adopt **technological solutions** e.g., physical/logical security (combined with legislative protections)

- Use **firewalls, Anti-Virus & Anti-Spam** gateways and Anti-spam Email Filtering System

- Continuously **update the front-end nodes** and equipments

- Implement systemic **mirroring and Network backups** of **Data Centers** in corporations to protect the Information Systems (IS) and the businesses

- **Secure access to the network** (e.g., user and data authentication)

- **Preserve personal data** for as long as is necessary (e.g., 1 year)

- Establish and maintain reasonable **procedures to protect the confidentiality/integrity** of personal data

- **Provide access to "LEGALLY AUTHORZIED ENFORCEMENT PERSONNEL**" as required

It is not possible to block undesirable content without inadvertently blocking some innocent content too

- **Parental control bar (free) http://www.parentalcontrolbar.org**

- **Parental filter http://www.parentalfilter.eu**

- **NetNanny – monitoring/blocking software http://www.netnanny.com**

- **Trend Micro Internet Security – Anti-Virus + Firewall with Parental Controls**

- **CyberPatrol Parental Controls Software – Anti-Virus + Firewall with Parental Controls**

- **Norton Internet Security (NIS) – Anti-Virus + Firewall with Parental Controls**

- **McAfee Security Suite – Anti-Virus (AV) + Firewall with Parental Controls**

- **CA Internet security suite – Anti-Virus + Firewall with Parental Controls**

- **SpectorSoft (www.spectorsoft.com) – monitoring of PC – Key logger included**

- **Google search "internet monitoring software"**

- **Provide special access areas for minors with special access constraints and protection**
    - Age verification, Identity Authentication, and Biometrics
    - Filtering, Auditing and Text Analysis
- **Keep logs** of use for required period
- **Allow inspection and provide access** to the data stored, when "**legally and judicially**" required
- Provide ability to **monitor the information traffic** and compilation of data and information **directly** when "**legally and judicially**" required (without accessing the data and violating the rules)
- Ability to **intercept the data** (content) when "**legally and judicially**" required
- Personal data shall be
    - **Appropriate, useful and not excessive**, and it is collected and **used for informative** purpose only
    - **Accurate and updated** as needed
    - **Preserved for as long as is necessary**
    - **Processed in a legal and fair manner** and in accordance with the rules (as stated in the Law!)
    - Take all necessary measures to **prevent unauthorized access** (or miss-manipulation or loss) to personal data – also protect personal information collected from children
    - **Written contractual obligation to ensure that the data owner must comply with the relevant legislation, and to ensure that such arrangements are in place and implemented**

Republic of Lebanon
Telecommunications
Regulatory Authority

Thank you!

www.tra.gov.lb