Asia-Pacific
Economic Cooperation

2009/TEL39/SPSG/SYM/018

Answers to APEC Children Protection Project Questionnaire

Submitted by: Japan

APEC 2009
Singapore

APEC-OECD Joint Symposium on Initiatives
Among Member Economies Promoting Safer
Internet Environment for Children
Singapore
15 April 2009

APEC Members

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

Issues include: Access to inappropriate material (for more information on what constitutes inappropriate content see http://www.acma.gov.au/WEB/STANDARD/pc=PC_90103), cyberbullying, scams/fraud and identity theft, and online grooming. For more information see http://www.netalert.gov.au/advice.html.

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

The Australian Government's National Filter Scheme provided people residing in Australia with access to free PC filter products. The scheme closed to new users as of 1 January 2009, although ongoing support for existing users will continue until 30 June 2010. See http://www.netalert.gov.au/.

Mandatory ISP level filtering is to be introduced which will block an Australian Communications and Media Authority blacklist of prohibited internet content. Consideration is also being given to more sophisticated filtering techniques for individual families who wish to exclude additional online content in their own homes. See http://www.dbcde.gov.au/communications_for_consumers/funding_programs__and__support/cyber-safety_plan/internet_service_provider_isp_filtering.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

Online content is regulated through the Online Content Scheme under Schedule 5 and 7 of the *Broadcasting Services Act 1992.* The Scheme is designed to protect consumers, particularly children, from exposure to inappropriate or harmful material.

The Scheme applies to content accessed through the internet, mobile phones and convergent devices, and applies to content delivered through emerging content services such as subscription-based internet portals, chat rooms, live audio-visual streaming, and link services.

Under Schedule 7, prohibited content includes content that has been classified or is likely to be classified:

- RC (refused classification);
- X18+;
- R18+ unless it is subject to a restricted access system; and
- MA15+ and is provided on a commercial basis (i.e. for a fee) unless it is subject to a restricted access system.

These prohibitions are backed by strong sanctions for non-compliance including criminal penalties for serious offences.

Where content is hosted in Australia and is found by the Australian Communications and Media Authority (ACMA) to be prohibited, ACMA has the authority to direct the relevant content service provider to remove the content from their service. Where content is not hosted in Australia and is prohibited, ACMA will notify the content to the suppliers of approved filters, so that access to the content using such filters is blocked.

In addition, if ACMA considers the content to be of a sufficiently serious nature, it will notify the content to an Australian police force or to an INHOPE member hotline.

Schedule 7 includes a complaints-based mechanism administered by ACMA. Information, including instructions for making a complaint to ACMA, is available at www.acma.gov.au/hotline.

(3) Contents of voluntary efforts, such as self-regulation?

(Does your economy have any self-regulation?

If there is some self-regulation, please describe the overview.

(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

Australia's scheme for internet content is 'co-regulatory', with roles for both industry and government. The scheme allows for and encourages the development of codes of practice by and for internet service providers (ISPs) and providers of online and mobile content. ACMA will register a code once it is satisfied that it has met certain criteria. The matters that must be dealt with in the codes, and the criteria for registration, are specified in Schedule 5 and Schedule 7 to the *Broadcasting Services Act 1992*.

The codes were developed by the Internet Industry Association (IIA) and apply to all Australian ISPs and providers and hosts of content with an Australian connection. ACMA may direct an ISP or content service provider to comply with a code if satisfied that they are not already doing so. Failure to comply with such a direction may amount to an offence under the Act.

The codes are at www.iia.net.au/index.php?option=com_content&task=category&sectionid=3&id=87&Itemid=33.

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

The Australian Government has a strong commitment to the promotion of cybersafety. For information on the government's plan, see http://www.dbcde.gov.au/communications_for_consumers/funding_programs__and__support/cyber-safety_plan .

The Australian Communications and Media Authority operates a number of best practice cybersafety programs, as below:

ACMA's outreach program has been expanded to provide additional general cyber-safety awareness presentations to teachers, parents and students which highlight the key issues and strategies to minimise potential online risks.

In February 2009, ACMA will also roll out an accredited Professional Development Workshop for Educators. The workshop will cover topics including how children use technology, digital literacy, cyberbullying, identity protection and the legal responsibility of schools to minimise risk. Resources will be provided to teachers to help establish an effective cyber-safety program in their school.

A program for trainee teachers is also being developed in consultation with the Deans of Education to ensure that all new student teachers achieve competency in cyber-safety.

ACMA is also continuing to develop and expand its existing education materials for young people, including:

- Cybersmart Detectives, the interactive online safety game that teaches children how to keep safe online (http://cybersmart.engagelive.net/);
- a new, multi-media resource for use by young children to be released in mid 2009; and
- its suite of cyberbullying materials 'Let's Fight it Together'.

ACMA currently operates an online safety website at www.cybersmartkids.com.au, and is in the process of developing a new, expanded cyber-safety website which will provide up-to-date information for parents, as well as information and activities specifically designed for children. The website will contain a link to an online help line, which will allow young people to chat online with a trained adult about issues that have happened to them online.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

In order to promote cooperation, the Minister for Broadband, Communications and the Digital Economy has formed a Consultative Working Group on Cybersafety. The Group comprises representatives from industry, government, and community groups. Information about the role and composition of the CWG is at:
http://www.minister.dbcde.gov.au/media/media_releases/2008/035

The Government is also in the process of setting up a Youth Advisory Group, to advise the CWG on cybersafety issues.

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

ACMA is a member of the European based INSAFE network of internet safety agencies, and it also has collaboration mechanisms with international safety organisations including NetSafe (New Zealand) and ChildNet International (UK) which assist it in developing safety resources and keeping across trends.

ACMA is also a member of the International Association of Internet Hotlines (INHOPE). INHOPE member hotlines deal with complaints about illegal internet content, actioning around 9,600 reports of child abuse material online per month. As well as expediting the handling of illegal material, membership of the INHOPE network provides a mechanism for information exchange on matters such as investigation techniques, hotline promotion, and the welfare of staff dealing with illegal content.

APEC Child Protection Project Questionnaire

Response from Canada

February 2009

Note: the following response is a non-exhaustive list of initiatives underway within Canada, recognizing the various levels of governments, and multitude of stakeholders, making significant contributions to this issue.

1. Current experiences regarding information considered harmful to children within economies: what kinds of issues is each economy concerned with?

Issues include, in no particular order: cyber-bullying; enhancing the protection of children's privacy online; ensuring a trusted, safe and positive online environment for children; empowering children online (through education and awareness); and preventing the exploitation of children online.

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

Within Canada, the discussion of technologies designed to manage access to information that may be considered harmful to children is set into a legislative context, outlined elsewhere in this survey, designed to protect freedom of expression.

Cleanfeed Canada

Cleanfeed Canada (www.cybertip.ca/app/en/cleanfeed) is an undertaking of the Canadian Coalition Against Internet Child Exploitation (CCAICE); a group which includes Cybertip.ca, Internet service providers, federal and provincial governments, and law enforcement. This initiative aims to reduce accidental access to child sexual abuse images as well as to discourage those trying to access or distribute child pornography.

Cybertip.ca created and maintains a regularly updated list of specific foreign-hosted Internet addresses (URLs) associated with images of child sexual abuse and provides that list in a secure manner to participating ISPs. The ISPs' filters automatically prevent access to addresses on the list. There is essentially no "human" intervention on the part of participating ISPs. ISPs do not have input into creating the list nor knowledge of what is contained on it. There is no legal obligation for ISPs to participate; ISPs may have technical or other reasons for not adopting the system. Most major ISPs do participate, including: Aliant, Bell, MTS Allstream, Rogers, Sasktel, Shaw, Telus, and Videotron.

The system is built to only prevent access to Internet addresses specifically containing child pornography images. A minimum of two analysts must review content and approve the URL before submission. Other automated checks are also performed to ensure the integrity and accuracy of information on the list. Additionally, while the child pornography provisions under the Criminal Code concern children under 18, the tipline only adds URLs displaying images of prepubescent children being assaulted or who are posed deliberately in a sexualized manner.

Only those URLs hosted outside Canada are added to the database. Law enforcement officials proceed with their normal course of investigation for those sites hosted within Canada. IP address lookup software is used to automatically exclude Canadian URLs.

If any party responsible for the hosting, content or design of material, or any person who seeks access to a URL stored within the Blocking List maintained by Cybertip.ca for the purpose of Project Cleanfeed Canada complains, appeals or makes representation about the accuracy of the content assessment, Cleanfeed Canada has published procedures for appeal online at: www.cybertip.ca/app/en/cleanfeed_p1#anchor_menu).

(2) Does your economy have relevant laws and regulation?

A. Laws of General Application and the Telecommunications Act

Within Canada, “laws of general application” apply to the Internet, i.e., content that is illegal offline is also illegal online. Issues relating to illegal content are addressed by law enforcement bodies. In its 1999 New Media Decision (www.crtc.gc.ca/eng/archive/1999/PT99-14.htm), the Canadian Radio-television and Telecommunications Commission (CRTC) interpreted the *Broadcasting Act* to exclude most Internet and new media services and exempted the rest from regulation. It was noted that regulating the Internet based on controlling traffic or access to content was difficult, costly and highly susceptible to bypass, and could also be counter-productive. Instead, generally applicable Canadian laws, coupled with self-regulatory initiatives, were found to be a more appropriate means for dealing with offensive material than the *Broadcasting Act*.

The topic of offensive content is an issue of consumer choice, user empowerment, and responsible industry practices. Canada’s *Telecommunications Act*, 1993 (available online at: http://laws.justice.gc.ca/en/T-3.4/index.html), specifically limits the role of Canadian telecommunications services providers in interfering with content transmitted over their networks. Section 36 stipulates that “*except where the Commission approves otherwise, a Canadian* *carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public*."

B. Other, related, legislative provisions

Canada's Criminal Code: Provisions to prevent sexual exploitation of children on the Internet

In June 2002, Bill C-15A, an act to amend the Criminal Code with respect to the sexual exploitation of children on the Internet, received royal assent. The amendments created new enforcement measures for these offences, and extended beyond the offence of possessing and distributing child pornography, to the offence of accessing child pornography. The amendments also made it an offence to communicate with children via a computer system for the purpose of facilitating or committing certain sexual offences, such as child luring or abduction.

Specifically:

- Amendments to section 163.1(3), include wording such as "transmission" to ensure that an offence applies to the distribution of child pornography over the Internet — including via e-mail, and by posting material on Web sites. A clause was also added to stipulate that the custodian of a computer system (such as an Internet Service Provider, or ISP) is not guilty of any offence merely for providing the telecommunication facility used by the person committing the offence.
- Luring of Children on the Internet: In 2002, Section 172.1 was added to the Code to criminalize electronic communication with a person believed to be a child for the purpose of facilitating the commission of sexual offences. Depending on the offence, the requisite age (real or believed) of the intended victim varies from 14 to 18.
- Deleting Child Pornography from Internet Sites: If there is reasonable grounds, a judge can issue a warrant of seizure on any material from a computer system presumed to constitute child pornography. The ISP or custodian of the system may be ordered to remove the material, provide the court with electronic copies of it, and/or provide information on the identity and location of the person who posted it. If the material is proven to be child pornography, the custodian may be ordered to delete the material.

Personal Information Protection and Electronic Documents Act

Bill C-6, an act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed, received royal assent in April 2000. The *Personal Information Protection and Electronic Documents Act*, or PIPEDA (http://laws.justice.gc.ca/en/P-8.6/), addresses the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use of disclose personal information in the course of commercial activities.

A statutory review of Canada's private sector privacy legislation, which began in 2006, is currently underway. Having recognized that the privacy of children can be vulnerable, particularly in an online environment, Canada is examining the issue of consent with respect to the collection, use or disclosure of personal information of children in a commercial context in order to determine the necessity and feasibility of amending the Act. Under consideration is whether to amend the Act to add explicit provisions for the protection of the personal information of children, such as clarifying the concepts of knowledge and consent relating to the collection, use or disclosure of personal information. Currently, the legislation identifies that "the knowledge and consent of the individual are required" (Schedule 1, Principle 4.3) and that to make the consent meaningful the purposes must be stated so that "the individual can reasonably understand how the information will be used or disclosed." (Schedule 1, Principle 4.3.2)

Canadian Human Rights Act

Section 13 of the *Canadian Human Rights Act* (http://laws.justice.gc.ca/en/H-6/index.html) prohibits the communication by means of a telecommunication undertaking (including the Internet) of messages that are likely to expose a person to hatred or contempt on the basis of: race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability; or conviction for which a pardon has been granted.

(3) Contents of voluntary efforts, such as self-regulation?

(Does your economy have any self-regulation?

If there is some self-regulation, please describe the overview.

(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

Several voluntary codes are in place to support the protection of children on the Internet. These include:

- Canadian Association of Internet Providers (CAIP) Code of Conduct (www.caip.ca/issues/selfreg/code-of-conduct/code.htm)
- Canadian Standards Association (CSA): Model Code for the Protection of Personal Information (www.csa.ca/standards/privacy/default.asp?load=code&language=english)
- Canadian Code of Practice for Consumer Protection in Electronic Commerce: www.cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00064.html

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues?   What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

A. Media Awareness Network

The Government of Canada is an active supporter of the Media Awareness Network, a Canadian not-for-profit centre of expertise and excellence in media education (www.media-awareness.ca). Its vision is to ensure children and youth possess the necessary critical thinking skills and tools to understand and actively engage with media. Its mission is to be the leading Canadian provider of media education resources and awareness programs for educators, parents, children and youth. In executing its mission, the Media Awareness Network is guided by its underlying philosophy of educating, not advocating, and by its fundamental goals to: develop and deliver high-quality Canadian-based media education resources; provide leadership in advancing media literacy and contributing to the development of public policy on issues related to the media; and build broad public support for media education.

MNet began studying the implications of the Internet for young people in 1996, and in 1999 launched Web Awareness Canada. This program uses a unique delivery model based on partnerships with public libraries, the education sector, parent groups, and community organizations. Its primary focus has been to help bring teachers and librarians up to speed on the issues emerging as young people go online. MNet licenses tools that can be purchased for professional development, including workshop topics such as: online safety, protecting personal privacy, authenticating information, and marketing to young people. Programs include:

- Be Web Aware: The Be Web Aware initiative includes a comprehensive Web site (www.bewebaware.ca). The site, developed by Media Awareness Network, is full of information and tools to help parents teach their children to handle the potential risks associated with going online. (www.media-awareness.ca/english/special_initiatives/be_web_aware/index.cfm)
- MNet and the Girl Guides of Canada have worked together to create a new Challenge badge for all levels of Guiding. The badge, released during National Media Education Week (November 3-7, 2008), is technology based and aimed at teaching girls and young women about internet literacy.
- Passport to the Internet: Student tutorial for Internet literacy (Grades 4-8) (www.media-awareness.ca/english/catalogue/products/descriptions/passport.cfm)
- Privacy Playground: The First Adventure of the Three CyberPigs (www.media-awareness.ca/english/games/privacy_playground)
- Jo Cool or Jo Fool: Interactive Module and Quiz on Critical Thinking for the Internet (www.media-awareness.ca/english/games/jocool_jofool)
- Co-Co's AdverSmarts: An Interactive Unit on Food Marketing on the

Web (www.media-awareness.ca/english/games/coco/)

- Allies and Aliens: Interactive Module on Online Hate (www.media-awareness.ca/english/games/allies_aliens/)

MNet developed its ***Young Canadians In A Wired World (YCWW)*** research program (www.media-awareness.ca/english/research/YCWW/) in order to build an extensive database about the role of the Internet in the lives of young people. The research project tracks and investigates the behaviours, attitudes, and opinions of Canadian children and youth with respect to their use of the Internet. From focus group discussions, interviews with parents and national student surveys, MNet has harvested a wealth of information and insights about how Canadian youth, who are among the most connected in the world, are using the Internet. The research raises a number of issues that demand society's attention and, more importantly, highlights the importance of adult involvement and education as key responses in helping young people make wise online decisions. To-date, two series of research have been completed.

B. Cybertip.ca

Cybertip.ca has developed a number of fact-sheets designed to protect children from exploitation on the Internet. They are available online at: www.cybertip.ca/app/en/fact_sheets.

(5) Please describe domestic cooperation framework in your economy.

(Example: public-private partnerships, inter-ministerial cooperation, cooperation among businesses, etc.)

In following with the CRTC's 1999 decision not to regulate "new media" under the *Broadcasting Act*, Industry Canada convened a committee with other federal government departments such as Justice Canada, Health Canada, Canadian Heritage, the Solicitor General and the Royal Canadian Mounted Police (RCMP), in order to develop a set of practical initiatives that would not require new legislation.

A. Cyberwise Strategy:

Recognizing that prevention through public education is an important element of any strategy to address Internet related activity, the federal government, in consultation with non-governmental and private sector partners, developed the ***Canadian Strategy to Promote Safe, Wise and Responsible Internet Use (Cyberwise)*** in 2001. The Strategy was designed to increase public awareness of issues relating to illegal and offensive Internet content by providing parents and teachers with access to a broad collection of tools and resources distributed to schools and libraries across Canada.

The strategy consisted of five elements:

1. ***Supporting initiatives that educate and empower users***, including

working with arms-length organizations already engaged in the field, such as the Media Awareness Network (www.media-awareness.ca) and the Canadian Association of Internet Providers (www.cata.ca/Communities/caip/), to establish an education and awareness strategy; advising private-sector efforts to develop content rating systems; and encouraging the use of software tools such as filtering and labeling;

2. ***Promoting effective self-regulation***, i.e., industry-led establishment of fair, standardized business practices, voluntary codes of conduct, and initiatives to educate consumers about choosing an Internet Service Provider;
3. ***Strengthening law enforcement***, including amendments to Canada's Criminal Code, the creation of a National Coordination Centre within the RCMP to address child sexual exploitation, and continued work on a comprehensive national strategy to combat Internet-based online child sexual exploitation;
4. ***Implementing hotline reporting systems (Cybertip.ca)***, to respond to concerns that Canadians were unaware of where they could report concerns about content. Hotlines are considered to be the key link between Internet users and law enforcement bodies, and are particularly useful as not all content is necessarily illegal;
5. ***Fostering international collaboration***, recognizing that the international nature of the Internet gives rise to cross-jurisdictional issues. Issues must be addressed globally, at the policy and law-enforcement levels.

Through this work, Canada has been successful in achieving commitment for a largely self-regulatory, non-legislative approach.

Cyberwise: lessons learned

Recognizing that many issues continue to evolve, Canada sees partnerships between various stakeholder groups, within both the private and public sectors, as critical. Similarly, Canadians support a collaborative approach, and see themselves as important part of the solution.

B. Ongoing initiatives

Cybertip.ca

Cybertip.ca is Canada's national tipline for reporting the online sexual exploitation of children. The tipline was originally established as a pilot project in 2002, and is owned and operated by the Canadian Centre for Child Protection. As Canada's national tipline, Cybertip.ca's mandate is to protect children from online sexual exploitation by:

- Receiving and analyzing tips from the public about potentially illegal material, as well as activities regarding the online sexual exploitation of children, and referring any relevant leads to the appropriate law enforcement agency; and
- Providing the public with information and other resources, as well as support and referral services, to help Canadians keep themselves and their families safe while using the Internet.

Cybertip.ca contributes to public education and prevention through its online safety strategies and national awareness campaigns.

Cybertip.ca accepts and addresses online and telephone reports from the public regarding: Child Pornography (child abuse images and material); online luring; child exploitation through prostitution; travelling to sexually exploit children; and child trafficking. On average, Cybertip.ca receives over 700 reports and 800,000 hits to its website per month. All reports that are in contravention of the Criminal Code (Canada) are sent to police for possible investigation. As of January 2008, reports to the tipline had resulted in 43 arrests and the removal of 2,850 websites from the Internet. In establishing Cybertip.ca, the Canadian Centre for Child Protection also worked closely with other successful tiplines around the world.

Canada's National Strategy to Protect Children from Sexual Exploitation on the Internet

On May 12, 2004, the Minister of Public Safety and Emergency Preparedness Canada, announced Canada's National Strategy to Protect Children from Sexual Exploitation on the Internet. Under the Strategy, the Government of Canada dedicated $43 million over five years to ensure a comprehensive, coordinated approach to protecting children on the Internet, and pursuing those who use technology to prey on them. The National Strategy has three main objectives: enhancing enforcement capacity; providing for public reporting and education to prevent victimization; and developing partnerships with the e-learning industry, the private sector and other levels of government to foster effective public awareness, education and crime prevention strategies.

Key elements include:

- The **National Steering Committee on Internet-Based Child Sexual Exploitation:** In January 2003, the RCMP and the Ontario Provincial Police created the National Steering Committee on Internet-Based Child Sexual Exploitation. The Committee, which is composed of members from law enforcement agencies across the country, as well as federal Government officials, provides strategic direction and leadership to law enforcement across Canada, particularly in the development of investigative standards and information and intelligence sharing. One of the Committee's first recommendations was that a central, coordinated unit be created to advance law enforcement strategies and provide for enhanced law enforcement capacity to deal with these types of crimes. Building on this recommendation, a national coordination centre was created in April 2003 at the RCMP, in an effort to improve coordination of law enforcement activities in the area of child sexual exploitation, and to address capacity gaps, overlaps in investigations, and requests for assistance and demands from Canadian and international law enforcement.

- The **National Child Exploitation Coordination Centre:** The NCECC was established in 2003 as the law enforcement component of Canada's National Strategy to Protect Children from Sexual Exploitation on the Internet. The Centre was created in response to the recognition that the Internet was being more frequently used to facilitated sexual exploitation crimes against children including the exchange of child sexual abuse images and child luring. The mandate of the NCECC is to reduce the vulnerability of children to Internet-facilitated sexual exploitation by identifying victimized children; investigating and assisting in the prosecution of sexual offenders; and, strengthening the capacity of municipal, territorial, provincial, federal, and international police agencies through training and investigative support. The NCECC is Canada's contact point for files involving Canadian victims and suspects. The Centre provides a number of services to law enforcement including the ability to respond immediately to a child at risk, the coordination of investigative files, expertise in victim identification techniques, management of multi-jurisdictional cases, operationally relevant research, and training specific to online child sexual exploitation investigations. The NCECC also manages and provides training for the Child Exploitation Tracking System (CETS), an intelligence tool that enhances information sharing among Canadian investigators.

- The **Criminal Intelligence Service Canada (CISC)**
  The CISC executive is made up of the Commissioner of the RCMP, the Commissioner of the OPP, and major police departments across Canada. Each province has a sexual exploitation coordinator that works for the province on a regional basis and we work in conjunction with them. CISC also has a partnership with Interpol. The CISC executive committee has agreed to focus on measures to prevent the sexual exploitation of children; child pornography on the Internet is part of that priority. CISC works closely with the Canadian Association of Internet Service Providers (CAIP).

Canada's National Cybersecurity Strategy
Securing an Open Society: Canada's National Security Policy (2004) mandated the development of a National Cybersecurity Strategy. While still under development, elements of this strategy will have implications to the online environment for children with various initiatives to tackle cyberthreats, enhance international co-operations and improve education and awareness of users.

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

Canadian policy is guided by the domestic frameworks articulated above, as well as various international policy instruments. Canadian organizations are actively involved in international cooperation efforts.

Policy instruments include: the UN Convention on the Rights of the Child; the Council of Europe Convention on Cybercrime (Additional Protocol); the Council of Europe Declaration on Protecting the Dignity, Security and Privacy of Children on the Internet; the Council of Europe Recommendation on Empowering Children in the new information and communications environment; and the Resolution on Children's Online Privacy (by the International Data Protection and Privacy Commissioners).

International outreach and cooperation includes:

- **Cybertip.ca**: Cybertip.ca is a member of the Association of Internet Hotlines (INHOPE, www.inhope.org);
- The **National Child Exploitation Coordination Centre (NCECC)** seeks to strengthen international partnerships and the expedient sharing of information between Canadian law enforcement agencies and those in other countries. The NCECC is a one-stop access for international partners to liaise or provide time sensitive intelligence or information pertaining to the sexual exploitation of children on the Internet.
  - The NCECC is also part of the Virtual Global Taskforce (VGT) which also includes the UK, USA and Australia. The VGT promotes unified efforts among world law enforcement agencies across the world in relation to prevention and awareness on the Internet (www.virtualglobaltaskforce.com).
  - The NCECC leads Canada's contribution to the G8 Image Database project. Currently, the NCECC is conducting a market scan for potential software to establish a Canadian database to support the Interpol image database and the potential G8 image database.
- Canada strongly supports cooperation between APEC TEL and the OECD on this project, and sees value in continued complementary efforts.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

1. **Increased risk of sexual exploitation among all Filipino children**. Studies show that children and adolescents in the Philippines are those who lead in using or accessing interactive technology such as the internet. Different kinds of risks face all children. Once online, these children and adolescents are at risk from exposure to abusive materials or images such as pornography. Unsuspecting children become vulnerable online in chat rooms wherein child molesters are known to prey on them and groom them for eventual real time abuse. Online children are also victimized being themselves recipients of unsolicited abusive or violent materials. Children such as those living on the streets, those living in poverty, out of school youth, and those involved in the sex industry are highly vulnerable to further exploitation as they are the ones who are easily lured to become objects of pornography. Middle class children who have access to technology are also victimized by way of being recipients of abusive materials. They are also more prone to victimize other children by way of sharing or sending materials they receive.

2. **Increasing number of clandestine cybersex den operations involving minors as 'models'**. In a study, the PNP confirmed the existence and operations of cybersex dens and websites that provide live erotic video stream with Asians as 'models', Filipino children included. [1] These operations are mainly funded by foreign men (more Japanese men are involved although there are also Americans, Europeans and Australians) but local cohorts are known to lure and recruit vulnerable children from the provinces. ECPAT has documented the case of a 6 year-old girl coaxed into dancing and posing on webcam. ECPAT has also noted an increasing number of local child exploiters who operate backyard-type cybersex dens with minors as chat room models. Actual cases handled by the Philippine police show that cybersex operations are structured and corporate-like with website owners usually living abroad. Police say that given their nature and set-up cybersex den operations will increase tenfold especially since there is no comprehensive law against it.

3, **Minors accessing technology as tool for sexual trading**. The internet café shop owners around the country state that minors are peddling themselves to foreign men for cybersex through webcam showing of private parts or even explicit sexually suggestive acts in return for money. [2] This is possible because some public internet shops still operate private cubicles. These minors may be male or female, straight or gay. It is also noticeable that money exchange outlets like Western Union have sprouted up next to where there are public icafe shops. In the book '*Child Pornography in the Philippines'* minor respondents state that they feel no harm in cybersex because they say they are only showing private body parts captured on camera; no real bodily contact done. However, these modern developments in technology have no doubt made many children become highly sexualized at very young ages. Though there are no studies to prove otherwise, there is a noted increase in teenage pregnancy including minors acting out sexually what they watch through the internet. There have been a noted number of minors who have sexually abused other minors too.

4**. Public access internet shops have evolved to become known as 'net nannies'**. Internet café shop owners say that many mothers leave their children, some as young as 4 or 5 years old, inside the café shops for long period of hours unattended and unsupervised. [3] The mothers pay a maximum amount equivalent to hours of unsupervised online access for the children. The nature of public internet shops are such that these young children are exposed to highly inappropriate materials when online. Owners have reported that these children get to see and watch pornographic materials or video when others inside the café access them or the children themselves access these sites wittingly or unwittingly.

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

(2) Does your economy have relevant laws and regulation? (If there are laws and regulation, please describe the overview.)

There is no current law against child pornography in particular. At the national level, the current legislative scheme on child pornography is not a single, coherently formulated scheme, but rather a patchwork of several different acts that each make tangential contributions to the overall legislative framework. None of these acts directly address the issue of child pornography. The most relevant such act is the Child Abuse Law, RA 7610.

- ✓ **RA 7610**

RA 7610, enacted in 1992, is an umbrella law that is designed to cover child abuse in all its forms. It partially implements the Philippines state's obligations under the UN Convention on the Rights of the Child.

Section 2 explicitly declares that the best interests of children are the **paramount** consideration in any action concerning them, pursuant to the United Nations Convention on the Rights of the Child. This is a useful and important interpretive principle. It places the rights of the child above conflicting ‘adult’ rights such as freedom of expression and the right to privacy.

Section 3 sets out important definitions, including “children,” “child abuse,” and “circumstances which gravely threaten or endanger the survival and normal development of children.” In particular, children are defined to include those over 18 who are “unable to fully take care of themselves” due to “a physical or mental disability or condition.”

- ✓ **RA 9208**

RA 9208, the Anti-Trafficking in Persons Act, addresses the issue of pornography, but does not touch specifically on child pornography. It is important, however, in that it provides a somewhat clearer definition of pornography in s. 3 – “any representation, through publication, exhibition, cinematography, indecent shows, information technology, or by whatever means, of a person engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual purposes.”

S. 6(b) also provides for a stricter penalty where a child is adopted for the purposes of pornography.

- ✓ **E-commerce Law or RA 8792** : signed into law last June 14, 2000 and took effect last June 19, 2000 penalizes certain acts related to ICT but nothing is made mention of child protection aspects.

(3) Contents of voluntary efforts, such as self-regulation?

In 2005, ECPAT conducted three regional consultations against child pornography which was participated by children and youth from the respective major regions of the country – Visayas, Mindanao, Luzon. This was followed by the National Consultation of Children and Young People Against Child Pornography held in August 2006 in Bayview Plaza Hotel in Manila. The major output of the national consultation was the document called **The Young People’s Call to Action** which outlines the youth’s call specifically for the government and the IT industry sector, including internet café owners /operators and ISPs, to make Information Technology or IT a safe virtual place for them.

Towards the end of 2006, ECPAT launched the Make Information Technology Safe campaign (Make-IT-Safe) by addressing three important components : reaching out to Internet café owners through a series of nationwide round table discussions (3 in the Visayas, 1 in Luzon and 4 in Mindanao); initiating advocacy campaigns in schools in Quezon City and awareness raising among local officials and key people in communities.

To make concrete ECPAT's online advocacy against child pornography, it opened its own **ECPAT ICafe Plus in August 2007**. From a simple technical assistance with Everything Online, Inc., an internet business franchising firm operating in 49 provinces around the country, the assistance grew into a relationship bound by a common desire to fight child pornography and protect children from online harm.

ECPAT and Everything Online initiated the drafting of the Code of Conduct in time for the holding of the first National Conference of Internet Café Owners and Operators Against Child Pornography in Grand Boulevard Hotel in Manila in December 2007.

It was during this national conference that the first **Code of Conduct for Internet Café Owners and Operators in the Philippines** was adopted. The Code is a document which outlines or sets the guidelines that covers behaviour and principles of internet café owners and operators in the country. It also describes the minimum standards of public access internet cafes in the Philippines in the fight against child pornography and other forms of online sexual exploitation of minors.

The Make-IT-Safe campaign targets other key groups in its advocacy work against child pornography. The involvement of children and young persons is very significant. Being leading ICT users, they know the situation and problems affecting them and ECPAT believes in providing themselves the platform by which they themselves actively identify the solutions to such. As early as August 2006, these children and young people drafted the document called 'Call to Action' which enumerated their specific plans of actions to fight the problem. They are now involved in school and community campaigns as facilitators, documenters or as speakers who share their own knowledge and experiences of technology.

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

In 2006 ECPAT with support from UNICEF, conducted the 1st National Consultation on Child Pornography; three (3) Sub-national Conferences on Child Pornography and community-based and school-based awareness raising activities on safety on the internet and anti-child pornography. ECPAT, as mentioned earlier, has also networked with the private sector i.e. Icafe franchise with nationwide coverage Everything ONLINE, Inc, the intershop shop owners also across the country. In this regard, ECPAT with technical assistance from EOL opened its own ICaFE Plus in 2007. The café promotes guidelines that will protect children from harmful material in the Internet and against unscrupulous individuals they may meet in computer shops or online sexual abuse.

With the advances in modern technology, other key sectors in the society like the travel and tour sector must also be reached in this advocacy since this sector likewise makes use of the ICT in promoting its business and services. This is made even important since the country is known as a sex tourist destination.

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

ECPAT International (www.ecpatinternational.net) of which ECPAT Philippines is the national representative, has been actively in coorperation with AOL, Microsoft, Vodafone, BT and others in the campaign for children's safety online. (Please see http://www.make-it-safe.net/eng/industry.asp#5 for more.)

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

A large number of Thai teenagers are using social networking websites without appropriate guidance. The majority of them do not have the necessary technical background to know the potential harm or possible dangerous consequences of their actions, such as posting sensitive information about themselves, their friends, or family members to cyberspace. Because children and teenagers can easily access the Internet from unsupervised locations, parents and concerned authorities often find it difficult to monitor their online behavior.

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

We currently employ two methods to address the problem of accessing potentially harmful information on the Internet:

1. For home and schools, we suggest the use of website blocking software provided by the Ministry of ICT. The program can automatically update its database and control access to blacklisted websites.
2. We coordinate with ISPs to block access to inappropriate content from within each ISP's network.

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

1. The Computer-related Crime Act (2007) provides legal support to counter criminal activities on the Internet. For example, Internet and telecommunication service providers must keep a log of activities that occur on their networks for a minimum of 90 days.
2. Internet and telecommunication service providers are obligated by their licensing contracts to avoid illegal use of their networks.

(Example: Current Status of Japan)

In Japan, following matters are stipulated by "The Law on environment of development for children's internet usage";

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

There are industry groups and non-profit organizations which assist government authorities in combating Internet misuse. These include the Thailand Internet Association, the Thai Internet Service Shop Association, and the parent-teacher association at each school.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues?　What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

Educating the concerned parties, including students, teachers, and parents, is a government priority. The Ministry of ICT and the Ministry of Education have organized information sessions to inform these groups at schools around the country of possible online dangers.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, inter-ministerial cooperation, cooperation among businesses, etc.)

We work closely with both the private and public sectors to provide a safe online environment for children and students. It is through public-private cooperation that we are able to effectively limit access to harmful content on the Internet. Private Internet service providers are encouraged to form alliances and be more proactive at monitoring their own networks.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

We would like to cooperate with other economies to make the Internet a safer place for children.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

NOTE: The following U.S. contributions to this APEC survey are not exhaustive, given the nature of the Internet and the many government and private sector initiatives.

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

In the **United States**, federal and state governments share responsibility in protecting minors (defined generally as persons under the age of 18) from harm. Because of the importance of the Internet in the economy and society and the cross-border nature of the Internet, the United States government has taken special interest in understanding and addressing the potential for harmful influences that minors might experience through their increasing access to the Internet. In particular, the growing importance of social networking sites for minors presents many challenges for parents and governments alike. Some of these challenges include privacy, cyberbullying and access to material deemed inappropriate for minors. However, it should be noted that with respect to inappropriate content, the U.S. generally supports an industry-led, self-regulatory approach reinforced by enhanced consumer awareness and the widespread availability of consumer empowerment technology whenever possible.

At the federal level, many agencies work to ensure that minors are protected from threats. The Federal Communications Commission (FCC), Federal Trade Commission (FTC), Department of Justice (DOJ), National Telecommunications and Information Administration (NTIA), Department of Education (DOEd), are just some of the agencies involved in this work.

For example, making the Internet more secure for children has long been a part of the **FTC's** civil law enforcement mission. Former FTC Chairman, Deborah Platt Majoras delivered a keynote address "Rights and Responsibility: Protecting Children in a Web 2.0 World" at the Family Online Safety Institute on December 6, 2007, which provides detailed information about the FTC's commitment in this area. See http://www.ftc.gov/speeches/majoras/071206fosi.pdf for the text of this address.

The Department of Justice (DOJ) leads the effort of the U.S. Government in the investigation and prosecution of federal child exploitation crimes. In 2006, DOJ launched Project Safe Childhood (PSC), an initiative that aims to combat the proliferation of technology-facilitated sexual exploitation crimes against children. PSC is implemented through a partnership of U.S. Attorneys; the Child Exploitation and Obscenity Section of the Department's Criminal Division, Internet Crimes Against Children (ICAC) task forces; federal partners, including the FBI, U.S. Postal Inspection Service, Immigration and Customs Enforcement and the U.S. Marshals Service; advocacy organizations such as the National Center for Missing and Exploited Children; and state and local law enforcement officials. There are five key components to Project Safe Childhood: greater integration of our law enforcement efforts; the local execution of leads developed from national and international operations; increased federal involvement in these cases; training of law enforcement and prosecutors; and community education and awareness. To date, PSC has lead to the conviction of thousands of individuals for various internet-based child exploitation offenses. More information can be found at www.projectsafechildhood.gov.

On October 13, 2008, the President signed into law S. 431, the Keeping the Internet Devoid of Sexual Predators Act of 2008 or the KIDS Act of 2008. S. 431 will require convicted sex offenders to provide their “internet identifiers” to the sex offender registries. This bill also establishes a system by which social networking websites can cross-check the list of their users with a database of “internet identifiers” belonging to registered sex offenders.

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

Due to the important constitutional protections related to free speech, the federal and state governments in the United States must carefully approach the issue of managing access to information on the Internet. National and state governments often seek to work with Internet Service Providers and businesses to help protect minors.

For example, The **FTC** explores technology developments in this area and has convened workshops where this topic has been discussed. For example, in the May 2008 workshop “Beyond Voice: Mapping the Mobile Marketplace” topics included consumers’ ability to control mobile applications; the challenges presented by small screen disclosures; and M-commerce practices targeting children and teens. Information about this workshop, including the transcript, is available at http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml and http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#May6_08.

Most recently, (October 28, 2008) the President signed into law the "Broadband Data Improvement Act" [Pub. L. No. 110-385. Section 214], which directs the National Telecommunications and Information Administration to establish the Online Safety and Technology Working Group (OSTWG). Two of the mandates of the working group is to review and evaluate [1] The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children; and [2] the development of technologies to help parents shield their children from inappropriate material on the Internet. The OSTWG is to be comprised of "representatives of relevant sectors of the business community, public interest groups, and other appropriate groups and Federal agencies." The Working Group is charged to report back to NTIA and Congress its findings and recommendations as to what types of incentives could be used or developed to increase the effectiveness and implementation of such technologies. (For additional information on the OSTWG, see question 5)

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

The United States does have relevant laws and regulations, although the U.S. and state governments must carefully distinguish between laws regulating access to content and laws protecting the privacy of minors and preventing their exploitation. For example:

A. The Children's Online Privacy Protection Act (COPPA), passed by Congress in October 1998, requires the Federal Trade Commission (FTC) to issue and enforce rules concerning children's online privacy. The FTC issued the Children's Online Privacy Protection Rule in November 1999; it has been in effect since April 21, 2000. The Rule's primary goal: to place parents in control over what information is collected from their children online. See http://www.ftc.gov/ogc/coppa1.shtm and http://ftc.gov/privacy/privacyinitiatives/childrens.html

The Rule applies to:

- Operators of commercial websites or online services directed to children under 13 that collect personal information from children;
- Operators of general audience sites that knowingly collect personal information from children under 13; and

- Operators of general audience sites that have a separate children's area and that collect personal information from children.

The Rule requires these operators to:

- Post a privacy policy on the homepage of the website and link to the privacy policy everywhere personal information is collected.
- Provide notice to parents about the site's information collection practices and, with some exceptions, get verifiable parental consent before collecting personal information from children.
- Give parents the choice to consent to the collection and use of a child's personal information for internal use by the website, and give them the chance to choose not to have that personal information disclosed to third parties.
- Provide parents with access to their child's information, and the opportunity to delete the information and opt out of the future collection or use of the information.
- Not condition a child's participation in an activity on the disclosure of more personal information than is reasonably necessary for the activity.
- Maintain the confidentiality, security and integrity of the personal information collected from children.

A recent example of the FTC’s enforcement of COPPA is the $1 million settlement by Sony BMG to resolve charges that it violated COPPA and the FTC’s implementing Rule. See http://www.ftc.gov/opa/2008/12/sonymusic.shtm. The FTC complaint alleges that, through its music fan Web sites, Sony Music improperly collected, maintained and disclosed personal information from thousands of children under the age of 13, without their parents’ consent. The Civil penalty to be paid by Sony Music matches the largest penalty ever in a COPPA case.

COPPA also includes a “safe harbor” provision allowing industry groups and others to request FTC approval of self-regulatory guidelines to govern participating Web sites’ compliance with the Rule. See http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html. COPPA requires the FTC to act on a request for "safe harbor" treatment within 180 days of the filing of the request, and after the proposed guidelines have been subject to notice and comment. Section 312.10 of the final Rule sets out the criteria for approval of guidelines and the materials that must be submitted as part of a safe harbor application. Available at http://www.ftc.gov/os/1999/10/64fr59888.pdf.

B. The FTC has used its unfairness authority pursuant to Section 5 of the FTC

Act to protect the rights of consumers, including children, to avoid unwanted and potentially offensive content online. See 15 U.S.C. §§ 41-58 at http://www.ftc.gov/ogc/FTC_Act_IncorporatingUS_SAFE_WEB_Act.pdf For example, see FTC v. Various, Inc. d/b/a AdultFriendFinder, No. 5:07-cv-6181 (N.D. Cal. Filed Dec. 6, 2007), available at http://ftc.gov/opa/2007/12/afriendfinder.shtm.

C. The FTC, along with other regulators, has authority to tackle the problem of sexually explicit email communications. The CAN-SPAM Act, 15 USC §§ 7701-7713, and the FTC's Adult Labeling Rule, 16 CFR Part 3164, strive to place a bumper between x-rated email and children. (See http://www.ftc.gov/bcp/conline/edcams/spam/rules.htm for information about and the text of this law and Rule.) Commercial emailers must alert recipients to the presence of sexually explicit content in the subject line, and must make sure that the initially viewable area of the email message contains no graphic images. See U.S. v. TJ Web Productions, LLC, Civil Action No: CV-S-05-0882-RLH-GWF (D.Nev. filed Dec. 7, 2006), available at http://www.ftc.gov/os/caselist/0523047/0523047.shtm.

D. On December 4, 2002, the President signed into law the Dot Kids Implementation and Efficiency Act of 2002 that requires NTIA to oversee the establishment of "kids.us" (www.kids.us) as a safe space for kids on the Internet. The President expressed his strong support for creating a positive Internet experience for America's children. The kids.us domain provides a trusted online forum for children 13 and under. NeuStar Inc. is operating this space on behalf of NTIA. To ensure that content on kids.us is "suitable for minors," all websites must conform to guidelines that are set forth at www.kids.us/content_policy/index.html. No interactive services or hyperlinks that take a user outside of the kids.us domain are allowed. Neustar removes content that violates the guidelines.

E. Federal criminal laws prohibit the transfer of obscene material, such as hard-core pornography, to children under the age of 16. Other laws prohibit the use of misleading domain names, words, or digital images on the Internet with intent to deceive people into viewing obscenity.

F. When internet service providers discover the use of their system in connection with the exploitation of a child, they are required to file a report with the National Center for Missing and Exploited Children. They could be subject to criminal penalties if they willfully fail to make such a report, and to civil penalties if they negligently fail to do so.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

With respect to inappropriate content, the U.S. generally supports an industry-led, self-regulatory approach reinforced by enhanced consumer awareness and the widespread availability of consumer empowerment technology whenever possible. However, there are few nation-wide standards for activities that take place on the Internet related to content and its use and there are still debates among state governments, the federal government and interest groups in the U.S. regarding the scope of oversight and intervention in this area. In particular, there are constitutional concerns about the rights of freed speech and free access to information. **Therefore, parental controls and public-private partnerships that emphasize self-regulation are often employed in strategies to protect minors from online dangers.**

A. There are a number of self-regulatory programs which protect children online in the area of advertising. For example, the Better Business Bureau's (BBB) self-regulatory oversight of national advertising (See http://www.nadreview.org/); the Children's Advertising Review Unit (see www.caru.org); the Electronic Retailing Self-Regulation Program (see www.narcpartners.org/ersp/) and the Children's Food and Beverage Advertising Initiative (see http://us.bbb.org/WWWRoot/SitePage.aspx?site=113&id=dba51fbb-9317-4f88-9bcb-3942d7336e87).

The BBB operates a National Advertising Division (NAD), which gathers complaints about advertising. In investigating challenges to a particular company's advertising, the NAD enforces FTC-like standards for truth and accuracy in advertising. Most NAD inquiries are resolved at this level; if however, the advertiser is not satisfied with the NAD's decision, the matter may be appealed to the National Advertising Review Board, or NARB. Then, if the advertiser refuses to comply with the decision of NAD or NARB, the matter may be referred to FTC for resolution. See "The Advertising Industry's Process of Voluntary Self-Regulation: Policies and Procedures by the National Advertising Review Council, Administered by the Council of Better Business Bureaus", part 3.1 and 3.7 available at http://www.narcpartners.org/about/files/07_Procedures.pdf.

B. In June 2006, the FTC called on representatives of the social networking industry to develop and implement safety guidelines. See Prepared Statement of the Federal Trade Commission On Social Networking Sites, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce of the United States House of Representatives, presented by Commissioner Pamela Jones Harbour (June 28, 2006), available at www.ftc.gov/os/2006/06/060626socialnetworking.pdf.

Several social networking sites now provide users with a wide spectrum of privacy controls that allow a more nuanced approach to the "friends" phenomenon. Several sites have established more responsive abuse reporting mechanisms, so that children who feel threatened or concerned have a reporting tool at their disposal. Some have linked to the OnGuard Online website (http://www.onguardonline.gov/) tips for staying safe on social networking sites. (See response to question 4 for more information about OnGuard Online.)

C. An example of a private sector-led voluntary initiative is "GetNetWise" (http://www.getnetwise.org). This is an online resource for parents that provides information on Internet safety tips, consumer content filtering products, law enforcement contacts, and guides to quality educational and age-appropriate online content. GetNetWise is a public service provided by a wide range of Internet industry corporations and public interest organizations. The GetNetWise coalition wants Internet users to be only "one click away" from the resources they need to make informed decisions about their family's use of the Internet.

D. MySpace and Facebook, have agreed to cooperate with state authorities to self-police their websites. Details of the agreements can be found at the following links:

- http://www.attorneygeneral.gov/uploadedFiles/Press/Facebook%20agreement.pdf
- http://www.attorneygeneral.gov/press.aspx?id=3293

MySpace is also engaged in numerous efforts to develop self-regulatory principles on safety, including in the UK and with the European Commission.

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or

private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

A. The FTC is actively engaged in a comprehensive education campaign to instill the values of safer and more secure computing. The cornerstone of the campaign is the multimedia website, OnGuardOnline.gov. The site was created in September 2005, partnering with other federal agencies, consumer advocates, and the technology industry to help computer users guard against Internet fraud, secure their systems, and protect their personal information. Among other topics, the site includes materials on spam, spyware, P2P file-sharing, phishing, identity theft, and wireless security. The FTC maintains OnGuardOnline.gov with significant content and marketing assistance from partners including: the U.S. Department of Justice, the United States Postal Inspection Service, the Department of Commerce, Technology Administration, the Internet Education Foundation, the National Cyber Security Alliance, i-SAFE, AARP, the Direct Marketing Association, the National Consumers League, the Better Business Bureaus, and others.

OnGuard Online is branded independently of the FTC, so other organizations can make the site and the
information their own. The FTC encourages companies and other organizations to help fight Internet fraud, scams, and identity theft by sharing the tips at OnGuardOnline.gov with their employees, customers, members and constituents. OnGuard Online materials also are available in Spanish, at AlertaenLinea.gov.

Many topics presented on OnGuard Online apply to consumers generally. In certain areas, however, we have focused on the issues uniquely important to children and their parents. OnGuard Online includes a video for parents on how to weigh the risks of children's online activities, and provides some thoughtful guidelines for kids' Internet use. With the rise in popularity of social networking sites, we introduced a set of tips about safer social networking. One bulletin is for parents, and one is specifically directed to teens, using different language for each audience. The site also includes an interactive "Buddy Builder" quiz aimed at getting teens to consider whom they "friend" online.

Our OnGuard Online materials are not static; they change as technological developments change. For example, after noting the reality that increasing numbers of children now access the Internet not from stand-alone PCs, but from their mobile handsets, the FTC updated the social networking tips for parents alerting them to possible limits that they can place on a child's cell phone. The FTC will continuously update its educational materials to take into account developments in children’s use of the Internet and technology.

In addition to OnGuard Online, the FTC maintains a web site devoted to children’s privacy issues with areas for both adults and children to explore, available at http://www.ftc.gov/kidzprivacy/.

B. The Broadband Data Improvement Act, 47 USCS § 1301 et seq, was passed in October 2008, and provides for the Protecting Children in the 21st Century Act. It directs the FTC to implement a national education campaign on the safe use of the Internet by children. See 15 USC § 6552. The FTC will build on the existing OnGuardOnline.gov site and partner with organizations to reach parents, children, and care givers. This Act expands the FTC's authority to educate on Internet safety issues.

C. On December 4, 2002, the President signed into law the Dot Kids Implementation and Efficiency Act of 2002 that requires NTIA to oversee the establishment of "kids.us" (www.kids.us) as a safe space for kids on the Internet. The President expressed his strong support for creating a positive Internet experience for America's children. The kids.us domain provides a trusted online forum for children 13 and under. NeuStar Inc. is operating this space on behalf of NTIA. To ensure that content on kids.us is "suitable for minors," all websites must conform to guidelines that are set forth at www.kids.us/content_policy/index.html. No interactive services or hyperlinks that take a user outside of the kids.us domain are allowed. Neustar removes content that violates the guidelines.

D. In November, 2008, the Department of Justice, as part of its Project Safe Childhood, announced an innovative national public service announcement (PSA) campaign to educate parents about the potential dangers that their children face online and, for the first time, warns potential online predators that exploiting a child online is a serious federal offense. Elements of this campaign include television, print, radio and Web advertisements, as well as ads in movie theaters and “webisodes.” The campaign includes ads in English and in Spanish.

E. Recently, a group of private sector participants of the Internet Safety Technical Task Force (ISTTF) under the auspices of a Harvard University project titled “Enhancing Child Safety and Online Technologies” took part in an effort to study the existing data regarding the activities of, and dangers to, children in the online environment. The project was supported by the Attorneys General of the U.S. states. Conclusions and data can be found at the website: http://cyber.law.harvard.edu/pubrelease/isttf/

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

A. A relatively new initiative intended to address the issue of protecting children online via a cooperative framework is being overseen by the National Telecommunications and Information Administration. On October 10, 2008, the President signed into law the "Broadband Data Improvement Act" (the Act), Pub. L. No. 110-385. Section 214 of that Act directs NTIA to establish the Online Safety and Technology Working Group (OSTWG) for a single 15 month term. At the conclusion of the working group's term, the OSTWG will provide a report to Congress on ways to promote and to preserve a safe environment for children using the Internet. The OSTWG will specifically work to review and evaluate:

- The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;
- The status of industry efforts to promote online safety among providers of electronic communications service providers related to record retentions in connection with crimes against children; and
- The development of technologies to help parents shield their children from inappropriate material on the Internet.

The Act specifies that the OSTWG must be comprised of "representatives of relevant sectors of the business community, public interest groups, and other appropriate groups and Federal agencies." For the purpose of establishing the OSTWG, the "business community" includes, at minimum, Internet service providers, Internet content providers (especially targeted towards children), producers of blocking and filtering software, operators of social networking sites, search engines, Web portals, and domain name service (DNS) providers. Public interest groups may include organizations that work on behalf of children or study children's issues, Internet safety groups, and education and academic entities. NTIA solicited nominations of representatives to serve on the OSTWG (See Federal Register/Vol. 73, No. 226/Friday, November 21, 2008) in November 2008 and is currently in the process of vetting those received. The first meeting of the OSTWG is expected to take place in late spring of 2009.

B. There are many examples of private sector engagement to protect children online. For example, Verizon and ATT both actively support online safety initiatives of organizations such as the Family Online Safety Institute (FOSI).

For other examples, see responses to questions 2, 3, and 4 above.

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

The FTC participates in international fora and international cooperation networks such as the International Consumer Protection Enforcement Network (www.icpen.org). The FTC cooperates with other spam enforcement authorities through the London Action Plan organization (www.londonactionplan.net). Cross-border enforcement cooperation is a priority within these organizations and topics relating to the safety of children online have been discussed within these groups.

OECD Members

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

1. Denmark has seen an explosive rise in the use of online social networks. Online harassment and abuse of information in connection with online social networks are issues that have been addressed.
2. Sexual violation of children linked to online networks has been addressed and is an ongoing concern for Denmark.

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

Age certificate regarding use of online social networks

Online age verification has not been implemented in Denmark, but The National IT and Telecom Agency has in 2008 prepared (in Danish only) a study on online age verification as a mechanism to prevent adult sexual violation of children in connection with online networks.

The Information Security Committee has prepared a technical study on implementation of online age verification.

Sexual violation of children linked to online networks

Filtering technology is used to prevent access to websites containing child pornography. The internet service providers cooperate with the police and the organization Save the Children on the matter.

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

Online social networks

The Danish Act on Processing of Personal Data regulates this area in general.

Sexual violation of children linked to online networks

Following is the wording of the clause on abuse images of children, including online distribution and use, currently held in Danish criminal law:

He, who disseminates obscene photographs, films or other obscene images and suchlike of persons under the age of 18, will be liable to a fine or be imprisoned up to two years or - under aggravating circumstances - be imprisoned up to six years. Aggravating circumstances are especially instances where the child's life has been put at risk, severe violence has been used, serious harm has been done to the child or dissemination has been carried out in a systematic or organised fashion.

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

Online social networks

Internet Service Providers (ISP) operating in Denmark have an agreement to filter spam and other malicious code.

Sexual violation of children linked to online networks

The use of filtering technology regarding access to websites containing child pornography is based on self-regulation. The participating parties are, as mentioned earlier, the police, the organization Save the Children and the internet service providers.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on "Action plan for encouraging dissemination of filtering service"

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues?　What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

Online social networks

The Ministry of Science Technology and Innovation yearly launches "Netsikker nu!" – Campaign (Net-secure now! -campaign). The campaign aims to improve knowledge and awareness of information security issues among Danish citizens.

Sexual violation of children linked to online networks

A number of polices raise awareness about the matter in both public and private sector. For example,

The Danish Media Council works together with national and international partners from all over the world via the European network Insafe. The aim is to create awareness and inform about children's use of the internet and new technologies as well as to provide parents and educators with knowledge and tools for raising children in the network society. The Council is Awareness Node under the EU Safer Internet programme.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of "learning information moral" based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

Online social networks

The Information Security Committee is a public private partnership setup by the Ministry of Science Technology and Innovation to promote and coordinate the information security field in Denmark. The Committee consists of 17 members composed of governmental, private and NGO organizations.

Sexual violation of children linked to online networks

The Internet Service Providers have established a network where they share relevant knowledge and experiences about handling of illegal content, including child pornography. The Ministry of Science Technology and Innovation is government representation and a number of organizations take part as well.

Beyond that, interministerial cooperation is close and a contact committee has been established to ensure a coordinated effort on the matter.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

Online social networks

Denmark participates in the European information security organization ENISA and the EU program Safer Internet.

Sexual violation of children linked to online networks

The matter is addressed through the participation in the EU Safer Internet as the programme aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, including child pornography. Safer Internet supports wide cooperation between stakeholders, from mobile operators to child welfare NGOs, to develop and spread the best ideas for making Internet use safer. The programme also coordinates activities between different member states.

Denmark also participates (the government as well as some private organizations) in the global Internet Governance Forum, which, among many matters, addresses the matter of sexual violation of children linked to online networks.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

Current status of Egypt:

- In general, it has been noticed the use of inappropriate content by minors in tele centers and internet clubs.
- There is a trend to download material without respect for property rights, in many cased due to ignorance about such laws.
- Some internet users, have been using the social sites to instigate religious issues.
- There is a tendency to post of personal information without awareness about the consequences especially on social networking sites; thus, exacerbating “the privacy” concerns.
- Increasing use of social networking sites without understanding the repercussions of info uploaded.
- The above mentioned remarks have been mentioned in a number of reports, though there is a need for a scientifically and objectively structured study on representative samples, to reach actual statistics concerning the real risks facing children on line in our economy.

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

“The Online Dating Sites regulation Law” is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website.

Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

- In Egypt, there are a number of filters/ safety tool kits provided by different companies, such as Microsoft. MS has recently Arabized its safety tool kit to accommodate the Arab countries
- ISPs are providing different types of filters, TEDATA, a major ISP in Egypt is offering the family internet service. The family filter service is a new service created to provide superior internet experiences while eliminating all of the internet indecent content that might affect the children. It effectively and automatically blocks inappropriate material on the internet based on the client's requirements, transparent filtering, no configuration or software installations are needed by the user, inappropriate sites can be manually added to the data base within an online cycle (ADSL feature), filtering indecent Arabic content/ Arabic keywords, cannot be turned off by the kids, no upgrade to the computer hardware is necessary and makes uses of safe search options provided by most search engines like Google, Yahoo, MSN live, Youtube. Etc available customer services 19777. TEDATA has also created a supporting web site for the family using this filter www.familyinternet.net
- The national telecommunication regulatory authority has developed a hot line for complains or issues related to misuse of technology 155

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation? (If there are laws and regulation, please describe the overview.)

The child law number 126 for 2008 amending child law 12 for 1996, article 116 bis is very clear in criminalizing and penalizing with imprisonment or severe financial penalties, anyone importing, issuing, preparing, promoting, owning or disseminating porn material involving children, using the computer, internet, www or cartoons for the purpose of pedophilia, or using the PC, internet or cartoons to instigate children to pedophilia, or immoral behavior (article 116 bis (a)).

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

In Egypt, the private sector such as Microsoft is producing guidelines and safety tips and brochures in Arabic.

Currently, the Suzanne Mubarak women's International peace movement is adopting the cyber peace initiative including a full track on the safe use of the internet. Part of the deliverables that have been issued by the project are: safety tips for children, safety tips for youth, safety tips for parents; all geared to self regulation.

In addition, a complete manual for the family has been Arabized and localized by the Initiative in cooperation with the European Insafe network.

More material has been produced and distributed to schools and public libraries based on Arabization and location of material. This effort is conducted with concerned companies.

For more details about the content produced and aiming at self regulation please visit our web site www.cyberpeaceinitiative.org

- Based on the second annual meeting of the cyber peace initiative on the 18th of Feb. 2009, more activities and guidance are expected to be in place in coordination with different actors, including ISPs.
- One of the main target groups in the coming period will be the educators.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association),

(IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

In Egypt, we have developed policies to improve literacy and raise awareness of safety issues. Our main work is the public private social partnership undertaken under the cyber peace initiative. Based on such initiative, a youth internet safety focus group (net- aman) and a parents internet safety focus group have been formed to improve safety literacy and awareness. The youth group and parents groups visit schools, public libraries, tele-centers and youth centers to spread the ethics of using the internet with the help of arabized resources.

Throughout the last period from September 2007 – February 2008, approximately 150,000 have received training or attended awareness sessions on internet safety under the umbrella of the initiative. There is a need to mainstream the effort into different government programs to be able to reach out to effectively to Egypt's youth population (approx. 40 million).

A curriculum has been formulated and produced for the first secondary grade in schools combining digital literacy and internet safety. The curriculum is a pilot and will be tested this year.

Plans for further curriculum development on safety are considered.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, inter ministerial cooperation, cooperation among businesses, etc.)

In Egypt, the cyber peace initiative of the Suzanne Mubarak Women's international Peace Movement is carrying the function of spreading internet safety awareness. The initiative is an international effort aiming at disseminating the message regionally. The initiative is based on a partnership between an NGO (the Suzanne Mubarak women's international peace movement), the government (the ministry of communications and information technology), international organizations (the international telecommunication Union, the UN Global Alliance for ICT and Development) and private sector (Microsoft, Cisco, Intel and Huwaie). In addition, a number of international NGOs have joined us, such as Child net International. Currently, we are cooperating with Diplo and the European Insafe.

The safety track implementation relies on cooperation with the ministry of education, and the national council for childhood and motherhood to disseminate the awareness and training plans. The national council has a hotline for child issue complains 16000

We are also cooperating with the ISPs, such as TEDATA to develop family filters. We are also aiming to have a dialogue with ISP and content providers to discuss other forms of filters.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

- The safety track of the cyber peace initiative cooperates with a number of international organizations and institutions.
- We are members of the dynamic coalition for child on line safety created within the internet governance forum set up.
- The cyber peace initiative has a partnership agreement with the ITU.
- We are cooperating with the ITU and are parts of the Child on line Protection project.
- We are cooperation with the Council of Europe for the Arabization of the digital literacy handbook and for adopting on line games for safety.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

The 2007 Eurobarometer survey, in which children and younger teenagers were interviewed in-depth about their use of online technologies, confirms that many children are disturbed, bothered and in some cases sometimes traumatized by being exposed to harmful content when using online technologies. see http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

The content most frequently mentioned refers to:

- pornographic images (according to the study, almost all the children questioned seem to have been exposed to this kind of content)
- extreme violence or torture (often mentioned)
- racism and xenophobia (to a lesser extent)

In addition, one should bear in mind that children are not only exposed to harmful content but also to harmful conduct such as

- being victims of cyber-bullying (from other children of their own age), statistically the most frequent type of harmful conduct
- being contacted by people who will befriend them in order to commit sexual abuse (grooming)
- being victims of sexual abuse, which is documented through photographs, films or audio files and then transmitted online

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

There exist many filtering software tools and systems for the European cultural context and there is considerable work to be done in identifying those that are most effective. For this purpose the Safer Internet programme has conducted a study SIP-BENCH for providing recommendations to empower parents and educators to choose and use adequate filtering solutions and to make them aware of their capabilities and limitations.

The 2007 SIP-BENCH report found that generally “filtering technology is maturing and can be made effective to live up to the expectations of child carers throughout the EU. Generally the filters designed for children up to 10 years old are more effective than those for older children, and tools work better on English language sites. However, generally most filters benchmarked in the study had improved compared to the previous year for general harmful content. Neither filtering nor blacklisting was found to be either sophisticated or fast-moving enough to cope with Web 2.0 content.

The Youth Protection Roundtable, another project funded by the programme, address the problem that existing technologies suffer many shortcomings and need to be better adapted to practical needs and requirements. The aim of this project is to encourage a collaborative and cross-sector dialogue focusing on the optimal mix of effective technology-enhanced strategies on the one hand and education-based strategies on the other hand, to enable youth for a safe and secure use of the Internet. The roundtable will produce two sets of Guidelines: one for technical developments in respect of educational issues, and the other product-neutral guidelines for use of filter technologies and pedagogical measures in public and private areas.

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?

(If there are laws and regulation, please describe the overview.)

Europe-wide standards exist for the protection of minors and human dignity, and for electronic commerce, privacy and electronic communications. (Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry (2006/952/EC), Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector).

Europe-wide standards also exist for illegal content in the form of child abuse material and racism and xenophobia. (Council Decision of 29 May 2000 to combat child pornography on the Internet (2000/375/JHA), Council Framework Decision of 20 January 2004 on combating the sexual exploitation of children and child pornography (2004/68/JHA) and Council Framework Decision on combating racism and xenophobia (COM/2001/0664))

Harmful contact refers to contact preparatory to committing a sexual offence against a child by contacting them online, sometimes referred to as "grooming". The preparatory acts for committing sexual offences are not, as such, yet considered as an offence in most Member States, but grooming is a criminal offence in the UK and a recent Council of Europe Convention makes it an offence in signatory countries (Council of Europe Convention on the Protection of children against sexual exploitation and sexual abuse, adopted by the Committee of Ministers on 12 July 2007 at the 1002nd meeting of the Ministers' Deputies. The Convention has opened for signature at the Conference of European Ministers of Justice on October 25 and 26 2007).

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations,

etc.))

The Safer Internet programme supports industry self-regulation regimes where they are broadly accepted by stakeholders and where they provide for effective enforcement. A successful example of this is the Commission initiative leading to the signature of the European Framework for Safer Mobile use by younger teenagers and children by leading mobile operators and content providers in 2007.
This framework describes principles and measures to protect children that those companies who signed the agreement commit to implement on the national level through out Europe.

In 2008, the agreement had been signed by a total of 24 mobile operators serving 96% of the EU mobile phone customers. As an offspring of the European initiative, the mobile operators GSM Association have further launched their Global alliance against child abuse images.

Moreover, in April 2008 fourteen leading European mobile operators, mobile content, social networking companies and internet providers launched TeachToday, an educational website designed to help teachers encourage children to use the internet and mobile technology responsibly and safely. The industry consortium worked closely with European Schoolnet, the co-ordinator of the INSAFE network initiated and funded by the Safer internet programme, to create the materials.

In order to strengthen the protecting of children when using social networking sites the European Commission has furthermore convened a Social networking Task force with 17 operators of social networking sites used by under18s, and a number of researchers and child welfare organizations. This initiative was initiated in 2008 and has had the concrete result of an agreement of voluntary guidelines for use of social networking sites by children, which will be presented at the Safer Internet Day on February10, 2009.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

The Safer Internet programme, has worked towards an inclusive approach bringing together all concerned stakeholders from industry to researchers, teachers, parents and NGOs active in child welfare and encouraged them to cooperate, exchange ideas, best practice and experience in order to empower and protect young people when using online and mobile technologies.

In order to use the Internet in a safer and more responsible way, parents and children need to be informed and educated. Through the programme, the European Commission has fostered the creation of a Europe-wide network (Insafe), which coordinates awareness raising activities in 26 European countries.

The activities of the network aim to empower children and to raise awareness among parents and teachers and include the organization of workshops in schools and cooperation with mobile phone companies and social networking sites to develop educational materials on safety issues.

INSAFE also organises Safer Internet Day in February every year, an event which has increased the public awareness of child online safety issues considerably, in addition to giving strong and positive visibility to European initiatives. Last year more than 120 organisations in 56 countries took part in this initiative, organising local, national and pan-European events ranging from safety sessions in schools and competitions for young people to public meetings and conferences.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

See under point 3 which describes some self-regulatory partnerships at the European level.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

Co-operation and collaboration with third countries – both within and outside Europe - on a policy and operational level is one of the programme's priorities in particularly with regard to identifying, tracing and eradicating illegal child abuse images but also with regard to sharing best practice of the awareness-raising activities of the Insafe network.

The network of hotlines, coordinated by the INHOPE Association, is a concrete example of the international cooperation which is particularly important in the fight against child abusive content since this material could be produced in one country, hosted in a second and accessed and downloaded all over the world.

The hotlines are important contact points for receiving reports of illegal content which they analysis and pass on to the appropriate body for action such as a law enforcement agency or an ISP provider. Today, the network has 33 members across the world, not only in the EU member states but also in the US, Canada, Australia, Taiwan, South Korea and the Internet Hotline Centre in Japan.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

The Finnish Consumer Agency/Consumer Ombudsman supervises the legality of marketing and contractual terms. An advertisement that is aimed at or reaches children is deemed to be in contrary to good practice if it may impact in the harmful way on the development of children. As an inappropriate marketing is deemed to be a direct appeal to buy targeted to children. On the internet a child may meet an inappropriate marketing for example in following connections:

1) Recognizability of advertising
   The advertising of product and brands targeted at children may dressed up as a game or activity page in such a way that makes recognizability impossible.
2) Collecting personal information
   A child can be asked personal information and permission to direct marketing when registering on the playsites
3) Violent models of behaviour
   Games and ringtones or logos of mobile phones aimed to children may include very violent or sexistic content.

http://www.kuluttajavirasto.fi/File/0586b0cc-6ff4-43e4-bcac-c89179c0ce52/Minors+marketing+and+purchases.pdf

http://www.kuluttajavirasto.fi/File/71c7279a-af1a-4cea-b858-ae7948ca96d8/Internet+marketing+aimed+at+children+and+minors.pdf

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

“The Online Dating Sites regulation Law” is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

In Finland in order to prevent problems arising from provision and use of telecommunications services, there are categories of calls that may be barred. A user may thus choose which calls he or she wishes to bar. **Barring may concern calls and text messages** to premium rate service numbers and international calls. Operators may provide additional barring options. The holder of the connection can have calls and text messages barred free of charge. (www.ficora.fi/ in English).

One objective of an efficient information society is for the same user to be able to identify him/herself in all, or at least nearly all, public and private sector services using one reliable method. Nevertheless, there may be a number of methods in use side by side.. For instance, the identification of an underage customer is vital, including the identification of loan applicants by the creditor, who also ensures that minor citizens cannot conclude agreements to which they, by law, are not entitled.
- > **The government draft proposal has been given about the requirements concerning strong identification**.

In Finland in order to stop spreading child pornography in the Internet the bill gives the **National Bureau of Investigation (Finnish State police) the authority to introduce a blacklist of foreign internet sites known to host child pornography and that blacklist is to be followed by commercial Internet Service Providers (ISP) to censor these sites from their respective customers**. The bill states that participation on behalf of the ISP is voluntary, but practice has proven this to be only nominally so.

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250

million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?

Legislation supervised by The Finnish Consumer Agency:

1) Consumer Protection Act

   Includes a.o.t. general regulation of marketing

Other legislation:

1) **The** Audiovisual Media Services Directive **covers all EU audiovisual media services (including on-demand services) in the digital age.** It amends and renames the Television without Frontiers Directive, providing less detailed but more flexible regulation. And it **modernises TV advertising rules** to better finance audiovisual content. The directive must be transposed in national law by the **end of 2009**. The new rules respond to **technological developments** and create a **level playing field** in Europe for emerging audiovisual media. The availability of harmful content in audiovisual media services continues to be a concern for legislators, the media industry and parents. There will also be new challenges, especially in connection with new platforms and new products. It is therefore necessary to introduce rules to protect the physical, mental and moral development of minors as well as human dignity in all audiovisual media services, including audiovisual commercial communications.(45) Measures taken to protect the physical, mental and moral development of minors and human dignity should be carefully balanced with the fundamental right to freedom of expression as laid down in the Charter on Fundamental Rights of the European Union. The aim of those measures, such as the use of personal identification numbers (PIN codes), filtering systems or labelling, should thus be to ensure an adequate level of protection of the physical, mental and moral development of minors and human dignity, especially with regard to on-demand audiovisual media services

2) **The Act on the Classification of Audiovisual Programmes** provides for the classification of audiovisual programmes and especially for restrictions on their exhibition and supply which are necessary for the protection of children.

   CHAPTER 2 (Inspection and classification of audiovisual programmes) Section 3 (Restrictions on exhibition and supply) says: *An audiovisual programme may not be publicly exhibited or supplied to persons who have not attained the age of 18, before the programme has been approved for exhibition and supply, unless otherwise provided in this Act. A supplier of on-demand services may make available to persons who have not attained the age of 18 only audiovisual programmes approved for exhibition or for supply to them by virtue of this Act and exempted programmes and their contents.*

3) **Under the Guardianship Act** a minor can only independently perform legal acts that are of a normal nature and of minor significance under the circumstances. A legal act that a minor is not entitled to perform is not binding unless a guardian has given consent

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?

(Does your economy have any self-regulation?

If there is some self-regulation, please describe the overview.

(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

The Finnish Direct Marketing Association (Finnish DMA http://www.ssml.fi/?l=en)

represents the major direct marketers in Finland. It has issued a code of conduct about marketing and selling of mobile services. There exists also **An Ethical Board for Telecommunication Services,** which has also issued its own self-regulation guidelines (http://www.mapel.fi/set_of_norms_in_english/)

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

The Finnish Consumer Agency has published the guidelines
as a guide for advertisers to use when planning marketing to children:

1) Minors, marketing and purchases
http://www.kuluttajavirasto.fi/File/0586b0cc-6ff4-43e4-bcac-c89179c0ce52/Minors+marketing+and+purchases.pdf
2) Mobile content services
http://www.kuluttajavirasto.fi/File/77c537f8-bc64-47a2-8133-8de59dc4f508/Mobile+content+services.pdf
3) E-Commerce and marketing on the internet
http://www.kuluttajavirasto.fi/File/e4e7a8d6-2cc2-426b-9cad-4e02ae04ad9e/E-Commerce+and+marketing+on+the+internet.pdf

In addition the website of Consumer Agency includes an item called A child as a consumer where parents can find a lots of information a child's position as a consumer.
(http://www.kuluttajavirasto.fi/en-GB/children/)

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

APEC Children Protection Project Questionnaire

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

Individual problem areas:

- Internet chat rooms and online communities (loss of control, paedophilia and cyber bullying)
  The majority of young Internet users divulge personal information in chat rooms and on other websites without thinking. Divulging personal information leads to a loss of control over the extremely sensitive area of personal data. This brings with it a risk which, in a worst case scenario, can have lifelong consequences (the Net never forgets). In particular, Internet chat rooms and online communities can help initiate contact between paedophiles and their victims. Even before a violent sexual assault has taken place it is easy for perpetrators to harass their victims by e-mail, mobile phone or instant messaging. The use of the Internet to abuse, insult, embarrass and disparage others, amongst other things, presents an additional problem.
- Online games
  This issue has gained significance following the shooting in the town of Emsdetten in November 2006 and other incidents. Online games also tend to be more addictive than computer games played alone in front of the computer screen. Therefore, thought must be given as to how addictive websites should be considered from the point of view of protecting children and young people from harmful media alongside other problems with their content.
- Violence in Web 2.0
  A recent study of the issue of “Violence in Web 2.0” investigated the Internet use of 12- to 19-year-olds, in particular the distribution of violent content (a summary is available at: http://www.nlm.de/fileadmin/dateien/aktuell/Studie_Prof._Grimm.pdf). The study identified severe reactions to the depictions of violence widely found on the Internet. These included strong emotional reactions (revulsion, shock and fear) as well as occasional nightmares and more sustained physical reactions.
- Fun sites
  At first glance websites known as fun sites appear entertaining and are particularly attractive to children and young people. Users are invited to click on links such as “accidents” or “sexy clips”; however, when they do so they find sexually

charged slogans, pictures of terribly mutilated accident victims or pornographic images.

- The glorification of anorexia
  A blog glorifying the illness anorexia nervosa is currently being indexed.
- Trivialization of alcohol consumption
  One German-language online forum trivializes excessive alcohol consumption. It relates closely to young people's lives and offers instructions for drinking games to play with friends. Rankings make drunken teenagers into heroes. This website could give young people the impression that excessive alcohol consumption is a normal part of everyday teenage life and party culture. The website hardly mentions the negative consequences.
- Mobile phones
  Problematic content is either downloaded from the Internet or passed between young people from mobile phone to mobile phone (e.g. "happy slapping" -videos). Individual data exchange between mobile phones is beyond the control of media regulators. Instead, the police are responsible for prosecuting such offences. Furthermore, it is required to work together with parents, teachers, etc. with a view to taking preventive measures.

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.).

(See also the answer to question 2.(2))
The most effective form of child protection in Germany is a white list of online content acceptable for minors. The list contains around 30 million sites. Children up to the age of twelve are the target group of this content. More information is provided under point 2.(4).

Besides, the programmes to protect minors used by content providers and access providers are made up of a combination of technical filters and the use of black lists of harmful content. The government agencies responsible for the assessment and approval of such programmes note that they are quite reliable when dealing with pornographic content. However, when it comes to violent material the underblocking or overblocking rate is regularly unacceptable. This assessment has meant that no programme for protecting children and young people has yet received state approval. This situation is dissatisfactory for companies as well as for government agencies, and there are plans to correct it in a joint initiative which will work out ways towards an obligatory self-assessment of content, the development of appropriate interfaces to process this information and towards requirements for black lists of inappropriate material.

(2) Does your economy have relevant laws and regulation? (If there are laws and regulation, please describe the overview.)

The provisions for protecting children and young people in the Internet are fixed in the **Jugendmedienschutz-Staatsvertrag** (JMStV), an interstate treaty which sets the common regulations for all Länder in Germany. The JMStV is legally binding for Internet service providers.

According to the JMStV, certain content is defined as absolutely illegal and cannot be posted on the Internet. An exception is, however, made for "mild pornography" and content which is "clearly extremely harmful to minors" or indexed content. As an exception, this content may be disseminated so long as it can only be accessed by **"closed user groups"**. Access to a closed user group is restricted by two steps: The first step involves checking that the user is over the age of 18. This step must involve personal contact. Secondly, each order must be authenticated so as to effectively reduce the risk of access details being passed on to minors.

The Kommission für Jugendmedienschutz (KJM, see answer to question 2.(5)) is the commission responsible for monitoring whether content which should not be accessible at all or should only be accessible to a closed user group is being publicly disseminated. The KJM works closely with "jugendschutz.net" to fulfil its responsibilities in the field of protecting children and young people. "jugendschutz.net" is a joint agency involving all the Länder and is closely associated with the KJM in its organization. It monitors websites which have come to officials' attention either as a result of general surveillance or due to complaints.

Certain content is not classified as harmful to children and young people. It can, however, impair minors' development into independent and active members of the community. This is content relevant to the protection of children and young people which is suitable to have a negative effect on a young person, but since it is not necessarily harmful to children and young people it is subject to looser restrictions. If service providers disseminate such content or provide access to it then they are responsible for ensuring that, under normal circumstances, minors in the affected age groups do not notice it. Internet service providers can comply with these requirements by ensuring that content which could harm the development and education of minors is included in approved **Internet filtering software**. Relevant filtering software for the protection

of minors is currently being tested, but thus far none has been approved by the KJM which is responsible for this. There is public demand for Internet filtering software for the protection of minors. Currently an **amendment to the law** is being discussed which is intended to lead to a new draft for the legal requirements for filtering software.
If it is suspected that content could have a harmful effect on a child's development only then the telecommunications provider fulfils its obligations by ensuring that the content is disseminated or accessible separate from content which is intended for children (content with the target group "children").

For information on the issue of **self-regulation** on the Internet see the answer to question 2.(3).

It is possible to index Internet content which is harmful to minors following a request or a suggestion. Media which has been indexed may not be advertised or made accessible to children and young people. A file which makes it possible to filter indexed online content, known as the **BPjM module**, has been prepared by the Federal Department for Media Harmful to Young Persons (BPjM, more information in English: http://www.bundespruefstelle.de/bmfsfj/generator/bpjm/information-in-english.html). Besides being used in filter programmes, the module is also an important part of the **voluntary commitment** made by German search engines. The module's integration in the participating search engines prevents the URLs of indexed Internet content appearing in the search results.

(3) Contents of voluntary efforts, such as self-regulation? (Does your economy have any self-regulation? If there is some self-regulation, please describe the overview. (Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.)

The Jugendmedienschutz-Staatsvertrag (JMStV) adheres to the principle of **regulated self-regulation** with the aim of strengthening the direct responsibility of broadcasters and Internet service providers and improving the opportunities for prior screening. The institutions of voluntary self-regulation are granted a statutory decision-making framework over which media monitoring has only limited inspection powers. This approach means that those adhering to voluntary self-regulation have a privileged position, providing an incentive to support the approach. The self-regulation institutions must be recognized by the KJM.

Self-regulation in the Internet: The **Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM)**, a registered association to oversee voluntary self-regulation, was founded in 1997 by media organizations and online industry companies. The association offers full members the opportunity to sign up to the voluntary self-regulation model contained in the JMStV. It also provides them with the opportunity to call on the FSM should they be involved in a dispute with the KJM. Therefore, these companies enjoy the privilege of approved self-monitoring for members as provided for in the JMStV. A company subject to the FSM's code of conduct can, nevertheless, be punished by the FSM for breaches of the code with a warning, a demand for remedial action, a disapprobation, a reprimand or an association penalty (monetary fine or exclusion) depending on the severity of the breach.

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

Germany has a wide range of policies to promote media competence and media education competence. The initiative **"A Net for Kids" – www.fragFINN.de** is a particularly promising project which seeks to promote child safety on the Internet. Children often surf the Internet unsupervised and in doing so may come across content which is harmful to them. Hitherto, approaches to solving these problems have simply been based on the use of filtering systems which are intended to block harmful content in various ways. The disadvantage of these conventional systems is that technical conditions mean that much harmless content, including websites intended for children, are unintentionally no longer accessible by the target group. This is where the initiative **www.fragFINN.de** has a role to play. The project is the first of its kind in Europe. It has created a safe space on the Internet in which children aged 8 to 12 can learn to use the Internet through independent navigation, without facing potential threats or the disadvantages of current filter systems. The project is backed by the Federal Government as well as the FSM and numerous media and telecommunications companies. It is supported by the public broadcasters, children's websites, the Land supervisory authorities for private broadcasters (*Landesmedienanstalten*) and institutions responsible for protecting minors from harmful media. Initially the project will run for a period of three years and is financed by the named companies. "fragFINN" is based on a databank, or "whitelist", put together by a team of editorially independent media pedagogy experts established at the FSM. The "whitelist" is consistently being monitored and expanded.

In its first five months “fragFINN” created a whitelist of several thousand domains and more than 30 million records. The whitelist is continually growing. All Internet service providers and users can contribute to www.fragfinn.de. The “Net for Kids” should also enable schools to purposefully integrate media competence into lessons without being restricted by the risks associated with the Internet.

An easy-to-install technical solution in the form of an Internet browser add-on enables parents and teachers to guarantee that children can only access websites which have been checked and are included in the fragFINN whitelist.

The second pillar of the initiative is an annual 1.5 million euros envelope which the Federal Government has allocated over a period of three years to provide financial support for high-quality and innovative Internet content for children. The funding is intended to increase the quantity, quality and accessibility of good online content for children.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

- **Kommission für Jugendmedienschutz (KJM)**

As laid down in the JMStV the KJM is introducing a joint system of broadcaster and telecommunications media monitoring for the first time in Germany (see above, question 2. (2)). This is to avoid the same content being subject to different laws in various media. The KJM acts in the service of the relevant Land supervisory authorities for private broadcasters and must ensure that private broadcasters and telecommunications media comply with the JMStV. The KJM guarantees close cooperation between all the institutions in Germany which work in the field of protecting minors. For example, the KJM works with the Federal Board for the Review of Media Harmful to Young Persons (BPjM) and with “jugendschutz.net”, which was created by the highest Land youth authorities as a central place for protecting children and young people in all Länder. Representatives of the BPjM, jugendschutz.net and the KJM meet regularly to exchange information and experience.

- **Voluntary self-regulation of multimedia service providers (FSM)**

The FSM cooperates with various partners, primarily on project level. The FSM has been a partner in the initiative “Deutschland sicher im Netz” (Safe on the Net in Germany) since 2005. In this way, the association has committed itself to an important cooperation with numerous companies in the IT sector and various associations. The common goal is to use various measures in order to increase Internet users' awareness of security issues. Ongoing communication with other German regulatory institutions and, above all, cooperation with international partners are of great significance in order to deal with complaints as effectively as possible. The FSM is in close contact with numerous foreign complaints offices. The association was one of the founding members of Internet Hotline Providers in Europe (INHOPE), the umbrella organization of European complaints offices.

- **Memorandum of understanding (November 2007)**

In November 2007 the operators of the Internet complaints office FSM, eco and jugendschutz.net together with the BPjM signed a memorandum of understanding with the aim of reducing punishable Internet content – in particular child pornography – in Germany. Increased cooperation and information-sharing between the different parties is intended to make their cooperation, which has been taking place for years, even more effective in forwarding, processing and pursuing leads on Internet child pornography.

- **"A Net for Kids"**

The initiative described in question 2.(4) is also an example of cooperation between state institutions and businesses in protecting minors from harmful media. This cooperation also exists in other contexts such as promoting parents' and teachers' media education competence.

- **Exchanging experiences with public service broadcasters on the law relating to protecting minors**

A regular exchange between representatives of the public broadcasters, the association of the Land supervisory authorities for private broadcasters (ALM) and the head of the KJM is required by law (Article 15.2 JMStV). It should be noted that in Germany the public broadcasters are autonomous and organized independently of the state. They themselves are responsible for complying with requirements for protecting minors (also with regard to their online services), whereas private broadcasters are subject to monitoring by the Land supervisory authorities (which utilize the KJM). The mandatory exchange is intended to promote the cooperation between the KJM and the supervisory authorities for private broadcasters and to guarantee that the law is consistently implemented.

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

Germany is part of the European support programme “Safer Internet Plus 2005-2008”. The current programme has a budget of 45 million euros to be spent on projects aimed at combating illegal and harmful Internet content internationally. The programme’s predecessors were created in 1999. For the longer term the European Union has already prepared a follow-up programme for the period 2009 to 2013. One focus of this work is establishing hotlines in the member states. In Germany the Internet association eco and the FSM are cooperating on this project and have established an Internet complaints office. The Länder agency “jugendschutz.net”, which has already been described, is a further example of a successful project which has received support. “jugendschutz.net” cooperates with 32 hotlines from 29 European countries and, as an Internet complaints office, is linked to other European and non-European complaints offices on the issues of racism and discrimination through the International Network against Cyber Hate (INACH).

The hotlines in the European Union member states work together as part of the INHOPE network, which is also supported by the programme. Operation “Marcy” in 2003 shows how successful these initiatives are. The police operation, which began in Germany, dealt a blow to Internet child pornography. This campaign was directly linked to a lead from the INHOPE network which had been passed on to the German law enforcement authorities.

A further focus of the programme is raising user awareness through national liaison offices, known as “Awareness Nodes”. These in turn cooperate on a European level through the INSAFE network. In Germany the initiative Klicksafe acts as the national liaison office and also receives public funding (information in English: https://www.klicksafe.de/ueber-klicksafe/die-initiative/Project_information/index.html). Furthermore, official “blocking orders” directed at domestic service providers can be used in individual cases to prevent the distribution of illegal content by natural persons or legal entities located abroad. During the negotiations on the European Community Audiovisual Media Services Directive Germany advocated keeping the law regarding blocking orders.

In Germany a discussion is currently taking place on limiting access to Internet child pornography which has been identified by the police. This instrument, known as access blocking, has been used by service providers in Norway, Denmark, Sweden, Finland, Italy, the United Kingdom, Switzerland, New Zealand, South Korea, Canada and Taiwan for many years. The Federal Government considers access blocking to be a suitable way to limit the scope of known child pornography websites. Accordingly, the Federal Government is currently examining how this could be implemented in Germany.

Under the German EU Presidency in the first half of 2007, the Federal Government organized the conference “More trust in content – the potential of co- and self-regulation in the digital media” in Leipzig with the support of the European Commission. Representatives of the European Union institutions, EU member states, voluntary self-regulation institutions, companies and associations as well as the research community took part. The aim of the conference was to share experience on successful models for co-regulation in the areas of protecting children and young people, protecting human dignity and consumer protection and to discuss the significance of and the requirements for co- and self-regulation. The process showed that transparency and a high profile, incentives for industry participation, effective sanctions, the guarantee of a procedure in accordance with the rule of law and an evaluation of the results are decisive for an effective co-regulation system.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

- It is the right and the obligation of the police world-wide to come up against illegal digital content. The arising problems stem from the lack of capacity of the authorities and the fact that citizens do not preferably turn directly to authorities in such fields. The solution was provided by the involvement of civil and professional organisations by „socialising" the above activities: introducing the www.internethotline.hu web address. The website has started operation in May 2005 based on European and international standards. Its main function was to receive notices concerning illegal and harmful content for the protection of those most endangered: children. The Hotline.hu project operated from 1st September 2004 to 31st August 2006 within the framework of the EU Safer Internet Action Plan.

As part of operating the above-mentioned website, the Hungarian Association of Content Industry (HACI) has concluded a cooperation agreement with the Hungarian police targeting illegal domestic online content.

About 50-60 percent of incoming notices had referred to pornographic or so considered contents and 20 percent of them referred to juvenile pornographic dissemination that is illegal by law (mainly photos, videos and chat forums). As an additional service complementing the hotline function, an Awareness Node was established too, that intended to provide a complex service against illegal and harmful online content.

As a result of the project it became evident that there was a clear need to provide wider scale and continuous promotion for the service, targeting mainly schools, teachers and parents.

- It also must be mentioned that there are several leaflets and booklets published for children to raise awareness of harmful Internet content.
- Other related issues concerned with: child pornography through the webcam, children's offensive behaviour against each other in school.

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy.
(filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

- The Hungarian Association of Content Providers has issued the self-regulatory Code of Content Providing that stipulates: "Content Providers commit themselves to make services, or information regarding the ways of utilizing services, easily accessible, when these may be used for the prior filtering of pages accessible for minors (the so-called filters) in the hands of persons in charge of taking care of minors. Such filters may include, among others: - AOL Parental Control – Bair Filtering System – CSM Proxy Server – Cyber Sentinel – Eyeguard – Genesis – Ifilter – Internet Sheriff – I-Gear – Kahootz – Kidz.Net – Net Nanny – Surfwatch – Too C.O.O.L. – Websense."

- There is a filtering software against Internet content labeled harmful by parents and school teachers. The so-called Safe Surfing Program is currently in use in 170 primary schools and 2500 homes. It is downloadable free of charge from the Safe Surfing Porgram's website: http://www.biztonsagosbongeszes.org/ (available only in Hungarian)

- There are some NGOs with websites for reporting harmful Internet content: e.g. Hungarian Association of Content-Industry (MATISZ)'s website: http://old.matisz.hu/urlap.php?id=27 (available only in Hungarian); Blue Line (Kék vonal)'s underaged victims' reporting website and telephone assistance: http://www.kek-vonal.hu/index2.php?m=16 (Hungarian speaking).

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

- According to the Act 4 of 1978 on the Criminal Code the following related acts are punishable by law: Crimes with Illegal Pornographic Material (Section 204), Abuse of a Minor (Section 195).

- It is forbidden by the Act XLVIII of 2008 (Advertisement Act) to advertise sexual services and sexual products, regardless of the way of appearance (e.g. newspaper, leaflet, website, etc.). The display of pornographic advertisement is also forbidden. Furthermore, the Advertisement Act laid down specific rules to protect children and juveniles:

Advertising may not be published if it may harm the physical, intellectual, emotional or moral development of children and juveniles.

Advertising targeted at children and juveniles may not be published if it may affect the physical, intellectual, emotional or moral development of them unfavourably, including in particular advertising which refers to or shows violence or sexuality, or the main characteristic of its subject is a violently solved conflict.

Advertising may not be published if it shows children or juveniles in dangerous, violent situations or in situations with sexual emphasis.

Advertisements of alcoholic beverages are also highly restricted (e.g. advertisements of alcoholic beverages shall not target children or juveniles).

- Law relating to new media (such as mobile phones) is currently developing based on EU Directives. The National Audio-Visual Media Strategy (NAMS) is also under development. NAMS will re-regulate the legal regulatory environment for confining paedophile content on the filed of the new media also (mobile, digital TV, cross-media).

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

- The Hungarian Association of Content Providers issued the self-regulatory Code of Content Providing concerning the regulation of operations, ethics, and procedures with respect to content providing. According to this Code the “Content Providers commit themselves to inform users before entering a service in case it is, wholly or partially, susceptible of being harmful for minors. Attention must be raised to the quality of such contents before accessing them, and the user must actively confirm that he/she has passed the prescribed age limit; the surface reserved for this purpose may not contain visual, textual, or any other kind of items pertaining to the actual content. Content Providers

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

- Within the framework of the Safer Internetplus (SIP) Programme of the European Union, Safer Internet Combined Nodes are to be established in Hungary to tackle illegal content and to promote a safer online environment.

To implement the complex and integrated project a consortium was established with the presence of the International Children’s Safety Service, the Hungarian Association of Content Industry, Theodore Puskas Foundation and Kék Vonal Child Crisis Foundation to manage the combined safer internet nodes, hotlines, awareness nodes and helplines.

- The development areas within which students are trained to evaluate the information deriving from the media and different information surfaces are defined in several subject fields of the National Core Curriculum, such as Man and Society, Our World and Environment, Visual Culture. Pupils interpret the message of advertisements and marketing effects, the possibility of choice and the adequate use of mass media through actual examples, role plays and controlled discussions.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of "learning information moral" based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

- The Hungarian Police created an Internet-Police department (specialised police unit for cyber-crime, child pornography) in 2000. In 2002-2003 the Internet Crime Department of the Hungarian Police Force – Directorate of Crimes was established. Nowadays the results of its work are emerging. According to the Police, there was a high increase in the disclosure of paedophile contents in 2006. There were 4 cases, where, based on previous hotline activities, a Hungarian member of an international paedophile network was found. The High-tech Crime and Extremism Department of National Buro of Investigation also deals with similar issues. Other bodies: National Institute of Criminology, Friendly Internet Forum (BIF including: Inforum (Forum of Hungarian IT Organizations for Information Society, www.inforum.org.hu), MTE (Hungarian Content Providers Association, www.mte.hu), CERT-Hungary, MATISZ), International Children Safety Service.

Related websites:
www.biztonsagosinternet.hu
www.baratsagosinternetforum.hu

- National Institute of Criminology, Safe Surfing Program and Symantec are on the way to work out Hungary's Internet child protection strategy. The strategy's aim is to develop an action plan according to "Safer Internet" program of the European Union embracing a raising awareness campaign to pupils, parents and teachers about how to use Internet safely, how to prepare for facing harmful and disturbing content, how to act when pupils encounter this kind of material. It is also planned to supervise current legal rules and prepare an empirical research on students' popular online activities and the risk factors. Ministry of Social Affairs and Labour has recently joined this project. For more details see http://www.police.hu/friss/BRF-20081108_23.html (in Hungarian).

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

- There is a Consumer Protection Cooperation network (CPC-network) including the consumer protection authorities of the 27 EU-member states, Norway and Iceland. In June 2008, enforcement authorities carried out simultaneous, coordinated checks of webpages in the sector of mobile phone content service (such as ring-tones and wallpapers).
- The Hungarian Association of Content-Industry (MATISZ) is a member and domestic representative of INHOPE.
- Other related forums (with Hungarian participation):
  - Building a Europe for and with children (www.coe.int/children) – i.e. a Council of Europe programme for the promotion of children's rights and the protection of children from violence
  - World Congress III Against the Sexual Exploitation of Children (Rio de Janeiro, 2008)

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

ITALIAN DATA PROTECTION AUTHORITY

WE HIGHLIGHT THAT OUR ANSWERS TO THE QUESTIONNAIRE DO NOT REPRESENT THE FULL VIEW OF THE ITALIAN GOVERNENMENT BUT ARE ONLY BASED ON THE EXPERIENCE AS DATA PROTECTION AUTHORITY

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

From the experience gained so far from our activity as data protection authority we can refer to:

- Growing cases of abuse against minors, often perpetrated by other minors, and poured into social network websites ("bullyism"). In particular, in one case some high school students, filmed their abuses against a schoolmate, with disabilities, and posted the video on YouTube. The Italian judicial authority intervened for defamation and privacy violation, not only against the students, but also – with a highly controversial decision – against Google. The case is being examined by the competent judicial authority.

  The press also reported of cases of suicides of teen agers caused by the shock of knowing that their photos showing them in sexual attitude, were posted on the web by their ex-boyfriends.
- Cases of publications by newspapers - also in their on-line version - of episodes of abuse against children who were made identifiable by various details given by journalists. The Italian Data protection authority, in a recent case (10 July 2008) has prohibited some newspapers to disseminate - also through their web site - information that could even indirectly identify minors involved in cases of sexual abuses (see also answer 2.2).

,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy.

(filtering technology, detecting technology, mobile phone and other handheld

device specific technology, etc.)

As data protection authority, we highlight that the need to protect children from harmful content must be balanced with the need to avoid arbitrary or unlawful interference with the minor's privacy, as recognized by the UN convention on the Rights of the child, and data protection laws.

(2) Does your economy have relevant laws and regulation? (If there are laws and regulation, please describe the overview.)

As regards the privacy issue, we recall that Italian law prohibits the identification of minors involved in criminal procedures, in particular where victims of sexual abuse. Safeguards for minors have been strengthened by the Data Protection Code that extends such safeguards to minors involved in civil law procedures. These provisions, applying also to on-line publications, were at the basis of the abovementioned decision of the Italian DPA (answer n. 1) regarding the prohibition of publishing – both off and on line –particularly sensitive information related to minors, that once revealed can cause serious infringement of their rights and dignity.

(3) Contents of voluntary efforts, such as self-regulation? (Does your economy have any self-regulation? If there is some self-regulation, please describe the overview. (Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

- On 2003 a "Code of Conduct on Internet and minors" was signed by different associations of Internet providers together with the Ministry of communications and the Ministry of new technologies. The Code aims at promoting measures to prevent minors from getting in touch with harmful contents, in the respect of the child's privacy and right to data protection. The Code promotes: a classification of contents in order to guarantee a selected access to certain contents; the use of system to understand the age of the user, in compliance with data protection law. More precisely such systems cannot lead to the identification of the minor, to his/her domicile, e-mail address, nickname, IP address and should not allow third parties to reach the minor directly or indirectly. Providers have to abstain from profiling the minor without his/her parents authorization.

- As regards data protection issues, on 2006 a new self regulation Charter has updated a previous one (Carta di Treviso, 1990) regarding the specific issue of protection of minors in the field of journalism. The new version of the Charter extends the principles that journalists have to respect regarding minors, also to the information given by the new media, namely the Internet. The Charter, aiming at balancing freedom of expression with minors' rights, states the principle of anonymity of the minor involved in reporting of court cases. Moreover, Journalists have to omit details that can lead to the identification of the minor, especially in cases of pedophilia or other abuses. Journalists have to avoid emphasis on particularly crude events regarding minors (suicide, etc.) that can cause an emulation effect. Such Charter is also referred to by the "Code of practice for data protection in journalism" that is annexed to the Data Protection Code. Such Code of practice, that also states that the child's right to privacy must take precedence over both freedom of expression and freedom of the press, is a peculiar one, since the violation of its principles leads to an illicit data processing. Its principles are valid also for on line journalism.

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

- Within social network, the Italian DPA is working on awareness raising campaigns, particularly towards young people, regarding the risks of this new phenomenon. The aim of such activity is to point out that notwithstanding the several positive features of social networks in terms of social aggregation, it is especially important for (young) users to be aware of the risks – both to themselves and to others - caused by an excessively "easy" use of such networks.

- On 30 September 2007, the Ministry of Education has circulated a directive regarding the use of videophones at school. The document aims at raising the awareness of students regarding the risks of unrestrained circulation (also over the web) of video recordings as refer to data subjects' rights and data protection.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

The Italian Data Protection authority participates in cooperation activities at both European and international level.

The Italian DPA took part to the “International Conference of Data Protection and Privacy Commissioners” (Strasbourg, 17th October 2008) where a “Resolution on Children’s Online Privacy” was adopted. In such Resolution the Commissioners resolved to strive to ensure children and young people around the world have access to a safe on line environment respectful of their privacy; to call for appropriate limitation of processing of information about children or the purposes of on line micro-targeting or behavioral advertising.

Moreover, the Italian DPA, as member of the Article 29 Working Party, (the independent EU Advisory Body on Data Protection and Privacy established by Directive 95/46), also participates in the activity carried out by the Working Party regarding privacy issues on the Internet and social network. The Article 29 WP is working on the drafting of an Opinion on social network.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

- ■ Posting of spams that advertise video chatting and online escort service agencies on blogs and online bulletins
  - ✓ Restrictions on the advertisement of video chatting and online escort service agencies, recognized as harmful-to-minor content in December, to minors
- ■ Inflow of Illegal gambling and sexually explicit websites operating with servers abroad
  - ✓ ISPs block access to harmful websites based on the list of illegal foreign websites containing harmful content that have been blockaded in Korea in accordance with the "Act on Promotion of Information and Communications Network Utilization and Information Protection" Item 1, Clause 7, Article 44-7

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008.

Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website.

Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

- ■ Korean ISPs are required to establish filtering measures against illegal foreign websites.
  - ✓ ISPs filter harmful illegal websites through international Internet gateways with exclusive equipment (Enables prevention of various loop around connection down to the sub-directory level)
- ■ As part of the policy for juvenile protection, the Korea Communications Standard Commission provides content filtering software technology and database of Internet content ratings to effectively block harmful websites for minors
  - ✓ Distribution of the database of over 540 thousand foreign websites that have been rated according to the SafeNet

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

- ■ In accordance with the "Act on Promotion of Information and Communications Network Utilization and Information Protection"
  - ✓ (Article 42) Those who provide harmful-to-minor content (defined by the Juvenile Protection Act, Item 3, Article 2) to the general public using telecommunications services shall indicate that the content is off-limits to those under the age of 19 in the form of voice, words or image.
  - ✓ (Clause 2, Article 42) Information containing advertisements of harmful-to-minor cannot be transmitted to minors and cannot be openly exhibited without any access limits.
  - ✓ (Clause 3, Article 42) Information and Communications service provider with daily hits of 100

(Example: Current Status of Japan)

In Japan, following matters are stipulated by "The Law on environment of development for children's internet usage";

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?

(Does your economy have any self-regulation?

If there is some self-regulation, please describe the overview.

(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

- Many private civic groups, namely KT Cultural Foundation, Internet Ethics Assembly, Voluntary Agency Network of Korea, Sunfull Declaration Campaign for Positive Web Comments and Parents Association, are promoting cyber ethics education programs for youth.
  - ✓ Various events – public campaigns, poster competitions, exhibitions and workshops- are held to raise the social awareness on the internet ethics.
- Corporate associations such as K-internet are also active in preventing possible side-effects of the Internet by establishing the Association of Voluntary Internet Regulation and coming up with an industry-wide universal guideline.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association),

(IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

- Schools are increasing internet ethics education programs in their regular curriculum. Besides this, various sessions about internet ethics are prepared for students' extra-curricular or after-school activities to improve pupils' understanding on the importance of ethical use of the internet.
- The KCC organized the internet ethics education session for students and teachers of elementary and middle schools through 2008 vocational training program for teachers, and is planning to further expand the program in 2009.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of "learning information moral" based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

- In 2008 the KCC supported various internet ethics campaigns and seminars organized by private groups and media companies.
- And in 2009, the Commission is planning to strengthen its effort of enhancing public awareness about internet ethics through various education programs, public campaigns and international cooperation, mainly in partnership with private organizations.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

- The KCC plans to organize “Safer Internet Day” event in collaboration with EU Insafe.
- Also it will actively cooperate with the international community through its activities in I-SOC and IGF, sharing related information with other member countries.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

1. Internet Access in Public Places

A large amount of people access the internet from public places, such as Internet cafes; around 39% of internet users, so they do not have parental supervision.

2. Increase in the use of Social Networks

Personal information is posted on these sites, as well as other kinds of harmful content, such as photo or video sharing.

3. Growing use of the internet by children and teenagers

The number of children and teenagers who use the Internet is in constant rise, and very often they use the Internet without parental supervision or guidance.

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

1. Some IPS have content filtering applications, but are not commonly installed and/or used. There is also available software; however, due to the lack of parental involvement, these are not used or children find a way to avoid them.

Mobile phones and handheld devices don't have content filters. Minor's use of these devices has spiraled in the past, and so has their exposure to harmful content.

(2) Does your economy have relevant laws and regulation? (If there are laws and regulation, please describe the overview.)

2. In Mexico there are no laws and regulations, only those adhered to by the Mexican Government in international treaties, such as the Convention of the Rights of the Child or pre-internet legislation relating to the Sexual and Commercial Exploitation of Minors. However, there is a Cyber Police division of the Public Safety Ministry, which deals with accusations related to safety matters on the internet.

(3) Contents of voluntary efforts, such as self-regulation? (Does your economy have any self-regulation? If there is some self-regulation, please describe the overview. (Example: participating parties, content, target contents, establish age restriction,

status of the implementation of content rating, relation with laws and regulations, etc.))

Some private efforts are made to create awareness and self-regulation. Some entities which do so are AMIPCI (Mexican Internet Association), ISI (Internet Safety Institute) and the Telmex Foundation. Work is being done to alert and educate users, specially parents, children and schools in order to restrict the content viewed by minors.

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

Mexico has no policies regarding these issues, but there is a growing awareness that access to harmful content among minors is an increasing problem. Some research sponsored by local governments, public and private institutions are being carried out to determine the extent of exposition among minors to harmful content.

Private institutions, such as ISI and Navega Protegido, give talks in schools to parents, teachers and students about addiction to online pornography, specifically mentioning causes, symptoms and rehabilitation. Other institutions have gone to schools, radio and television to talk about risks to be encountered with internet use; held seminars among mental health professionals to discuss therapy and rehabilitation for minors addicted to online pornography; there is a safety campaign promoting safe websurfing; AMIPCI issues a safety seal to websites without harmful content and safety and privacy of information policies, and there has been numerous media activity to raise awareness.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

There is cooperation between representatives of the civil society, AMIPCI, ISI and "Navega Protegido", and government health ministry and the senate to promote children protection when using the internet.

(6) Does your economy cooperate internationally on these issues? If there is some

Yes, Mexican representatives have attended ICANN Meetings and AMIPCI create Sellos de Confianza AMIPCI (AMIPCI's Trust Mark). Telmex and ISI are active in the Family Online Safety Institute (FOSI) .

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

No specific concerns regarding information harmful to children. In general The Netherlands, in line with European policy focuses on the safety and wellbeing of children online. Important these are cyber bullying, grooming, child pornography en digital identity (also in relation to networking sites).

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008.

Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website.

Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

In the Netherlands, different companies and organisations and ISP's provide filtering software. Filtering software offered is based upon black-listing or white-listing. In the Netherlands, inspired by the British good practice, we conduct a joint survey of the various technical possibilities and determine their effectiveness and lawfulness. The intention is for ISPs to jointly establish a platform that designs and distributes filters for its clients and maintains a so-called blacklist.

In 2008 the Dutch government and private parties agreed on a Notice and Take code. This voluntary code agrees on a set of guidelines for the response to unlawful content on the Internet and the way private parties erase this from the internet.

The "Meldpunt ter bestrijding van Kinderpornografie op Internet" (the Hotline combating Child Pornography on the Internet) is an independent private foundation and was officially opened by the Ministry of Justice in June 1996. The Dutch Hotline was created at the initiative of internet providers joined in the (now dissolved) NLIP as well as individual Internet users. Main objective is to contribute to the reduction of the distribution of child abuse images via the internet. The hotline is part of the INHOPE network and was founded in 1999 under the EC Safer Internet Action Plan.

The 9th of feruari 2009 Europe's major social networking sites (Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo!Europe, and Zap.lu) have come together for the first time at this year's Safer Internet Day to recognise their responsibility and identify potential risks on their sites for under 18s. These include cyberbullying (harassing children on internet sites or via mobile messages), grooming (when an adult befriends a child with the intention of committing sexual abuse) and risky behaviour like revealing personal information. They aim to limit these risks by:

- Providing an easy to use and accessible **"report abuse" button**, allowing users to report inappropriate contact from or conduct by another user with one click.
- Making sure that the full online profiles and contact lists of website users who are registered as under 18s are **set to "private" by default.** This will make it harder for people with bad intentions to get in touch with the young person.
- Ensuring that **private profiles** of users under the age of 18 are **not searchable** (on the websites or via search engines)
- Guaranteeing that **privacy options** are **prominent and accessible** at all times, so that users can easily work out if just their friends, or the entire world, can see what they post online.
- Preventing **under-age users** from using their services: if a social networking site targets teenagers over 13, it should be difficult for people below that age to register.

Social networking sites will inform the Commission about their individual safety policies and how they will put these principles in place **by April 2009**.

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

Undesirable / unasked communication

- European Privacy Directive
- National Telecommunication law

Unfair business-to-consumer commercial practices in the internal market

The laws relating to unfair commercial practices show marked differences which can generate appreciable distortions of competition and obstacles to the smooth functioning of the internal market. In the field of advertising and misleading advertising,.

In the past decade, the Netherlands has worked hard at organising our legislation on the sexual abuse of children and aligning it with various international legislative instruments. Currently we are implementing the so-called Lanzarote Convention[1]. The manifestation of commercial child abuse is, after all, greatly influenced by rapidly changing information and communication technology. The Lanzarote Convention has a wide scope and multidisciplinary charachter and especially deals with phenomena such as online sexual abuse and virtual child pornography.

- Dutch legislation on sexual abuse, prostitution, trafficking in human beings, child pornography and adoption, viewed as a whole, criminalizes the behaviours addressed in the relevant international teaties and agreements. Protocol.
- The implementation of the Lanzarote Convention leads to further tightening Dutch criminal legislation on four important points, namely:

  - tightening the penalisation of child pornography (criminalisation of obtaining access, through information and communication technologies, to child pornography);
  - specific penalisation of corrupting children;
  - separate penalisation of ‘grooming’;
  - extension of jurisdiction for sexual exploitation and sexual abuse when the offence is committed abroad against a national or a person who has his or her habitual residence in the Netherlands.

Further, the statutory penalties for trafficking in Article 273f of the Criminal Code will be raised. The statutory penalty for trafficking in minors will be raised from six to eight years (Article 273f, paragraph 1, Criminal Code).

When the offence is committed in conjunction or against victims below the age of sixteen the statutory penalty will be raised from eight to twelve years (Article 273f, paragraph 3, Criminal Code).

Penalties can rise up to eighteen years when committed under further aggravating circumstances. This legislation is pending in Parliament.

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

Notice and Takedown code of conduct (NTD)

This NTD code is an initiative of organizations that are willing to combat the presence of unlawful information (‘content’) on (the Dutch component of) the Internet. The initiative has originated from the desire of governmental and private sector organizations to establish agreements in the field of Notice-and-Take-Down (NTD). A description of the form and substance that these organizations have given to these agreements is presented in this code. Use has been made of both expertise in the field and best practices in the drawing up of the NTD code. The code establishes no new statutory obligations, but is intended to help organizations to operate with care within the existing legislative framework in the removal of information from the Internet at the request of third parties. A procedure is described for this. Complying with the code is voluntary, and there is no formal enforcement in the case of noncompliance. The benefits of complying with the code lie in the achievement of more efficient procedures and in the reduction of liability risks. The organizations that endorse the code operate according to the procedures described here. It is therefore a code of conduct that lays down the conditions for the interactions between the parties involved. The NTD code addresses the way reports concerning (alleged) unlawful content on the Internet are dealt with. In addition, the code can also be employed with respect to content that intermediaries consider to be undesirable or damaging. The code should contribute to the ability of private individuals and organizations to deal effectively with these types of reports between themselves as far as possible. The possibility always remains for them to bring the matter before the courts or to make an official report to the police.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

The programma Digivaardig en Digibewust (digitally competent & digitally aware) is a 5 year program The total budget for this programme is estimated to be € 2,5 million per year. € 2 Million per year is made available by the Ministry of Economic Affairs. Several partners (both private sector and civil society) will each bring € 50.000. Each year the Safer Internet Day is being organised to raise e-safety awareness amongst children in the Netherlands.

Also the ministry of Education, Culture and Science launched a programme on Media Awareness (www.mediawijsheid.nl). And the Ministry of Justice will launch in the summer of 2009 a country wide campaign to gain awareness on cybercrime.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

Several public, private and civil society partners are involved in a programme on digitally competence & digitally awareness (www.digivaardigdigibewust.nl) . Part of this programme is specifically targeted at children. Activities focus on matters such as password protection, digital identity management, cybercrime, cyber bulling, grooming, social networking sites, gaming etc. The programme is a PPP. Public partners that are involved are for example the Ministry of Home Affairs and the Ministries of Education and Justice. Private sector partners are e.g. Microsoft, UPC, KPN and IBM. Civil society partners include several interests groups (the central organisation of libraries, Secondary Schools, etc.) and several leading scientists. We are constantly striving towards more involvement and commitment of relevant partners.

Notice and Take Down

The Code of Conduct is based on good practices from businesses, governments and other parties involved in fighting cybercrime. The Code has been drawn up under the flag of the National Infrastructure Cybercrime (Ministry of Economic Affairs) by market parties including KPN, XS4ALL, ISPConnect, Dutch Hosting Provider Association, NLKabel, Ziggo, UPC, CAIW, Zeelandnet and SIDN. Ministries, the police and investigation services and organisations including Marktplaats/eBay and the BREIN foundations collaborated in setting up the code. “Affiliated businesses - 85% of all access providers and the large majority of hosting providers – hereby send a clear signal that the internet is not to be used for illegal practices.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

The Internet Hotline Center in the Netherlands joined the INHOPE network in 1999. The program “digitally competent & digitally aware” functions also a the awareness node in the Insafe network of the European Commission (www.saferinternet.org) which is part of the Digital Safer Internet Program Plus.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008.

Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website.

Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

CATEGORIES OF PROBLEMS AND RISKS

1 TRUTHFULNESS OF INFORMATION FOUND ON THE INTERNET

Younger girls trust some information from the Internet and some not. They agreed not to trust horror stories – even though they make them upset and cry.

- *They also distrust funny websites – but information presented in a factual way, about people (not*

about ghosts or poltergeists); they trust them.

- *When comparing truthfulness of information from different sources, they first trust their parents,*

teachers and books rather than the Internet, and equally to the Internet and information from TV. As far as classmates are concerned, only one trusts them more than the Internet. The main reason

for certain distrust in classmates is the assumption they've obtained most information from the Internet.

- *Older girls broadly agreed that their parents do not have to worry about believing untruthful*

information from the Internet. They believe in themselves and they are convinced they can find out what's true and what's false by checking other information sources. They also rely on their ability of logical (see: correct) thinking.

- *They also use their experience in what can be considered truthful/untruthful: e.g. www.sme.sk is* much more truthful than www.bleskovky.sk.

- When comparing the truthfulness of the Internet with other sources – parents, teachers, books, their opinions are not as unambiguous as the younger girls. To a certain extent, they doubt the truthfulness of information from books. In this context, they admire only that logic is not enough to decide what information is correct (an example of unambiguous information is history matters, different interpretation from different sources, including school).
- Parents and teachers were considered to be rather reliable sources with substantially lower conviction than in the younger group.
- Younger boys spontaneously expressed their trust in information from the Internet in 50:50 proportions. They think there is rubbish that may not be right and that cannot be verified from other sources. They give examples of a loaded game costing 72 SKK but it deducted much more from their credit, etc.
- Unambiguously, everyone primarily trusts their parents. Truthfulness of information from the Internet is equal to information from TV. As far as friends are concerned, they trust some of them. It depends on the matter discussed.
- They found false information on the Internet – e.g. about a prize that was not a prize in reality.
- Also, older boys think the Internet is a truthful source of information in 50:50 proportions. In comparison, they trust encyclopaedias 100%, whereas other books rather conditionally. Also, teachers are a more truthful source of information than the Internet. Parents, friends and Internet are truthful sources in equal proportions.
- And they more trust learning TV channels than the Internet.

2 POTENTIALLY SHOCKING CONTENTS

- If younger girls encounter erotic information (particularly pictures but texts as well), they unload to their mothers who usually advise them to pay no attention to it and if possible, they delete such information from the computer. A specific step – to write to the sender of the pictures to stop doing that – was taken by two fathers.
- This group contained one girl who asked her teacher (without any success) and a girl saying that she does not deal with such matters with adults.
- Specifically, one girl recalled a scene sent by her classmates on affliction and torture of a cat. She was shocked and supposedly said to the boys to stop it and delete it. She also told her mother, who advised her to forget it and think about school and her obligations.
- Older girls mentioned brutal scenes they saw not only on the Internet but also on mobile

phones of their classmates. These were scenes from the Hostel movie as well as the Iraq war, pictures of a fight between a human and anaconda, pictures from necropsy. Girls talk about these shocking scenes and denounce them.

“We say together it is disgusting and that’s it.” (Girls group, 12 - 14 years).

- One girl talked about it with her mother.

“I have to say she disliked me watching it.” (Girls group, 12 - 14 years).

- Girls agree that parents can see it as a risk but they believe it is particularly bad for small kids who are shaping their opinions now. They also noted that such pictures are not only on the Internet but also in different magazines as well.
- Younger boys spontaneously mentioned porn; brutal was the killing (!) of Saddam Hussein, burning of a cat to death, scenes from fights in a Russian school as well as a game where a woman gets undressed/dressed, etc. Most of them do not talk about it, exceptionally with friends, nobody with parents. They watch it secretly and know their parents would disagree. They know this is a risk. Most of them say they turn it immediately off so that their mothers don’t see it.
- The group of older boys spontaneously mentioned the burnt cat from Trnava – those publishing it on the Internet were classified as “stupid bastards”. Detailed discussion revealed they were incensed by it as well as by the boasting (therefore the bastards) and by hurting the feelings of other people.
- Porn websites, often within online games, are another shocking experience; everybody experienced that as well as Rodem – morbid pictures from all around the world.
- They talk about it with their classmates, friends; not with parents. Some of them do not talk about it at all. Reactions from the boys are mostly negative, they feel caught, they are tuned to a game and now

“…that is so disgusting” (Boys group, 12 - 14 years.)

- Classmates also navigated them to Rodem (most of them know it). The group considers it brutal and according to the boys, Nazis produce these websites.

3 POTENTIALLY DANGEROUS CONTACTS

- Some of the younger girls admitted they had already chatted with unknown people – some say they were addressed and maintained written contact with somebody (they did not always believe they’d get truthful information from the strangers), but fears of further steps always won over and they terminated the contact before any personal meeting. Should they be addressed – without their *own initiative –half of them say they would talk about it with her parents; the second half with their best friend.*

- *During the discussions, the girls seemed to the risks of this theme and although they nodded affirmatively to the fact this is dangerous and that they can see the fears of their parents, they consider it rather an abstract problem, a game they have control over.*
- *Older girls normally chat – mostly with friends. But they also consider chatting with an unknown person as an adventure. Many of them have already chatted with an unknown person but they think they can estimate whether that person is telling the truth about his/her age. They make sure – both themselves and the people around them – that they never give any details, address, phone numbers, etc. They are also convinced they can guess when questions from the other person start to exceed the framework of common conversation. At this moment, the contact terminates – many of them terminated the contacts. The reasons for terminating were queries about the school they attend as well as other queries facilitating their identification. This type of relationship excites them and they are willing to violate bans of parents, who in one case revealed the relationship thanks to the mail the contact sent (despite the ban of parents, the girl still keeps in contact and asked the unknown not to send any mail).*
- *Girls mentioned positive cases as well, when coevals of their parents found life partners via chatting. Girls also mentioned cases of their acquaintances that changed their name and address so as not to be bothered further. But in principle they think that when somebody sails under false colours "it is not so bad; it is less risky than if it happened to us personally."(Girls group, 12 - 14 years).*
- *Most of them think their parents trust them and that they are able not to take risks. They divulge nothing, do not ease identification, stop reactions in the event of the first feelings of danger, they change their address.*
- *Spontaneously, there was the opinion that such contact is much worse via mobile phone, which is easily detectable and more risky, especially because "I can't have my mobile turned off for long and the number is more difficult to change." (Girls group, 12 - 14 years)*
- *Younger boys recalled information from the Internet and radio and TV news on children being kidnapped because of organs transplants or for porn movies. Supposedly, they do not establish such contacts but almost everybody knows a person doing it – either a relative or classmate.*

They would advise such a person to contact the police, e.g. in the form of meeting under its assistance.

Again, they would rather not inform their parents.

- Older boys do not have this experience and they know nobody doing that because – as they say – nobody unloads them. They believe they would not be tricked to say a contact to them – and they would not go anywhere with unknown people. But they can see it as a risk.
- **Bullying**
- The girls have vicarious experiences with Internet bullying (it happened to a friend). They believe it is necessary to reply (if possible) and ask them to stop it or ignore it,

"…do not bother about it because stupid people send such things" (Girls group, 9 - 10 years).

- Older girls see no risk in **slandering** either by them or against them on the Internet. According to them, it hurts nobody and it is the same as if friends traduce each other. The protection is – if somebody worries – finding who wrote that and respond and tell the truth. Most of them admit they would be personally offended, however after certain time they would be willing to settle. They do not consider it a problem and see it as highly unlikely that something could happen to them.
- The first reactions of younger boys were **threats by Nazis or skinheads**. Then one remembered the threats the mother of one of them received. They would recommend contacting the police, not a friend:

"he would blow it open" (Boys group, 9-10 years).

They can consider it as a risk and threats as a criminal offence. (Boys group, 9-10 years).

- Older boys revealed in the discussion that they know a classmate who misused a photo of a female classmate and published it with defamatory text on the Internet. Supposedly, it was revenge. The participants classified it as a funny act.
- When the discussion touched what they would do if something like this happened to them, the first reaction would be to turn it off, and send a similar thing to the author to see how's that. One participant would tell the police, another their parents and then the police, somebody a friend. There was also the idea of sending a virus to give over. The discussion was rather inconsistent, surprising in the light of the earlier mentioned negative experiences of this group. Things that involved or could involve them were classified and experienced rather differently than the same committed to somebody else.

IV.4 DECEPTION ON FREE OF CHARGE CHARACTER

- Almost all the girls, at least from friends, have experience with Internet deceptions. For example, all of someone's credit was used for downloading a file although promised it would not happen.

More girls have similar experiences with Moje hry, particularly with IQ-tests. The girls think the only solution is not to download them. In principle, they think their parents may not worry about them because they punish (and learn) themselves for being without credit.

- *Many girls in the older girls group know – at least by hearsay – that warning on charge is written by small and almost invisible letters. They consider it incorrect and unfair. They have their own experience with deceptions via mobile phone when their credit fell to minus amount. They know it happens more often with mobile phones than on Internet. Somebody also experienced payment of 200 SKK instead of 2 x 36 SKK advised in advance. They warn their friends to pay attention to such deceptions. One complained to a friend who tells her off for downloading this. Nobody discussed this matter with their parents and would not do it in future. They would rather stop downloading.*
- *Younger boys gave examples that they received a different song than ordered. They also downloaded a game, which was subsequently charged. They advise to find help – without detailed specification; the hint to ask parents for help did not succeed.*
- *One boy of the group has a friend who paid 1,700 SKK for participation in a competition. The story made the group rather incensed, the group spontaneously called for punishment with the help of parents, the police and the court.*
- *It was considered a serious problem and big risk. Other competitions with unreal promises were named as a deception.*

5 ILLEGAL DOWNLOADING

According to statements from the group of younger girls, none download music or movies that have to be paid for. The girls think that the pictures they download are for free and they have no idea of payments for music. Only one knows that intermediately – her parents own a shop and always mute music when a customer enters their shop because they don't want to pay for the music. The others are surprised that payments are required.

Younger boys knew that downloading some things is illegal but admitted they would never think of preying on the author. After a silence, one said: “We should not do it”, another boy said: “Just a few people, it won't do any harm”; another boy argued about the high prices of a new game he could download for free, etc. Finally, the opinion of the impossibility of downloading it and protecting it against downloading won. They consider it to be a problem but much less than killing somebody.

The group of older boys knows the possibility of illegal burning and downloading but they think it should not be illegal if it is for their own use without trading. They think that if burning a DVD were

impossible, for what purposes are DVD burners? Therefore, it should not be considered a criminal
offence.
(PSYMARECO study 2007)

2. Current methods to manage access to information considered harmful to children

- *Filtering technology,detecting technology (Crawler Parental Control, K9 Web Protection, ParentalControl Bar, Internet Explorer controll, PassManager, AreaGuard, OptimAccess..)*
- *Creating conditions not permitting production of websites of unwanted content Boys group,9-10 years;*
- *Implementing and enforcing protection against burning (optionally all);*
- *Do not uploading games to Internet – to produce CDs for loading "appropriate" games and the others with fight games. This differentiation would allow parents to select what to buy fortheir children Girls group, 9 - 10 years;*
- *Emphasising and to legally and socially supporting the responsibility of parents – transfering risks upon them including responsibility (let them contact admin to discuss what's authorized for a computer and what is not), disable unauthorized things (Boys group, 12 - 14 years)*
- *Sanctions and bans:*
- *to disable the websites – the codes would be known to parents only (optionally all);*
- *in case of breaching the ban, to apply sanctions – rejecting a PC (Boys group, 9-10 years);*
- *developing and implementing an application allowing parents to check via a mobile phone what websites are being browsed right now by their children (Boys group, 12 - 14 years);*
- *determine an age limit for individual applications – 14 years of age proposed (Girls group, 9 - 10 years). The most frequent proposals applied to the possibility of disabling certain websites to avoid unauthorized access (by a child).*

***More drastic forms**:*

- *to ban access to the PC, internet. Contra-proposal: banned things are more attractive;*
- *to ban access to some applications. Contra-proposal: see above, results in the opposite;*
- *not to access Internet;*
- *an application informing parents who was where and when (optionally different);*
- *an application rejects a computer if the ban is breached;*
- *protect games from burning – software exists.*

(Psymareco study 2007)

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

*Law **22/2004** Coll**. on Electronic Commerce and on Amendment of Act No. 128/2002** Coll**.,** Act No. **147/2001 Coll**. **on Advertisement**, **428/2002 Coll**. **on Protection of personal data** as later amended, we do not have specific legislation concerning protection of children on internet.*

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.

(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

Self regulation – civil associations such as eSlovensko, organization SK-NIC, as, Ministry of interior of the Slovak republic, Unicef, Telefonica O2 are partners of the project concerning protection on internet: www.zodpovedne.sk.
They are active working in area of propagation of danger for kids on internet, producing materials, prospects, brochures to prevent the risk of dangerous and abusive informations from internet, mobile communications and new technologies for kids.

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification

etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association),

(IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues?　What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

As I mentioned before-Unicef together with partners organize the discussion,promotion of brossures,　and other activities as education in the school to rise awareness
The protection have to be provided by parents, controlling the activities of the kids on internet, eventually protection software on the home or school computers.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

Civil associations such as eSlovensko,organization SK-NIC, Ministry of interior of the Slovak republic, Unicef, Telefonica O2 are partners of the project concerning protection on internet: www.zodpovedne.sk.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

There is a webwww.pomoc.sk. part of the project “www.zodpovedne.sk, supported by European commission within the program “SAFER INTERNET PLUS”. We can find the similar links in other eu countries and they are coordinating the help and counseling in area of safe internet communication and the new technologies.

European partners of the project www.zodpovedne.sk

EURÓPSKI PARTNERI PROJEKTU

🇧🇪	http://saferinternet.be/
🇨🇿	http://www.saferinternet.cz/
🇩🇰	http://www.medieraadet.dk/
🇫🇮	http://tietoturvakoulu.fi/
🇮🇪	http://www.webwise.ie/
🇮🇸	http://www.saft.is/
🇮🇹	http://www.easy4.it/
🇨🇾	http://www.cyberethics.info/
🇱🇻	http://netsafe.lv/
🇱🇹	http://www.draugiskasinternetas.lt/
🇱🇺	http://lusi.lu/
🇲🇹	http://appogg.gov.mt/
🇳🇱	http://digibewust.nl/
🇳🇴	http://www.saftonline.no/
🇩🇪	http://www.klicksafe.de/
🇵🇱	http://saferinternet.pl/
🇵🇹	http://www.internetsegura.pt/

【APEC Children Protection Project Questionnaire】

SPAIN

Nota: The questionnaire has been responded by Ministry of Industry, Tourism and Commerce in an informal way.

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

A set of main issues:

- Child pornography
- Incitement to Racial Hatred
- Anorexia and bulimia defense and support
- Safer use of mobile phones
- Terrorism support and defense
- Bullying
- Drugs trafficking
- Videogames

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

- Content filtering tools are common technologies for parents and schools. Main ISPs and software vendors provide general products and services for this purpose.
- The mobile telecom sector has also a self-regulation initiative that provides procedures to manage harmful content and to protect children. (see question 2.3)

(2) Does your economy have relevant laws and regulation? (If there are laws and regulation, please describe the overview.)

The Law 32/2002 of Information Society Services and Electronic Commerce introduces some obligations for ISP in relation to children protection and harmful and illegal content.

In general, ISPs are obliged to collaborate with Law Enforcement Bodies and must block the access or retire illegal content.

In 2008, a modification of the Law 32/2002 (article 12 bis) introduced new provisions for ISP and ESP. These provisions oblige ISP and ESP to inform users about technical means and security threats with the aim to allow protecting themselves against information security incidents. In addition, ISPs are also obliged to inform customers about available filtering tools and access management software with the purpose to avoid the access to harmful or illegal content and services in Internet for children and young people. ISPs are also obliged to inform customers about their responsibility when using Internet for illegal purposes.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

In general, there is a successful collaboration between ISPs, Telecom Operators, Law Enforcement Bodies, Hotlines Agents, and other public and private stakeholders regarding the fight against harmful and illegal content for children.

Additionally, there is a self-regulation agreement for Spanish Mobile Operators on how to protect minors using mobile phones. This agreement is based on the general framework promoted by the European Commision.
(see http://www.gsmworld.com/gsmeurope/documents/eu_codes/spain_coc_0308.pdf)

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

Some of the public policies regarding the promotion of a safer use of Internet for children are included in the National Strategy for the development of the Information Society in Spain. The main policy framework is the National "Plan Avanza2", in particular, the strategic line concerning minors. This line funds awareness and inclusion initiatives for minors, parents and schools, but also provides financial aids for software and service providers to develop better and safer products and services for children.

See also
http://www.planavanza.es/LineasEstrategicas/AreasDeActuacion/CiudadaniaDigital/Infancia/
www.chaval.es

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

In Spain, notification regarding harmful and illegal content has to be preferably submitted to:

- National Hotline operated by the NGO called "Protegeles" (see www.protegeles.org) that is also integrated in the European Network INHOPE funded by the European Commission through the Multiannual Program "Safer Internet".
- National Police Department in Home Office Ministry (see National Police Force and Guardia Civil at https://www.policia.es/bit/index.htm and http://www.guardiacivil.org/seguridad)

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

International Cooperation is performed by:

- the National Hotline "Protegeles" (see www.protegeles.org) by means of the European Network INHOPE for hotlines and the European Network of Awareness Nodes (INSAFE), both in the framework of the European Commission Multiannual Program "Safer Internet".
- National Police Departments through their particular international crossborder mechanisms in place.
- Other Public Agents through multilateral crossborder cooperation instruments like WPISP or ENISA.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

The major Swedish Internet Service Providers started a voluntary filtering project for blocking child abuse images and movies in 2006. The Swedish Police provides information on illegal websites to the industry.

There are also voluntary blocking projects for financial transactions related to purchasing child abuse content. The Swedish Financial Sector will establish a Financial Coalition against these phenomena.

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

Statutory law on responsibility for providers of Bulletin Board Systems, as well as other forms of services for electronic communication of messages, to supervise communication and to remove illegal content such as child pornographic images and unlawful depiction of violence.
A new legislation for the prevention of grooming activities will be presented to the Swedish parliament in early 2009.

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to

receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?
If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

Se answer above (1).

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA : Content Evaluation and Monitoring Association), (IROI : Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on "Action plan for encouraging dissemination of filtering service"

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

Se answer above (1).

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

Sweden cooperates with Interpol as well as Europol. Sweden also takes part in the Cospol Internet Related Child Abuse Material Project – “Cospol Circamp”.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.

【APEC Children Protection Project Questionnaire】

1. Current experiences regarding information considered harmful to children within economies (What kinds of issues is each economy concerned with?)

1) In Switzerland, an increasing number of interventions in the Swiss Parliament concern the easy and unprotected access by children to harmful content on Internet (on pornographic and violent Internet sites), possible even on their mobile phones, as well as the risks for children of being victims on Internet-Chatrooms (paedophilia, cyberbullying etc.).
2) No statistics or studies are however available on this issue.

(Example: Current Status of Japan)

(1) Increasing Online Dating Site

"The Online Dating Sites regulation Law" is planned to enter into force in December, 2008. Social networking service sites have sometimes been used as online dating services.

(2) Increasing of hydrogen sulfide suicide

The problem is that method of the preparation of hydrogen sulfide is introduced on website. Industry groups have been developing model provisions to prohibit writing method of the preparation of hydrogen sulfide on contractual policy.

(3) Rise in posting messages about claim of responsibility and bomb threats in the wake of the Akihabara Massacre

Composed of industry groups, liaison meeting for illegal information has been studying how to manage a claim of responsibility,

2. Current methods to manage access to information considered harmful to children

(1) Please describe status of technology development in your economy. (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)

1) *Filtering database:* In Switzerland, telecommunication service providers such as Swisscom and Sunrise offer to their clients a filtering database in order to give parents the opportunity to limit to a certain extent the access of their children to harmful content.
2) *Bar access to certain services:* Telecommunication service providers shall bar access to value-added services with erotic or pornographic content (0906 numbers; see also answer below).

(Example: Current Status of Japan)

In Japan, filtering software companies provide filtering database. (For example, NetSTAR Inc. divides 78 million sites into 73 categories.) Based on the blacklist approach, each mobile phone company limits access to the 34 categories of them.

NICT (National Institute of Information and Communications Technology) has implemented technical development to assess information credibility. In the wake of the Akihabara Massacre, MIC has requested next fiscal budget in order to develop technology that enables semantic analysis of messages about a pre-announced murder. (Corporate subsidy: 250 million yen) And , METI opened the elemental technology to analyze meaning of contexts to the relative entities, in order to promote their voluntary effort.

Each mobile phone company has been developing and selling cell phones limited the functions to call and GPS.

(2) Does your economy have relevant laws and regulation?
(If there are laws and regulation, please describe the overview.)

1) The Swiss legislation on Telecommunications (Ordinance of 9 March 2007 on Telecommunications Services, Art. 41) stipulates that, for the protection of minors, the telecommunications service providers shall bar access to the following services to customers or users under 16 years of age provided their age is known to the provider: a. value-added services with erotic or pornographic content (0906 numbers); b. SMS and MMS services with erotic or pornographic content provided via short numbers; c. value-added services with erotic or pornographic content provided in accordance with Article 35 paragraph 2. (See the website of the Swiss Federal Office of Communications OFCOM:
http://www.bakom.admin.ch/org/grundlagen/00955/00957/index.html?lang=en

2) The Swiss legislation prohibits images that glorify violence (Art. 135 and 197 StGB). Its enforcement is in the competence of the cantons.

3) Criminal responsibility of internet service providers (ISPs): On 27 February 2008 the Federal Council came to the conclusion that the current general regulation in relation to the criminal responsibility of internet providers is sufficient to effectively combat network criminality. A new, explicit regulation would not improve the effectiveness of law enforcement but would only serve the interests of representatives of the provider sector by freeing them of a large part of their responsibility in criminal matters.

(Example: Current Status of Japan)

In Japan, following matters are stipulated by “The Law on environment of development for children’s internet usage”;

1. Obliging operators to supply filtering service to internet mobile phone users, 18 years old or younger.
2. Obliging operators to take measures to facilitate usage of filtering service as of sale regarding internet-enabled equipment.
3. Imposing effort duty on operators to set up the call center in order for server managers to receive the harmful information report from users.

(3) Contents of voluntary efforts, such as self-regulation?
(Does your economy have any self-regulation?

If there is some self-regulation, please describe the overview.
(Example: participating parties, content, target contents, establish age restriction, status of the implementation of content rating, relation with laws and regulations, etc.))

1) The members of the Swiss Telecommunication Association ASUT (Swisscom, Sunrise, Orange, Cablecom) elaborated in June 2008 a Convention on Child Protection as self-regulation instrument to foster the responsibility of the telecommunication services providers in combatting cybercrime.
Link to ASUT: http://www.asut.ch

2) The Swiss Interactive Entertainment Association (SIEA), an association of developers and publishers of video and computer games, has taken the lead in the application of the PEGI ONLINE SAFETY CODE, the Code of Conduct for the European Interactive Software Industry, in Switzerland.

3) The Swiss Coordination Unit for Cybercrime Control (CYCOS) is a competence center available to the public, the authorities and internet service providers for any legal, technical and crime related questions in the field of cybercrime. It is the central office where persons can report suspect Internet subject matter. After an initial examination of the report and securing the data, the report is forwarded to the respective national or foreign law enforcement.
Link CYCOS: http://www.kobik.ch/

(Example: Current Status of Japan)

In Japan, there is the guideline provided by relevant industry groups.

From now, the development of safer internet council will formulate milder and expanded self-regulation to be able to declare, not only for internet-related companies, but also for internet-using companies.

Implementing the study to develop the classification, rating criteria, and health certification etc. at third-party organizations (EMA：Content Evaluation and Monitoring Association), (IROI：Internet-Rating Observation Institute), (Rating and Filtering liaison council).

Promoting the improvement of filtering service availability based on “Action plan for encouraging dissemination of filtering service”

(4) Does your economy have policies to improve literacy or raise awareness regarding these issues?　What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.

1) Various associations or organisations offer on their websites (www.pro-juventute.ch ; www.Elternet.ch ; www.security4kids.ch ; www.Kinderonline.ch) specific information for adults or children on how to protect themselves against harmful content.Some, as Pro Juventute, organise also workshops on this issue: http://www.pro-juventute.ch/pro-juventute-Handyprofis.4921.0.html

2) The Swiss Agency for Crime Prevention (SKP PSC) has the mission to develop prevention campaigns in different areas of life. Since 2005, it is running two campaigns against paedophilic crime, and offers specific information on its website for adults (www.stopp-kinderpornografie.ch) and for children with a self-test (www.safersurfing.ch). Link to SKP: http://www.skppsc.ch/1/en

3) CYCOS (see above) orgnises awareness campaigns on the risks run by children using the new technologies. It is also responsible for in-depth analysis of cybercrime.

(Example: Current Status of Japan)

Japan is developing various public and private approaches to improve literacy, such as the e-Net Caravan and Cyber Security College.

In Japan, the current curriculum guidelines at middle school contain information moral education in the field of technology of domestic science, while information-related subjects in high school have the same moral education, which are prerequisite. From 2009, new school curriculum guideline at elementary and middle schools, carried out advanced implementation of some of it, will promote information moral education with new provision of “learning information moral” based on guidance of each subject.

(5) Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, interministerial cooperation, cooperation among businesses, etc.)

1) *Public Private Partnership – Schools on the Net (PPP-SiN):* cooperation program which ran from 2002 to 2007, supported by the Confederation, the cantons and large corporations (Swisscom, Apple, Cisco, Dell, IBM, Microsoft and Sun). Its objective was to integrate information and communication technologies in schools and the education sector, by contributing infrastructure and services to Swiss schools (special terms for hardware/software and internet access) and by training teaching staff in this area. There have been positive results: the average number of learners per computer was reduced from 12.8 (2001) to 8.4 (2007). With reference to the 5,300 or so schools (school buildings) in Switzerland, the proportion of buildings connected to the internet was increased from 65.8% (2001) to 95.4% (2007).

The Confederation made a financial contribution, on the basis of the federal law (of limited duration) concerning the promotion of ICT in schools, to cantonal ICT projects in the areas of continuing education, advice and support for teachers in the use of ICT in education. It supported 33 management training courses, in which 1730 senior teachers were trained. Between 8000 and 9000 teachers also attended training as users supported by the Confederation; this means that PPP-SiN directly or indirectly reached a total of about 20% of all Swiss teachers.

The successful cooperation between the public and private sectors will continue although the program has ended. Schools will continue to benefit from special terms for hardware and software, and for internet access.

2) *Elaboration of a concept on public awareness rising*: In December 2008, the Swiss Government mandated an interdepartmental coordinating group in the Federal Administration to elaborate until the end of 2009 a concept on how to rise awareness of the people concerning the risks and benefits of the use of Internet.

(Example: Current Status of Japan)

In Japan, while dividing notifications submitted in the Internet Hotline Center (http://www.internethotline.jp/index-en.html) based on a guideline, website managers or ISPs are requested to delete those information concerning harmful information

(6) Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

The Swiss Government has signed the Cybercrime Convention of the Council of Europe and is proceeding to its ratification.

(Example: Current Status of Japan)

The Internet Hotline Center in Japan has joined in INHOPE, which is the global hotline center, and has implemented mutual notification and information exchange.