Guidelines for Policy Makers on Child Online Protection

www.itu.int/cop

Legal notice

This document may be updated from time to time.

Third-party sources are quoted as appropriate. The International Telecommunication Union (ITU) is not responsible for the content of external sources including external websites referenced in this publication.

Neither ITU nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Disclaimer

Mention of and references to specific countries, companies, products, initiatives or guidelines do not in any way imply that they are endorsed or recommended by ITU, the authors, or any other organization that the authors are affiliated with, in preference to others of a similar nature that are not mentioned.

Requests to reproduce extracts of this publication may be submitted to: jur@itu.int

ACKNOWLEDGEMENTS

These Guidelines have been prepared by the International Telecommunication Union (ITU) and a team of contributing authors from leading institutions active in the information and communications technologies (ICT) sector and in child online safety issues. These Guidelines would not have been possible without the time, enthusiasm and dedication of its contributing authors.

ITU is grateful to all of the following authors, who have contributed their valuable time and insights: (listed in alphabetical order)

- Cristina Bueti and Sandra Pandi (ITU)
- John Carr (Children's Charities' Coalition on Internet Safety)
- Raoul Chiesa and Francesca Bosco (United Nations Interregional Crime and Justice Research Institute)
- Catherine Cummings and Jessica Sarra (International Centre for Missing & Exploited Children)
- Johan Martens (Child Helpline International)
- Michael Moran (Interpol)

The authors wish to thank Kristin Kvigne (Interpol) for her detailed review and comments.

ITU wishes to acknowledge Salma Abbasi from eWWG for her valuable involvement in the Child Online Protection (COP) Initiative.

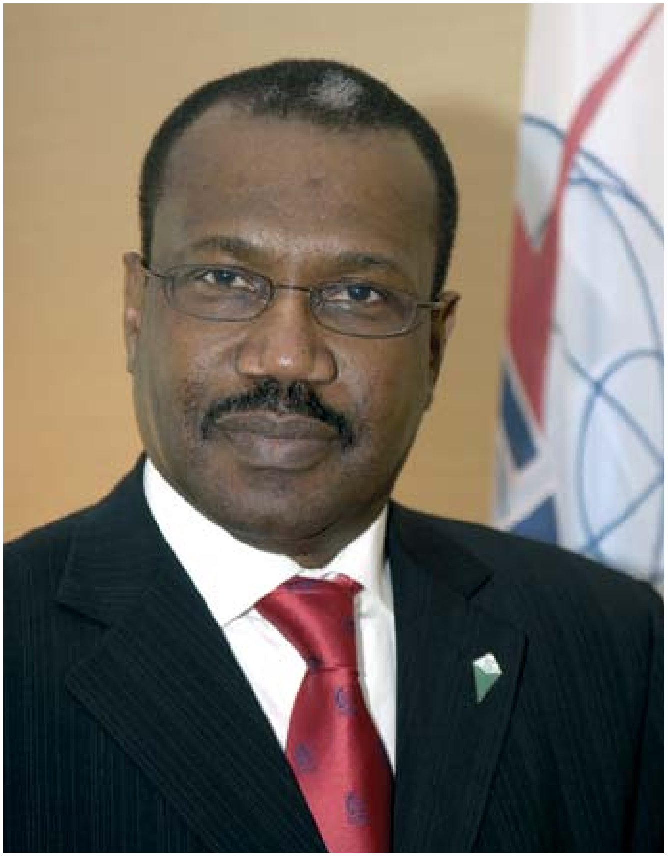
Additional information and materials relating to these Draft Guidelines can be found at: http://www.itu.int/cop/ and will be updated on a regular basis.

If you have any comments, or if you would like to provide any additional information, please contact Ms. Cristina Bueti at cop@itu.int

Table of Contents

> *“Protecting children online is a global issue, so a global response is needed”*

Foreword



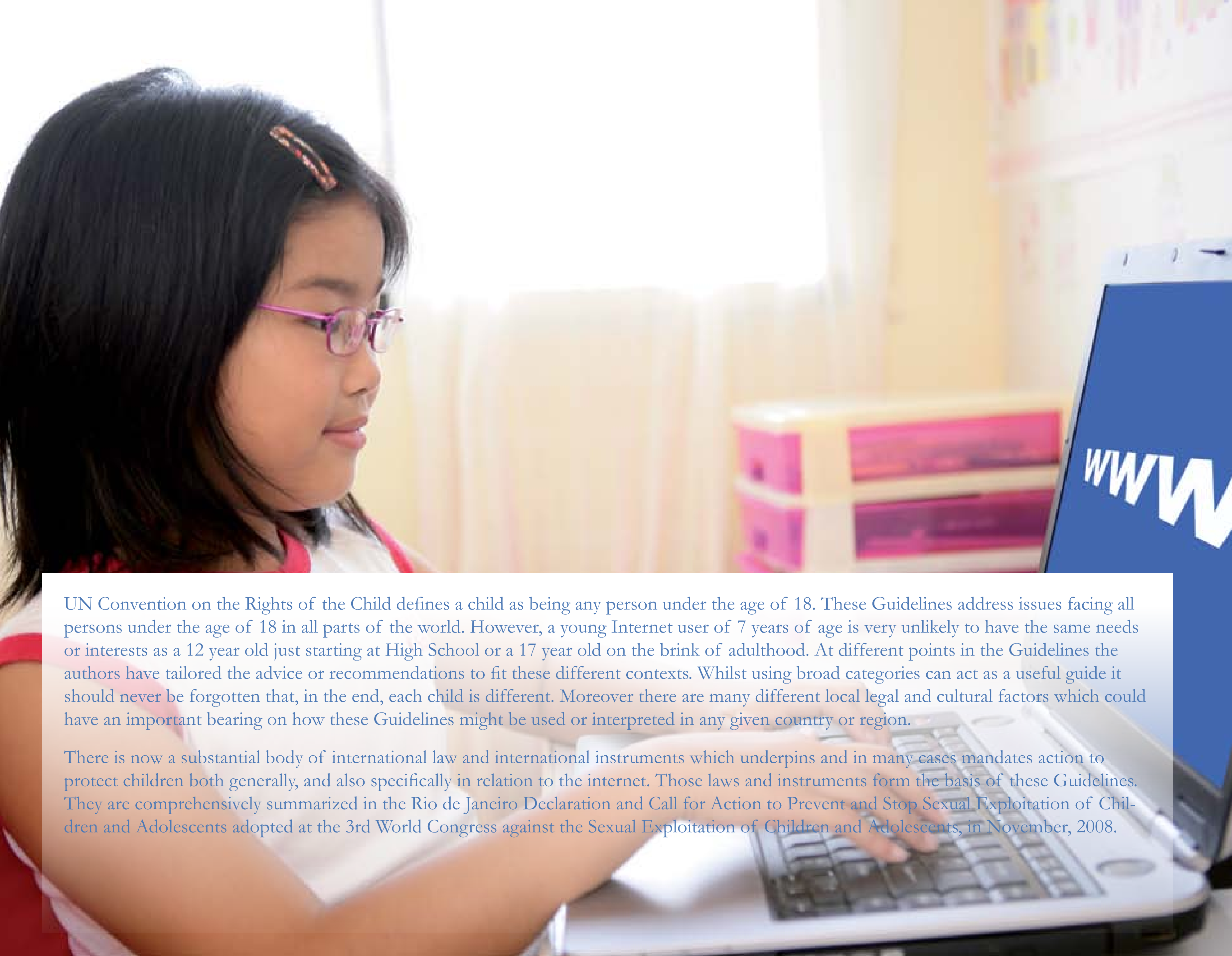
I welcome this opportunity to share with you these guidelines which have been developed with the invaluable help of multiple stakeholders.

Child Online Protection – in the era of the massively-available broadband Internet – is a critical issue that urgently requires a global, coordinated response. While local and even national initiatives certainly have their place, the Internet knows no boundaries, and an international cooperation will be the key to our success in winning the battles ahead.

Policy makers are key to winning the fight against cybercrime and cyberthreats, and I am personally grateful for your support.

Dr Hamadoun I. Touré

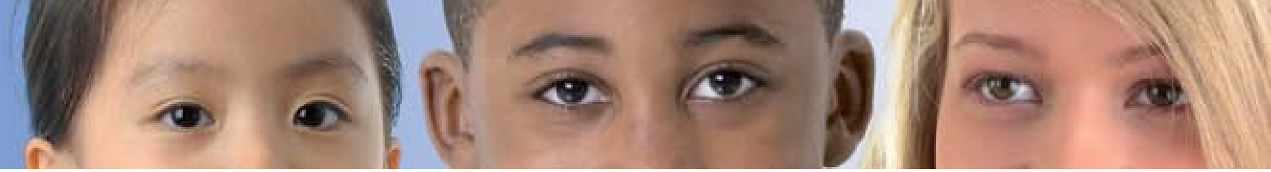
Secretary-General of the International Telecommunication Union (ITU)



UN Convention on the Rights of the Child defines a child as being any person under the age of 18. These Guidelines address issues facing all persons under the age of 18 in all parts of the world. However, a young Internet user of 7 years of age is very unlikely to have the same needs or interests as a 12 year old just starting at High School or a 17 year old on the brink of adulthood. At different points in the Guidelines the authors have tailored the advice or recommendations to fit these different contexts. Whilst using broad categories can act as a useful guide it should never be forgotten that, in the end, each child is different. Moreover there are many different local legal and cultural factors which could have an important bearing on how these Guidelines might be used or interpreted in any given country or region.

There is now a substantial body of international law and international instruments which underpins and in many cases mandates action to protect children both generally, and also specifically in relation to the internet. Those laws and instruments form the basis of these Guidelines. They are comprehensively summarized in the Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents adopted at the 3rd World Congress against the Sexual Exploitation of Children and Adolescents, in November, 2008.

1



Executive Summary

A decade ago, approximately 182 million people accessed the Internet globally — and almost all of them lived in the developed world. Remarkably, by early 2009, there were over 1.5 billion Internet users worldwide, with over 400 million of those having access to broadband. Today, while not ubiquitous, Internet users are truly worldwide with over 600 million users in Asia, 130 million in Latin America and the Caribbean, and 50 million in Africa[1]. The Internet continues to be a dynamic and incredible resource with almost unlimited capabilities to address societal problems from improved access to healthcare to remote learning opportunities to e-government to innovative and higher paying jobs. However, the growing global issues surrounding online cybersecurity require a global response, especially when it comes to the protection of our youngest and most vulnerable digital citizens: our children.

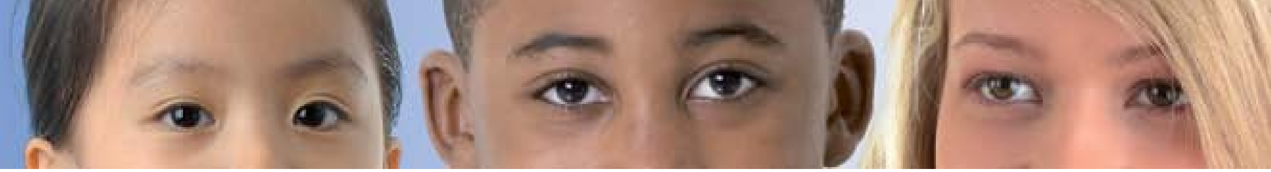
According to recent surveys, over 60 per cent of children and young people talk in chat rooms on a daily basis. Three out of four children online are willing to share personal information about themselves and their family in exchange for goods and services and as many as one in five children could be targeted by a predator each year.

These Guidelines have been prepared in the context of the Child Online Protection (COP)[2] Initiative in order to establish the foundations for a safe and secure cyberworld for future generations. They are meant to act as a blueprint which can be adapted and used in a way which is consistent with national or local customs and laws. Moreover, it will be appreciated that these guidelines address issues which might affect all children and young people under the age of 18 but each age group will have different needs.

The Guidelines have been developed by ITU in a very collaborative way involving a team of contributing authors from leading institutions active in the ICT sector and in child online safety

[1] World Telecommunication/ICT Indicators Database 2008, 12th Edition

[2] www.itu.int/cop



issues, namely, Children's Charities' Coalition on Internet Safety (CHIS), Child Helpline International (CHI), International Centre for Missing & Exploited Children (ICMEC), Interpol and United Nations Interregional Crime and Justice Research Institute (UNICRI). Invaluable contributions were also received from individual national governments and high- tech companies who share a common objective of making the Internet a better and safer place for children and young people.

It is hoped that these Guidelines will not only lead to the building of a more inclusive information society, but also enable ITU Member States to meet their obligations towards protecting and realizing the rights of children as laid out in the UN Convention on the Rights of the Child[3], adopted by UN General Assembly resolution 44/25 of 20 November 1989 and the World Summit on Information Society[4] (WSIS) Outcomes Document[5].

At WSIS, ITU was entrusted by leaders of the international community with Action Line C5: "building confidence and security in the use of ICTs". The WSIS outcomes also specifically recognized the needs of children and young people and their protection in cyberspace. The Tunis Commitment recognized "the role of ICTs in the protection of children and in enhancing the development of children" as well as the need to "strengthen action to protect children from abuse and defend their rights in the context of ICTs".

Through issuing these Guidelines, the COP Initiative calls upon all stakeholders to promote the adoption of policies and strategies that will protect children in cyberspace and promote their safer access to all the extraordinary opportunities online resources can provide.

[3] www.unicef.org/crc/

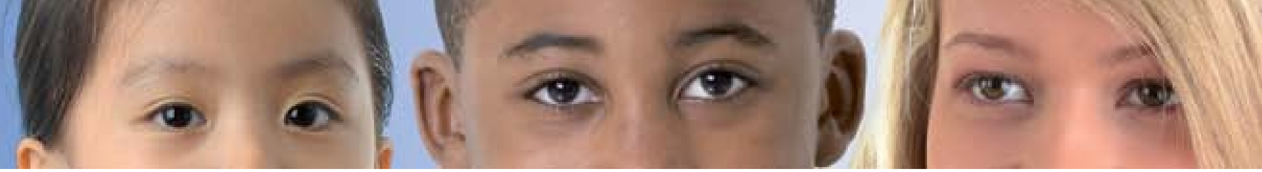
[4] WSIS was held in two phases: in Geneva (10-12 December 2003) and in Tunis (16-18 November 2005). WSIS concluded with a bold commitment "to build a people-centred, inclusive and development oriented information society, where everyone can create, access, utilize and share information and knowledge." See www.itu.int/wsis.

[5] www.itu.int/wsis

Guidelines for Policy Makers

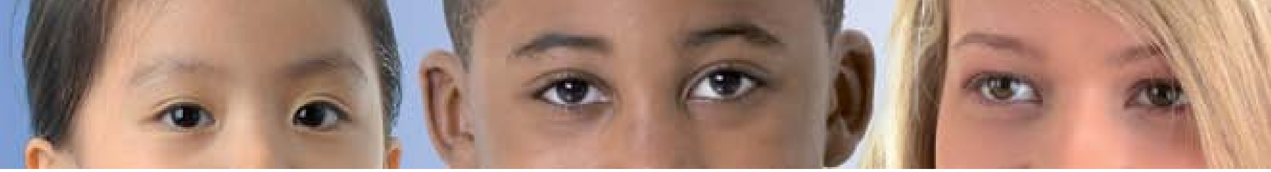
In order to formulate a national strategy focusing on online child safety, policy makers need to consider a range of strategies. Below are a number of key areas for consideration. Further suggestions will also be found in Appendix 4.

	#	Key Areas for Consideration
Legal Framework	1.	Review the existing legal framework to determine that all necessary legal powers exist to enable law enforcement and other relevant agencies to protect persons under the age of 18 online on all Internet-enabled platforms.
	2.	Establish, *mutatis mutandis*, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for legal minors are also adequate.
Law Enforcement Resources and Reporting Mechanisms	3.	Ensure that a mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the Internet, for example, a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible.



	#	Key Areas for Consideration
National Focus	4.	Draw together all of the relevant stakeholders with an interest in online child safety, in particular: • Government agencies • Law enforcement • Social services organizations • Internet Service Providers (ISPs) and other Electronic Service Providers (ESPs) • Mobile phone network providers • Other relevant hi-tech companies • Teacher organizations • Parent organizations • Children and young people • Child protection and other relevant NGOs • Academic and research community • Owners of Internet cafés and other public access providers e.g. libraries, telecentres, PC Bangs[6] and online gaming centres etc.
	5.	Consider the advantages that a self or co-regulatory policy development model might present, as expressed by the formulation and publication of codes of good practice, both in terms of helping to engage and sustain the involvement of all relevant stakeholders and in terms of enhancing the speed with which appropriate responses to technological change can be formulated and put into effect.
Education and Awareness Resources	6.	Draw on the knowledge and experience of all stakeholders and develop Internet safety messages and materials which reflect local cultural norms and laws and ensure that these are efficiently distributed and appropriately presented to all key target audiences. Consider enlisting the aid of the mass media in promoting awareness messages. Develop materials which emphasise the positive and empowering aspects of the Internet for children and young people and avoid fear-based messaging. Promote positive and responsible forms of online behaviour.
	7.	Consider the role that technical tools such as filtering programmes and child safety software can play in supporting and supplementing education and awareness initiatives.
	8.	Encourage users to take responsibility for their computers by encouraging regular servicing which includes updates of the operating system plus the installation and upgrading of a firewall and antivirus application.

[6] A "PC Bang" is term commonly used in South Korea and in some other countries to describe a large room where a LAN facilitates large scale game playing, either online or between players in the room.



1. Background

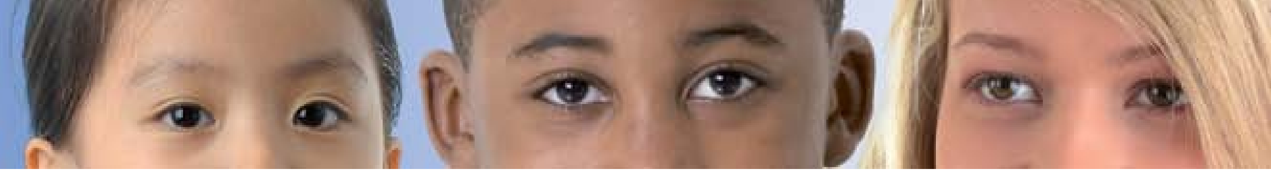
The technology which today we refer to as "the Internet" can trace its origins back to the 1950s and beyond. However, it was the development of the World Wide Web in the early 1990s that sparked the exponential growth of the Internet which led to it becoming an extremely valuable aspect of our lives, both economically and socially, and has led it to become a seemingly permanent feature of modern day life.

At the dawn of the Internet revolution, users were amazed at the possibility of contacting people and accessing information across oceans and time zones through a few clicks of their mouse. In order to do so, however, typically they had to be in a fixed location in front of an often large or bulky computer device, typically a PC. Today people can connect to the global network using a mobile phone, a laptop computer or other portable devices, often with video capabilities and very high-speed access. Many game consoles are also Internet enabled and this has fostered a huge growth in on-line game playing among children and young people.

It took around 20 years to reach the first billion mobile phone users, yet the second billion signed up in just the last few years. In contrast, it took 125 years to reach the first billion fixed-line telephone users.

The evolution from second to third generation mobile phone networks is arguably just as important as the initial jump from analogue to digital. It began more than a decade ago and is progressing at a rapid speed. The

“Draw together all of the relevant stakeholders with an interest in online child safety”



newly emerging fourth-generation technologies maintain the emphasis on mobile access but at even higher speeds. Broadband networks and media convergence are generating new avenues for distributing digital entertainment.

User devices are now multi-functional and increasingly personalized. In the near future, advances in connected computing will make it possible for hundreds of millions of objects to have the ability to communicate with each other over the Internet, opening up countless household and business applications.

In both fixed-line and cellular markets, the transition to higher capacity networks is accompanied by a shift to IP-based networks. As a consequence, voice over Internet Protocol (VoIP) usage is on the rise (for example through services like Skype or Vonage) but so too is the possibility of watching moving images over IP networks. New technologies such as digital video broadcasting and digital multimedia broadcasting will allow viewers to watch streamed content on mobile devices anytime, anywhere.

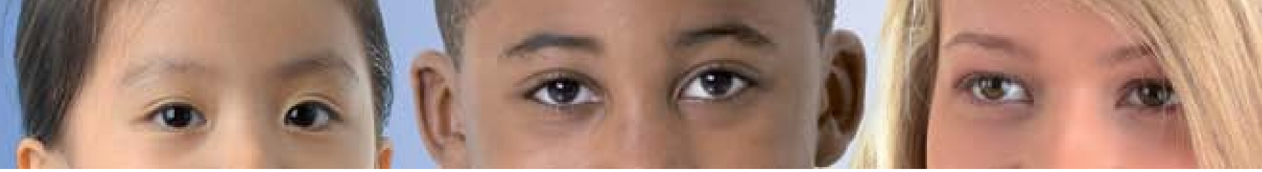
The world of entertainment appears to be entering a whole new era. At the same time, digital technology is having a significant impact on the nature of social interactions. Mobile phones have already changed the way people communicate, arrange meetings and multitask.

The expansion of electronic and digital infrastructure has given many millions of people the potential to learn, publish and communicate on an unprecedented scale. Children and young people have very often been the "pioneers " of adopting and adapting to the new possibilities presented by these new and emerging technologies. It has been tremendously empowering for many young people and is opening up huge new possibilities in the fields of education and personalized learning.

The rapidly declining real cost of the requisite information and communication technologies, combined with vast changes and enhancements to the available infrastructure, have allowed many children and young people to take advantage of technology to do and achieve things unknown to earlier generations.

While the development of the Internet differs by country and region, Internet access is available almost anywhere. In developing countries, many Internet and phone connections are using wireless technology rather than fixed-line access; data storage and transfer are becoming decentralised and seemingly limitless. The "networked society" that has been visualised for some decades is becoming a reality.

With increasing access, the Internet is becoming truly global, offering its benefits to more and more people, including children and young people. The culture and economy of a country will shape how the Internet develops and this will have an impact on the risks that children will face as well as how those risks are addressed by the different local stakeholders. There can be no simple or single blueprint to tackle such a complex issue.



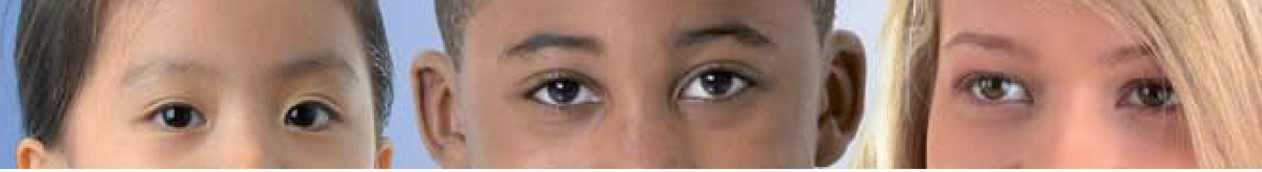
2. Children's and Young People's Use of the Internet

The Internet has now been in existence for several decades, however, the nature of it has changed dramatically since its inception. In the beginning it was mainly a tool to exchange information and data between governmental agencies and academic institutions. In the 1980s, the Internet was opened to the general public. With the advent of the World Wide Web in the 1990s, the Internet started to grow at an astonishing rate. In recent years another revolution has taken place: the emergence of Web 2.0. The web is becoming more interactive and a much larger cross section of society has a presence on the Internet. More people are connected now, with children and young people very often leading the pack as early users.

While the development of the web opened up the Internet to the general public, for some time it remained a network that was owned and populated mainly by governments, academic institutions and commercial corporations. Individuals largely went online to access information that was provided to them by these large players. This early period of the web was marked by several characteristics:

- Low levels of connectivity
- Mainly low bandwidth
- Low capacity for data storage
- One way communication and access

form
one
little
traditional
examples
initially
term
example
crafts
store
government
public's
capabilities
world
network
ipv6
interoperable
servers
corporation
wide
global
using
document
influence
lagging
may
graphics
interactive
infrastructure
systems
generally
local
databases
blogs
find
standardized
connection
physical
data
access
brand
discussions
series
interconnection
communications
content
groups
terms
synonymous
strict
widely
management
implementations
files
lan
internet
applied
food
communities
encyclopedias
growth
maintaining
areas
standardization
controlling
progressed
logs



Over time the Internet continued to evolve with four developments being of special importance:

- Increase in affordable bandwidth
- Increase in comparatively inexpensive storage capacity
- Lower access costs
- Development of the mobile Internet

These new developments helped to establish a new type of Internet; instead of simply connecting individuals to firms, organizations and governments, the Internet also began to enable individuals to connect to each other and for them to become online publishers in their own right. This new Internet, often referred to as Web 2.0, has the following characteristics:

- High levels of connectivity
- High bandwidth
- High levels of storage capacity
- Personalized and interactive contact (user generated content)

New tools have been developed that provide users with various means to socialize and to connect with each other. These tools include: instant messaging, chat and message boards, photo and video hosting services, and peer-to-peer file exchange programmes (P2P). Taken together these technologies, and others, have given rise to the phenomenal growth in social networking sites which in a very short period of time have become enormously popular with children and young people.

Interactivity and User Generated Content

Children and young people, as well as adults, increasingly live out important parts of their lives with the assistance of these new technologies, and as a result, the nature of the risks they take have become inextricably entangled with wider aspects of their behaviors. It is now no longer possible to draw neat lines between so called “Internet issues”, and “real world” problems.

Social Networking Sites

The qualitatively new and very clever dimension that is the hallmark of social networking sites is the way they have brought several pre-existing Internet technologies together into a single place, added new features, and created very user friendly interfaces. These new interfaces mean it has become extremely easy to use the various features. Taken together this has triggered the rapid growth in the popularity of social networking sites which has caught many people by surprise, particularly parents.

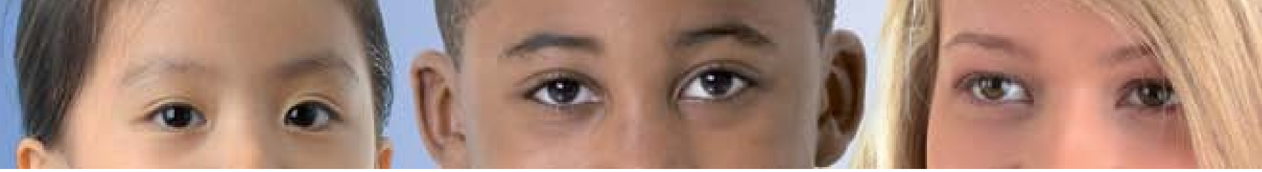
Social networking sites allow users to create an online profile in which they can display a range of personal information, such as age, gender, home town and interests. In particular the new interfaces developed by the social networking sites make it simple to personalize individual user web pages, for example by adding some of the users' favourite music, photographs and videos. Children and young people have become very creatively engaged with this process. User profiles on a social networking site have become extensions of the users and an important way for the users to make a statement about themselves to their friends and to the wider world.

Most importantly, social networking sites allow users to add friends with whom they can exchange messages. The audience that can view an individual's profile typically depends on how the person has utilized the site's privacy settings. Too often, particularly in the early days of social networking, children and young people appeared to be unaware that, unless they took specific steps to limit access, for example by setting their profile to "private" or "friends only", their full profiles would be open for anyone to view. This made them vulnerable to predators who might have masked their age in order to build a relationship with the child or young person. There have been cases reported where some children and young people have posted sexualized images of themselves, or have exchanged them via mobile phones, a phenomenon known as "sexting"[7], often without realizing that the image itself might be both harmful to them and illegal, but in addition it might be viewable by large numbers of people who could visit their site or profile. More generally social networking sites have highlighted the problem of how to manage user generated content, the characteristic feature of Web 2.0. Some sites have developed proactive moderation policies, where they search out inappropriate or illegal videos and images, whereas others will only look at an individual picture or video if it is drawn to their attention by a report from someone who finds it to be objectionable and wants it removed.

The popularity of individual social networking sites often follows language and regional factors. A few examples are: MySpace (particularly popular in Northern America), Facebook (most popular in North America, Europe and Oceania), Hi5 (most popular in Latin America), Orkut (Latin America), SkyBlog (Francophone countries), Live Journal (Russia and CIS), Friendster (Asia Pacific), Cyworld (Republic of Korea and PR of China), LinkedIn (Europe, US and India), Last.fm (Nordic and Baltic Countries and Central Europe).

[7] Sexting - the relatively new phenomenon where children and young people are putting themselves at risk by posting sexually provocative images of themselves online or sending them to friends using mobile technologies.

Source: Draft Guidelines for Parents, Guardians and Educators on Child Online Protection, ITU 2009



According to Danah Boyd[8], online expressions, personal profiles or other types of postings have four fundamental characteristics that can lead to additional risks for children and young people:

1. Persistence: Networked communications are recorded and this extends the period of life of any communication.

2. Searchability: Because online communications are recorded and identity is established through text, search and discovery tools help people find other people.

3. Replicability: Networked communications can be copied from one place to another verbatim in such a way that there is no possibility to distinguish the "original" from the "copy."

4. Invisible audiences: For practical purposes it is impossible to determine who might run across profiles or other online communications. This is further complicated by the other three characteristics mentioned above, since profiles may be viewed or accessed at a different time and place from when and where they were originally created.

Instant Messaging and Chat

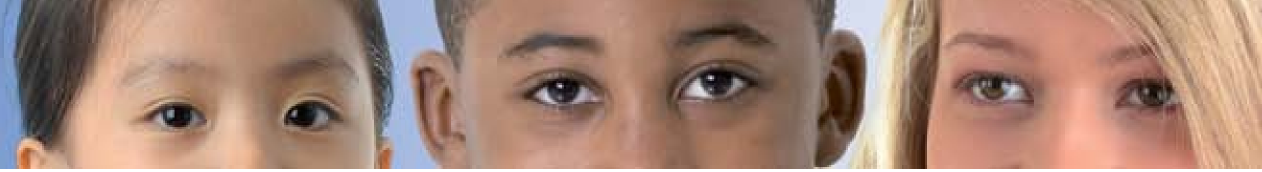
Instant messaging (IM) tools allow people to connect to others online directly and to have conversations through written messages (and increasingly through video conferencing). People can add the names of individuals they know to their contact list and can see if they are available (online) to talk with. These conversations, or "chats", can be held with one person (bilaterally) or with a group of people (multilaterally). With most programmes the content of the conversations can be saved if wanted or needed. Well known IM and chat programmes include MSN Chat, Yahoo! Messenger, Google Talk, and AOL Instant Messenger.

Peer-to-Peer File Exchange Programmes

Peer-to-peer file exchange programmes (also called P2P programmes) allow individuals to directly upload and download files from and to their own storage discs. Anyone using the same programme can search for files and download them from others that have these files available. These programmes facilitate the sharing of knowledge and information, but have also led to copyright infringement and the proliferation of malicious ware (malware) such as viruses and Trojans[9]. These networks are also used to distribute CAM. Well-known P2P programmes include Bittorrent, E-mule, E-donkey and Kazaa.

[8] Danah Boyd, Fellow at Harvard Law School's Berkman Center for Internet and Society.

[9] The Trojan horse, also known as **Trojan**, in the context of computing and software, describes a class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen and control the computer. See: http://en.wikipedia.org/wiki/Trojan_horse_(computing)



3. Child Abuse Material

A Definition

In many jurisdictions still photographs or videos of children being sexually exploited and abused are called either “child pornography” or “indecent images of children”. Today many practitioners prefer to use the term “child abuse material” or CAM because it is felt that this term more accurately conveys the real nature of the content. This is the term which is normally used in this document.

The Internet has completely transformed the scale and nature of the production and distribution of CAM.

The sexual revolution of the mid-1960s, marked by an openness to sexual expression and variation, heralded a burgeoning demand for pornography, with adult bookstores springing up in many European and American cities[10]. These shops and indeed a whole mail order style business stocked and supplied a massive amount of pornography of all kinds right across the severity spectrum. The demand for pornography was met with vigour by a number of key players all over the world. Like all vacuums it was filled quickly by entrepreneurs and a large supply network arose very quickly.

[10] O’Donnell and Milner, (2007), Child Pornography, Crime computers and society, Willan.

Some of the pornography being bought, sold and traded included images of children being sexually abused. Anti-CAM laws passed in 1977 in the United States soon spread to Europe and the production of CAM soon waned and was driven underground. By 1986, virtually all the traditional avenues for obtaining this kind of material had been firmly closed, raising the possibility of a thorough suppression of the CAM trade.[11]

Historically, the difficulties of finding CAM at this point meant that people who wanted to indulge in CAM had to take huge risks and a lot of expense in order to get access to material. All of this changed with the advent of the Internet. Dr. Alvin Cooper spoke about the "triple A engine" for cyber sexuality which can easily be transferred to the way the Internet revolutionised the possession and distribution of CAM:

- Accessibility (the Internet makes CAM available 24/7 all the year round);
- Affordability (most CAM is free and available for swap or simple download); and
- Anonymity (people genuinely believe that their communications on the Internet are private and hidden).

This encouraged them to seek out and deal in CAM as they felt there were no repercussions. The fact that it was free and available also encouraged the belief that it was harmless.

In 1997, Sir William Utting, a distinguished expert in child social services, described CAM as a "cottage industry"[12]. That was probably the last moment in history when such a claim could be made. Today it is a global industry. It seems that no country is immune.

It is very difficult to determine the precise size or shape of what is essentially a clandestine and often illegal enterprise. All kinds of estimates have been made at different points about of the number of web sites involved[13], the number of children being abused to create the images[14] and of the total monetary value of the market in the images. No one who is familiar with the terrain doubts that there are a substantial number of people involved in the viewing and distribution of CAM and that there has been evidence of the involvement of organized crime[15] in the commercial distribution of this material. Equally there can be no doubt that the number of illegal images now in circulation on the Internet runs into many millions, while the number of individual children depicted in those images runs into the tens of thousands[16]. And these are only the ones that have so far been discovered.

[11] Jenkins, P, Beyond Tolerance, 2001, New York University Press.

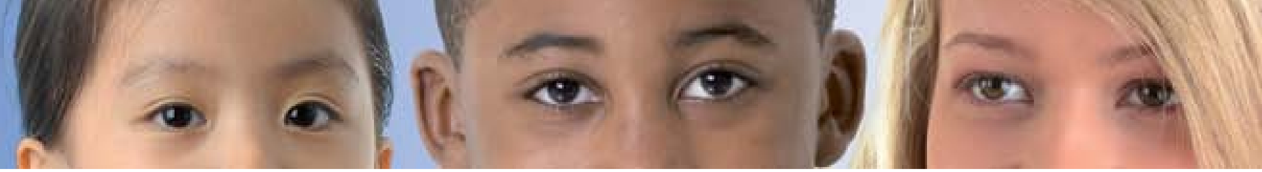
[12] UK, HMSO, 1997

[13] In its Annual Report for 2007 the IWF maintained that fewer than 3,000 English-language web sites accounted for the bulk of child abuse images available online. Three years earlier, the US based Computer Crime Research Center said the number was greater than 100,000

[14] Correspondence with Interpol. And see report by Telefono Arcobaleno. http://www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf

[15] See details of the "Reg Pay" case. http://www.usdoj.gov/criminal/ceos/Press%20Releases/ICE%20Reg-pay%20PR_080906.pdf

[16] Correspondence with Interpol, referred to above.Telefono Arcobaleno in their report speak of 36,000 children of whom "42% are under 7 years of age and 77% are under the age of 12." http://www.telefono-arcobaleno.org/pdf/tredicmoreport_ta.pdf



Originally one of the main ways of distributing CAM over the Internet was from within Usenet Newsgroups. That remains an important source but today several other Internet technologies are also being used. Of these perhaps the World Wide Web is the most important, because it is the most accessible and easiest to use. However, as some countries have made it very difficult to use the web to distribute CAM, other Internet technologies are also being used more and more frequently. Of these perhaps P2P or file sharing software is the most significant. According to Interpol, Peer2Peer is technically quite easy to police but the sheer volume of people involved makes it practically very difficult.

Every time an image of a child being abused appears on the Internet or is downloaded, in an important sense that child is being re-abused. Victims must live with the longevity and circulation of these images for the rest of their lives. The best proof of this is the reaction of the victims and their families when they learn the images have been put into circulation or uploaded to the Internet[17].

For that reason there is widespread agreement that as soon as a child abuse image or web site is discovered it is important to move as quickly as possible to remove the image or have the web site taken down or rendered inaccessible. In order to facilitate this process a system of national hotlines has been developed. Currently hotlines are operational in over 30 different countries and they are growing in number.[18] A major growth in hotlines is highly desirable as part of a renewed global campaign to end the traffic in CAM online.

Another reason for moving quickly to remove or render inaccessible any illegal images found on the Internet is because the longer they stay up the greater the possibility that a new person will find the image and perhaps download it. There is some evidence to suggest that people who get involved in downloading and collecting CAM are more likely to engage in contact offending or abusing children in the real world. *(From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children. Kim, C (2004).*

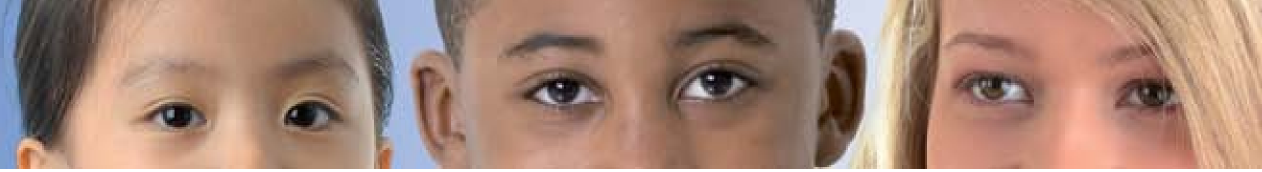
In the law enforcement sphere the importance of victim identification from the CAM posted on the Internet has gained ground.

Processes and systems are being put in place nationally which means that CAM seized during investigations or otherwise coming into the hands of investigators is being examined with a view to identifying the victim of the abuse and therefore the perpetrator. Materials which have not been seen before and cannot be marked as locally generated are floated into an international network of investigators and national CAM specialists. This network has evolved around the INTERPOL International Child Sexual Exploitation Database (ICSE) and is coordinated at the Trafficking in Human Beings section of INTERPOL along with the INTERPOL Specialist Group on Crimes against Children.

The aim of this Database is to capture in one place all of the CAM that exists on the Internet and that comes into the hands of law enforcement. This material is examined by the network of

[17] Child Molesters: a behavioral Analysis, Kenneth V. Lanning, 2001.

[18] See www.inhope.org



specialised officers worldwide and, where possible, is referred to the country of origin for an investigation into the identity of the child being victimized. Where this is not possible the material is filed in the Database with details as to where it was found, by whom and when.

Powerful retrieval tools indicate whether these images were seen before or not and, as is often the case, images found in one country can often hold clues which can help identify an abuse case in another country. Sometimes, the face of the abuser can be seen in the images, leading to apprehension.

INTERPOL and the COP Initiative encourage best practice in this area by encouraging the formation of a centralised, national resource which can manage all the material being seized inside its borders, creating a national hash set and contributing to the international efforts being made in this area.

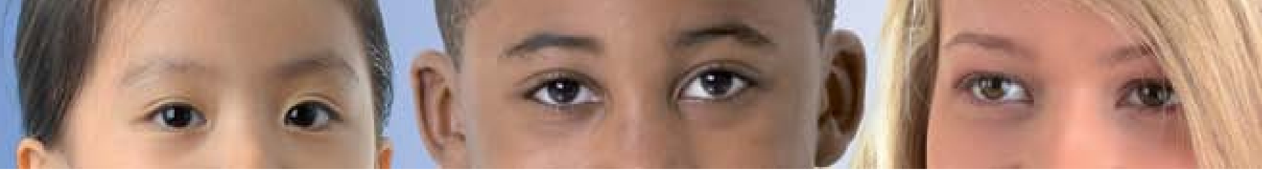
All this reduces effort for investigators, avoids duplication of efforts worldwide, and ultimately leads to the identification of victims and the apprehension of offenders.

Harmonisation of Laws

The adoption by all countries of appropriate legislation against the misuse of information and communication technologies (ICTs) for criminal or other purposes is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime, protect children online and facilitate international cooperation.

The development of adequate national legislation, the related cybercrime legal framework, and within this approach, harmonization at the international level is a key step towards the success of any national strategy for child online protection. This requires first and foremost the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and CAM. The fact that provisions exist in the criminal code that are applicable to similar acts committed in the real world does not mean that they can be applied to acts committed over the Internet as well. Therefore, a thorough analysis of current national laws is vital to identify any possible gaps. The next step would be to identify and define legislative language and reference material that can assist countries in the establishment of harmonized cybercrime laws and procedural rules. Such practical instruments can be used by countries for the elaboration of a cybersecurity legal framework and related laws. The ITU has been working with Member States and relevant stakeholders in this direction and is heavily contributing to the advance the global harmonization of cybercrime laws.

The International Centre for Missing & Exploited Children (ICMEC) released its report on “Child Pornography: Model Legislation & Global Review” in April 2006. The primary purpose of the report, which is now in its 5th Edition, was to gain an understanding of existing CAM legislation and to ascertain the importance of the issue with regard to national political agendas. The study focused on a number of key areas: legislation specific to CAM; laws that provide a definition of CAM; laws that criminalize possession, regardless of intent to distribute; laws that address computer facilitated crimes related to CAM; and reporting by ISPs.



A copy of ICMEC's detailed findings is provided in Appendix4. It is evident from the report that there are considerable and very important variations in the legislative approaches taken by different countries. The international community must find a way to bring greater coherence to the attack on this global problem.

Another goal of the ICMEC report on model legislation is to recommend areas where legislation is needed to address the various aspects of CAM and related crimes on a worldwide basis. As with other types of cybercrime, the possession, manufacture and distribution of CAM is often conducted without regard to international borders and therefore requires laws in each country that are comparable or legally equivalent — this is referred to as harmonization.

Criminals who sexually exploit children, whether it is through the use of computers and the Internet or by travel to other countries, will prefer to victimize children in countries lacking legislation or strict enforcement and in countries that exist outside the framework of international cooperation. Complying with international legal standards and adopting corresponding national laws and practices is a requirement in order to address child exploitation on an international level.

Many countries broadly address child exploitation as it relates to labour or other offences or they may ban pornography in general; however, these laws are not enough as they do not specifically address the criminal aspects of various forms of child sexual exploitation and child abuse images. In order to be truly effective, countries should be encouraged to adopt specific legislation to criminalize CAM and include offences specific to the use of technology and the Internet as it relates to CAM; otherwise criminals will take advantage of loopholes in the law.

There should also be provisions in the law for a greater commitment of resources in order to enforce these specific laws and for training for judicial, prosecutorial and law enforcement officials who will invariably be challenged to keep up with the use of technology by offenders.

Fundamental areas of concern and guidance for the adoption of legislation include:

- Defining a "child" in a precise and clear manner in accordance with the UN Convention of the Rights of the Child;
- Defining "child abuse material" (CAM) to include specific computer and Internet terminology;
- Creating criminal offences specific to: possession, manufacture and distribution of CAM, including pseudo images, deliberately downloading or viewing such images on the Internet;
- Creating criminal penalties for parents or guardians who agree to or who facilitate their child's participation in CAM;
- Creating penalties for those who make known to others where to find CAM;
- Making attempts at crimes related to CAM a criminal offence;
- Addressing criminal liability of children involved in CAM. Criminal liability must focus on the adult offender, not the child victim;

- Enhancing penalties for repeat offenders, organized crime members and other aggravated factors to be considered upon sentencing.

A basic definition of CAM should include the visual representation or depiction of a child engaged in a real or simulated sexual display or act, or pseudo images of the same; it should also take into account how technology such as computers, the Internet, cell phones, PDAs, game consoles, video cameras, and DVDs, are used to facilitate CAM, making it clear that CAM and everything connected with it is illegal, irrespective of the platform.

Forensic Computer Training for Law Enforcement

Apart from substantive criminal law provisions, law enforcement agencies need the necessary tools and instruments to investigate cybercrime. Such investigations themselves present a number of challenges. Perpetrators can act from nearly any location in the world and take measures to mask their identity. The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.

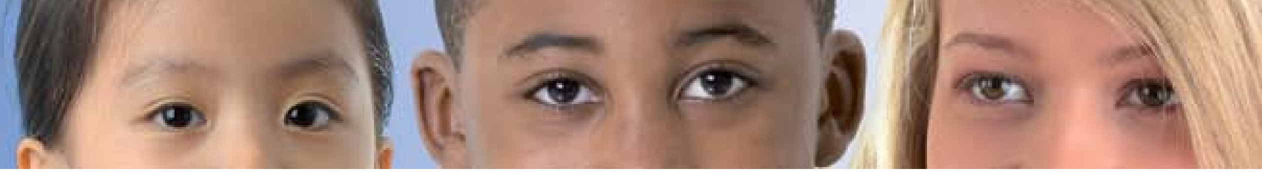
The Internet, computers, cell phones, PDAs and digital devices of all types have become indispensible tools for predators seeking to sexually exploit children. The technology on which these devices operate is increasingly complex and changes at a rapid rate. In order to capture and preserve important evidence left by offenders it is essential for law enforcement authorities to have the training and technical expertise to retrieve evidence consistent with domestic and international court requirements. Therefore, training must be made available to law enforcement, judicial and prosecutorial officials to help them understand how to conduct forensic analysis of computer hard drives and other devices. This training must be constantly updated to keep up with ever-changing technology and give them hands-on experience. There are many software suites which provide the tools to carry out read only examinations of seized media and training is often included in the purchase price of the suite. Unfortunately these solutions are often quite expensive and beyond the reach of developing countries. Training from within the law enforcement and private security industry may be available with proper funding.

Many companies in the private sector have the technology and the expertise to assist with this type of work so partnerships between the public and private sectors for training and technical support may be able to provide critical assistance.

International Cooperation and Data Sharing

It is very important to develop a high level of international cooperation and data sharing.

A fundamental role of ITU, following WSIS is to build confidence and security in the use of ICTs. Heads of states and government and other global leaders par-



ticipating in WSIS as well as ITU Member States entrusted ITU to take concrete steps towards curbing the threats and insecurities related to the information society.

WSIS considered that Action Line C5 encompasses a broad range of themes and stakeholders. As emphasized in paragraph 110 of the Tunis Agenda, the "*coordination of multi-stakeholder implementation activities would help to avoid duplication of activities. This should include, inter alia, information exchange, creation of knowledge, sharing of best practices, and assistance in developing multi-stakeholder and public/private partnership*".

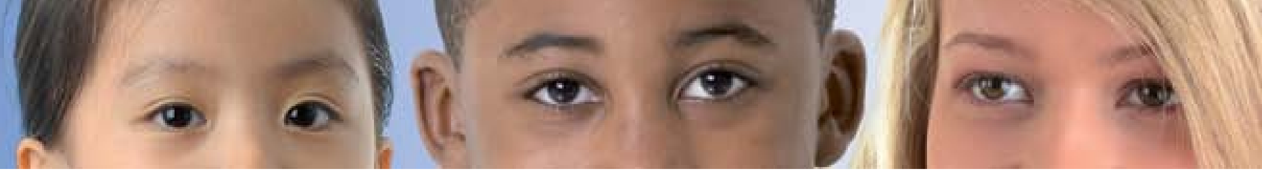
INTERPOL[19], through its network of 187 countries, specializes in facilitating the exchange of police-to-police information. This network allows the instant exchange of information between countries and by extension of the i24/7 system, directly to specialist units.

Where the exchange of information and evidence is in the judicial sphere, mutual cooperation on international criminal investigations is accomplished under the legal framework and provisions of bilateral mutual legal assistance treaties or multilateral conventions. These are not always suited to the fast moving world of the Internet.

In spite of treaty agreements, if there is not a corresponding law in the country where cooperation is requested, assistance may not be provided at all or it may be provided on a very restricted basis. The party providing the information may place conditions upon the use of the information and may require confidentiality.

A collaborative approach aimed at building consensus at the global level on those common elements that should be part of any legal framework for protecting the children in cyberspace is fundamental. Given the international nature of cybercrime and of child exploitation in particular, effective international law enforcement cooperation is imperative if we are to address the problem on a global scale.

[19] INTERPOL also coordinates the INTERPOL working party on crimes against children which meets once a year in a group session. There are five sub groups within the working party and members of this group meet virtually throughout the year in an effort to work on projects. The five sub-groups are: Internet facilitated crimes against children, Sex Offenders, Child Trafficking and Serious and violent crimes against children. The fifth sub-group is a victim identification subgroup which facilitates the international cooperation which is a daily fact around the International Child Sexual Exploitation database.



Reporting Requirements

Members of the public who come into contact with CAM should report it to local law enforcement and/or to a national hotline.[20] Additionally, there are three classes of individuals and organizations that should be particularly encouraged to report suspected CAM, either directly to a law enforcement agency or another designated organization, such as a hotline:

1. Individuals who in their professional capacity come into contact with children and owe a duty of care to the children, e.g. teachers, coaches, counsellors, healthcare providers and law enforcement officers.
2. Individuals who in their professional capacity do not necessarily come into contact with children but may be exposed to CAM in the course of their work, e.g. computer technicians, photo developers.
3. Organizations or corporations whose services are being used to proliferate CAM and who should exercise corporate citizenship responsibility, e.g. ISPs and other ESPs, credit card companies and banks.

While the inclusion of people in categories 1. and 2. are self-explanatory, reporting by ISPs, banks and credit card companies is critical in that their services are essential in the transmission of such material and their services are being "misused" by criminals to victimize children. These industries are in a position to detect evidence of CAM and should be strongly encouraged to cooperate with authorities to provide information regarding CAM when they come upon it.

It should be noted that some companies are currently providing valuable assistance of this nature. In the case of ISPs and ESPs, it is more likely that they themselves will come across evidence of CAM in files, URLs, domain names and actual images that should be reported to the appropriate authorities immediately. Moreover, the sharing of URLs, domain names and IP addresses provides an opportunity for disrupting access to known child abuse web sites. ISPs and ESPs should also be encouraged to proactively scan their networks for CAM and report it to the relevant law enforcement authorities.

Given the current role of the Internet and its use for criminal purposes, cooperation with Internet-related companies is essential. Furthermore, legislation should provide protection for ISPs, ESPs and other private entities that report CAM and should include guidance for the safe handling and transmission of images.

A "Notice and Takedown" regime should be established to allow ISPs, ESPs, domain registrars and web hosts to close an offending site or cancel an email account upon request. In most cases, such criminal use will be in violation of the "Terms of Use" contract that the user agrees to with the ISP or ESPs, thus giving the company uncontested rights to take appropriate action. When possible, these actions should be closely coordinated with law enforcement in an effort to ensure that an investigation is launched that may

[20] National hotlines will refer reports to law enforcement; law enforcement can then analyse the reports for local connections or send the information on to the International Child Sexual Exploitation Database for analysis.

save a child from abuse and that will allow for the capture of the criminals involved.

Unfortunately the sale of CAM on the Internet has become a lucrative global enterprise that relies on bank services, wire transfers and credit cards to facilitate the sale, distribution or transmission of CAM. Financial industry officials who come upon information related to CAM should report it to the appropriate authorities. Often web sites offering "pay per view" or subscriptions to CAM accept credit cards or money transfer services for payment.

As a general rule the financial services industry should be encouraged to cooperate in line with the model of the Financial Coalition Against Child Pornography (FCACP)[21], a joint project of ICMEC and its sister organisation, the National Center for Missing & Exploited Children (NCMEC). This effective coalition provides a vehicle for close cooperation among the financial services industry, the Internet services industry, law enforcement and NGOs. It has achieved noteworthy success in denying commercial suppliers of CAM the use of the international financial system. Working together, the members of the FCACP have been able to not only report transactions and suspicious accounts, but also to track account activity and money flows in order to identify persons and organizations ultimately responsible for selling CAM. A European version of this coalition was launched in 2009.

Reducing the Availability of Child Abuse Images

The proliferation of CAM on the Internet has created a public outcry for action. Law enforcement, ISPs, ESPs and NGOs across the globe are collaborating to combat this content online. It is clear that law enforcement cannot arrest their way out of this problem and that more needs to be done to disrupt and reduce the traffic in CAM. As a result, many countries have begun to explore additional remedies that augment traditional law enforcement approaches.

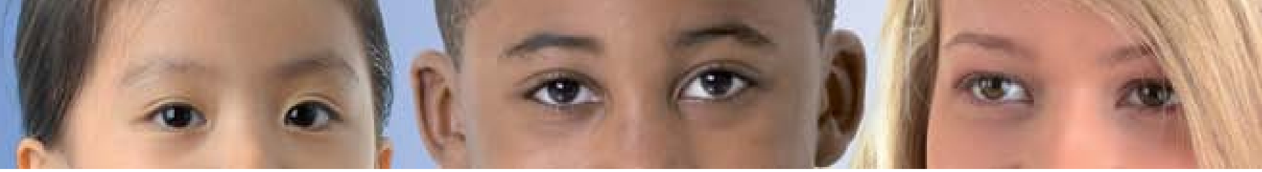
An approach which has been adopted in several countries is to encourage ISPs and other ESPs to reduce the availability of web pages that are known to offer CAM and to block access to Usenet Newsgroups that either regularly contain such content or advertise its availability.

In this approach, a "list" of Usenet Newsgroups and active web pages containing or advertising CAM is provided to ISPs and ESPs. This list is constructed and provided either by law enforcement or, in some cases, directly by national hotlines. It is very important that the basis on which such lists are constructed is clearly articulated. There should be no room for any suspicion that governmental, law enforcement or other bodies are able to influence its composition so as to include Newsgroups or web sites which do not contain CAM but instead contain items which they do not want to be published for other reasons.

When producing and distributing the list to ISPs and ESPs, an ongoing dialogue with law enforcement is crucial. Law enforcement needs adequate time to access, review and document the content and, if appropriate, to initiate an investigation. Failure to account for law enforcement activity could obstruct or delay an on-going investigation. Further, without law enforcement participation and investigation, the individuals who continuously distribute CAM online will never be apprehended and brought to justice.

It is important that the list of known sites and Usenet News-

[21] FCACP : http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=3064.

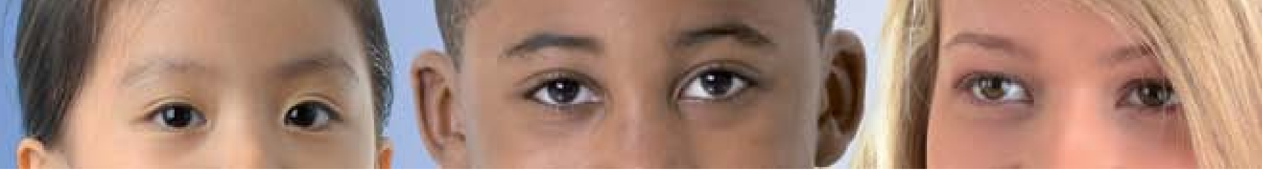


groups is tested frequently, updated and verified to ensure accuracy. The list should not be cumulative; rather, a multi-layered retesting procedure will help to ensure public confidence in the operation of the list. It is also important to ensure that guidelines on list criteria be transparent. Some countries utilize an independent means of auditing the performance and operation of the list. Lastly, a mechanism should exist to allow for an appeal against inclusion on the list. The only sites on the list should be those which allow the publishing or display of content which is illegal according to the national laws of the country concerned. When a site is blocked, a STOP page should be displayed to the user. This STOP page has the dual function of giving information as to the reason the site was blocked (illegality of content) plus acting as a prevention vehicle that reminds the user/consumer of the illegal nature of the material, as well as the presence of law enforcement agencies online.

Blocking access to web sites and Usenet Newsgroups containing CAM can make an important contribution to disrupting and reducing the volume of content being circulated or distributed over the Internet. However, this is recognized as only a part of the solution. This approach is not meant to be the only solution. The goal is to complement the efforts of law enforcement and to reduce the availability of CAM online. Individuals who have a sexual interest in children and enough technical knowledge and determination, may still be able to locate it. However, the web in particular, has such an easy user interface and has become one of the most widely used and most popular Internet applications, that it is essential to develop specific approaches for tackling it while continuing to evaluate new methods to thwart distribution on the other platforms of the Internet.

Thought should always be given to a joint government/industry awareness media campaign aimed at the consumers of CAM. Users/consumers should be reminded that CAM represents real pain for real children, and creating, possessing or distributing CAM is illegal in many countries.

> “Children and young people are often particularly vulnerable online”



4. Key Risks to Children Online

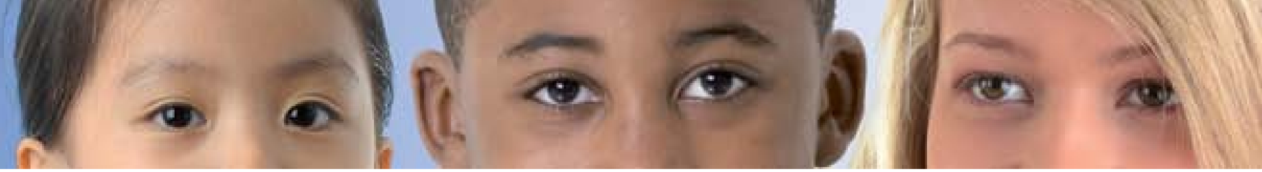
While adults and children alike are exposed to a range of risks and dangers online, children and young people are often particularly vulnerable. Children are still in a process of developing and learning. This has consequences for their capacity to identify, assess and manage potential risks. The idea that children are vulnerable and should be protected from all forms of exploitation is outlined in the UN Convention on the Rights of the Child[22].

There are a number of issues in relation to children's and young people's use of the Internet which are of on going concern to parents and children alike, as well as to governments, politicians and the policy making community. These concerns can be summarized as follows:

Content

- The Internet's ability to expose children and young people to illegal content, e.g. CAM.
- The Internet's ability to expose children and young people to legal but age inappropriate material e.g. very violent imagery.

[22] http://www.unhchr.ch/html/menu3/b/k2crc.htm



Contact

- The Internet's ability to expose children and young people to sexual predators, be they adults or other legal minors[23].
- The way in which the Internet may expose children to harmful online communities such as sites which encourage anorexia, self harm or suicide – as well as sources of political influence espousing violence, hate and political extremism.

Conduct

- The way in which the Internet facilitates and can promote risky sexual interactions between children themselves, including encouraging them to take and post pictures of themselves or others (sexting) which, aside from being harmful, may also be illegal. Normal sexual development and experimentation online can sometimes result in the inadvertent production and distribution of CAM exposing the child and his or her friends to possible legal sanction or involvement with the blunt edge of the criminal justice system.
- The way in which some aspects of the Internet encourage children to place in the public domain information about themselves, or post pictures or videos or text which might compromise their personal safety or jeopardize a number of career options for them in the future.
- The Internet's ability to expose children and young people to bullying and to allow or promote an environment in which children and young people are encouraged to bully others.

Commerce

- The ways in which the Internet has enabled children to access or acquire age inappropriate goods and services, typically goods and services which they could not purchase in person from a shop.
- The Internet's ability to expose children and young people to scams, identity theft, fraud and similar threats which are economic in nature or are rooted in inadequate data protection or privacy laws.

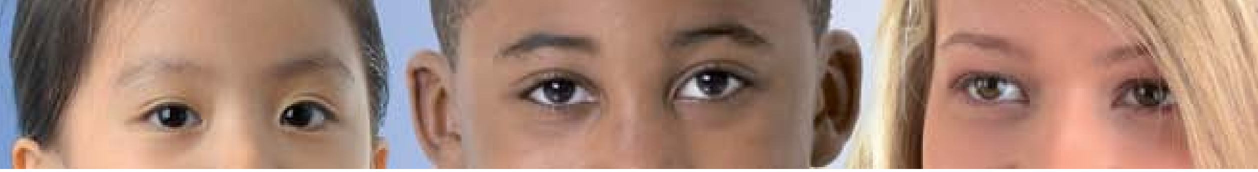
Excessive use

- The way the Internet seems, with some children and young people, to have encouraged forms of obsessive behavior or excessive use which may have deleterious effects on children's and young people's health or social skills, or both. Games and gaming over the Internet often feature in this type of online behavior which in some countries is referred to as a form of addiction.

Societal

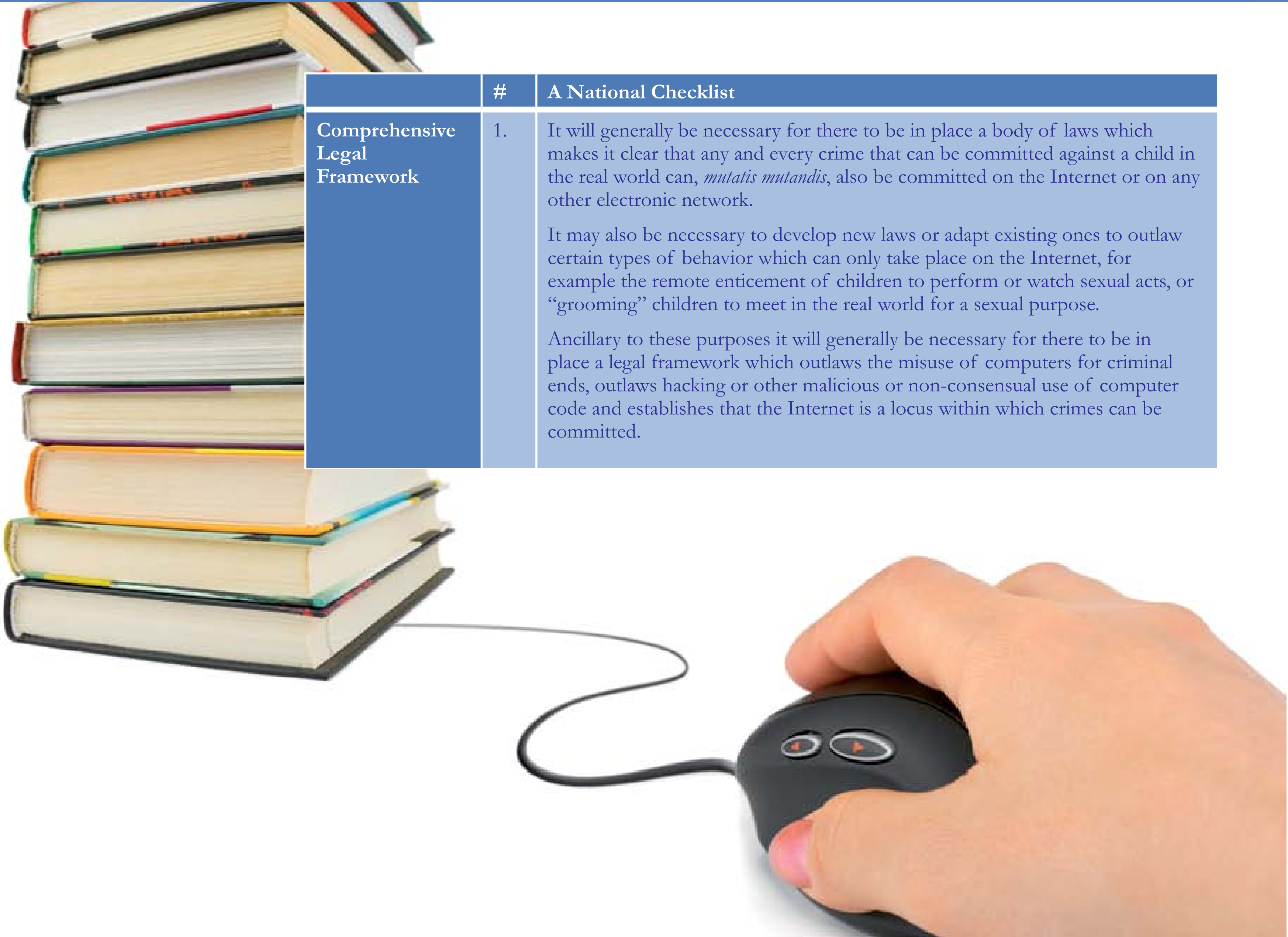
- The way the Internet has opened up a new digital divide among children and young people, both in terms of those who have ready and convenient access to it at home, school and elsewhere, and those who do not; between those who are confident and proficient users of it and those who are not. This divide threatens to entrench or widen existing patterns of advantage and disadvantage or perhaps create new divides.
- The potential of the Internet to compound and even magnify the existing vulnerabilities of particular children and young people and add to adversities that they may face in the offline world.

[23] See Appendix 1 for further detailed discussion of this aspect.

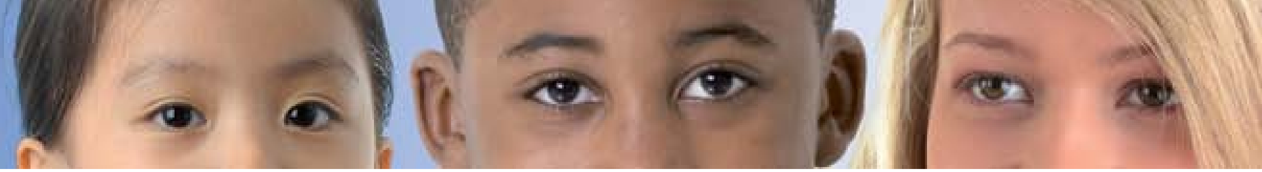


5. Addressing the Risks

A National Checklist

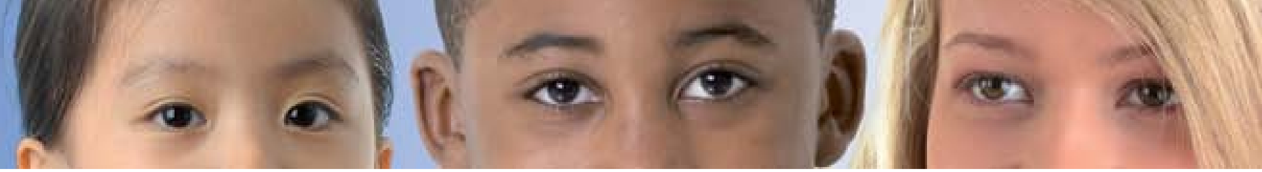


	#	A National Checklist
Comprehensive Legal Framework	1.	It will generally be necessary for there to be in place a body of laws which makes it clear that any and every crime that can be committed against a child in the real world can, *mutatis mutandis*, also be committed on the Internet or on any other electronic network. It may also be necessary to develop new laws or adapt existing ones to outlaw certain types of behavior which can only take place on the Internet, for example the remote enticement of children to perform or watch sexual acts, or "grooming" children to meet in the real world for a sexual purpose. Ancillary to these purposes it will generally be necessary for there to be in place a legal framework which outlaws the misuse of computers for criminal ends, outlaws hacking or other malicious or non-consensual use of computer code and establishes that the Internet is a locus within which crimes can be committed.

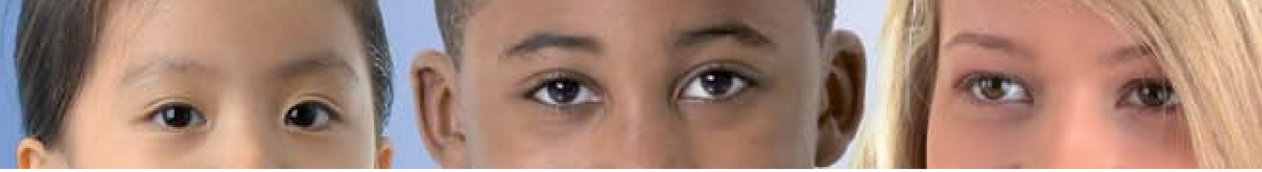


	#	A National Checklist
Need For a National Focus on Online Child Protection	2.	Several national governments have found it useful to bring together all of the key stakeholders and players to focus on developing and implementing a national initiative around making the Internet a safer place for children and young people, and raising awareness of the issues and how to deal with them in a very practical way. It will be important within this strategy to realise that the Internet can now be accessed via several different kinds of devices. Computers are only one of many ways of going online. Mobile phones, games consoles and PDAs are also increasingly important. The providers of both wireless and fixed-line access need to be involved. Additionally in many countries the network of public libraries, telecentres and Internet cafes can be important sources of Internet access particularly for children and young people. Some countries have found it to be advantageous to establish a self or co-regulatory model in relation to developing policy in this area and through such models they have, for example, published codes of good practice to guide the Internet industry in terms of the measures which may work best when it comes to keeping children and young people safer online. This has also worked at the regional level, for example within the European Union where EU-wide codes have been published both for social networking sites and mobile phone networks in relation to the provision of content and services to children and young people via their networks. Self and co-regulation can be a very effective way of helping to engage and sustain the involvement of all relevant stakeholders and can also be very effective in terms of enhancing the speed with which appropriate responses to technological change can be formulated and put into effect. Schools and the education system generally will play a very important part in rolling out such a national strategy, but the strategy also needs to go wider than that.

	#	A National Checklist
Need For a National Focus on Online Child Protection		Consideration should also be given to enlisting the aid of the mass media in promoting awareness messages and campaigns.
Need to Develop Local Resources Which Reflect National Laws and Local Cultural Norms	3.	Many of the large Internet companies produce web sites which contain a great deal of information about online issues for children and young people. However, very often this material will only be available in English or in a very narrow band of languages. It is very important, therefore, that materials are produced locally which reflect local laws as well as local cultural norms. This will be essential for any Internet safety campaign or any training materials that are developed.
Need for Public Education and Awareness Activities	4.	Parents and guardians and professional, such as teachers, have a crucial role to play in helping to keep children and young people safer online. Educational and outreach programmes should be developed which help build awareness of the issues and also provide strategies for dealing with them. When producing educational materials it is important to bear in mind that many people who are new to the technology will not feel comfortable using it. For that reason it is important to ensure that safety materials are made available in either written form or produced using other media with which newcomers will feel more familiar, for example, with video. Within any education and awareness campaign it will be important to strike the right tone. Fear-based messaging should be avoided and due prominence should be given to the new technology's many positive and fun features. The Internet has great potential as a means of empowering children and young people to discover new worlds.. Teaching positive and responsible forms of online behaviour is a key objective of education and awareness programs.



	#	A National Checklist
Need for Reporting Mechanisms for Online Predatory Behavior, Including Bullying	5.	Mechanisms for reporting abuse of an online service or for reporting objectionable or illegal behavior online, for example to a national hotline, should be widely advertised and promoted both on the Internet and in other media. Links to report abuse mechanisms should be prominently displayed on relevant parts of any web site that allows user generated content to appear. It should also be possible for people who feel threatened in any way, or for people who have witnessed any worrying activity on the Internet, to be able to report it as quickly as possible to the relevant law enforcement agencies who need to be trained and ready to respond. The Virtual Global Taskforce is a law enforcement body which provides a 24/7 mechanism to receive reports about illegal behaviour or content from persons in the USA, Canada, Australia and Italy, with other countries expected to join soon. See www.virtualglobaltaskforce.com
Helping Children to Stay Safer Through the Use of Technical Tools	6	There are a number of software programmes available which can help screen out unwanted material or block unwanted contacts. Some of these child safety and filtering programmes may be essentially free because they are part of a computer's operating system or they are provided as part of a package available from an ISP or ESP. The manufacturers of some game consoles also provide similar tools if the device is Internet enabled. These programmes are not foolproof but they can provide a welcome level of support, particularly in families with younger children. These technical tools should be used as part of a broader arsenal. Parental and/or guardian involvement is critical. As children start getting a bit older they will want more privacy and they will also feel a strong desire to start exploring on their own. In addition, where a billing relationship exists between vendor and customer, age verification processes can play a very valuable role in helping vendors of age restricted goods and services or the publishers of material which is intended only for audiences at or above a certain age, to reach out to those specific audiences. Where no billing relationship exists the use of age verification technology may be problematic or in many countries it may be impossible due to a lack of reliable data sources..



6. Stakeholders

In developing a national strategy to promote online safety for children and young people national governments and the policy making institutions need to identify and engage with the key stakeholders.

Children and Young People

Across the world children and young people have shown that they can adapt to and use the new technologies with great ease. The Internet is becoming increasingly important within schools and as an arena where children and young people work, play and communicate.

Most children and young people have no fear of the Internet and are comfortable using the different devices that can now provide access to it. Children's and young people's knowledge of how computers and the Internet work will often exceed that of their parents or teachers.

But knowledge is not the same as wisdom. Children's and young people's lack of experience of the wider world can render them vulnerable to a range of risks. They have a right to expect help and protection. It is also important to remember that not all children and young people will experience the Internet or the new technologies in the same way. Some children with special needs caused by physical or other disabilities may be particularly vulnerable in an online environment and so will need extra support.

Surveys have repeatedly shown that what adults think children and young people are doing online and what is actually happening can be very different. For this reason, if for no other, it is important to ensure, in whatever arrangements are made at the national level to develop policy in this area, that appropriate mechanisms are found to enable all children's and young people's voices to be heard and that their concrete experiences of using the technology are taken into account.

Parents, Guardians and Educators

One of the reasons many parents are buying computers with Internet access for use at home is to help with their children's education and to help with homework assignments. Schools therefore have a particular responsibility to teach children about how to stay safer online, whether they are using the Internet in school, at home or anywhere else. In order for teachers to be able to do that they, in turn, need professional training linked to first class, up to date teaching resources.

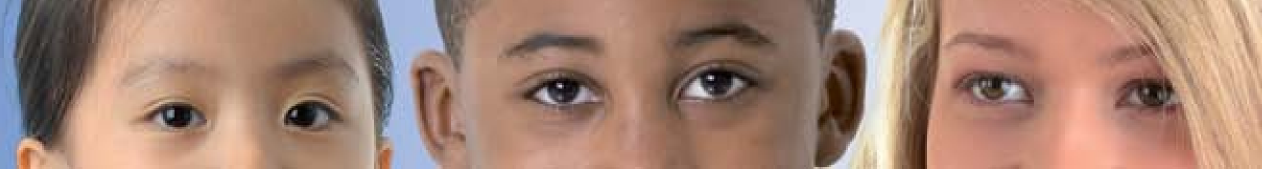
Parents and guardians will almost always be the first, last and best line of defense and support for their own children. Yet when it comes to the Internet they might feel a little lost. Again schools can act as an important channel for reaching out to parents and guardians, to make them aware both of the risks and the many positive possibilities which the new technologies present. However, schools should not be the only route used to reach out to parents and guardians. It is important to use many different channels so as to maximize the possibility of reaching out to as large a number of parents and guardians as possible. Public libraries, health centres, even shopping malls and other major retail centres can all provide accessible venues for thepresentation of safety information.

Industry

Clearly companies that are developing or providing new technology products and services are going to be well placed to help other stakeholders understand how they work and how to use them safely and appropriately. For that reason it is important to engage with businesses to encourage them to share their knowledge and expertise.

The industry also has a major responsibility to help promote awareness of the online and safety agenda, particularly to children and young people and their parents or guardians, but also to the wider community. By engaging in this way the industry will learn more about different stakeholders' concerns and that knowledge will help them to identify such hazards in any new products or services they have in development, as well as enable them to correct existing ones.

In some countries the Internet is governed by a framework of self regulation or co-regulation. This can give the Internet industry a voice in the development of public policy and can help ensure that policy is well founded technically. It also can mean that, as technology changes, adjustments in practice can be introduced quite rapidly without having to wait for the sometimes lengthy processes involved in devising and passing new laws. While welcoming industry's engagement in helping to promote a better understanding of online safety issues it will also be important for national governments and other parts of the policy making community to have their own independent sources of advice.



The Research Community and NGOs

Within the universities and other parts of the research community there is very likely to be a range of academics and scholars who have a professional interest in and a very detailed knowledge of both the social and the technical aspects and impact of the Internet. They could be a very valuable resource in terms of helping national governments and policy makers to develop strategies which are based on hard facts and good evidence. They can also act as an intellectual counterweight to the high-tech companies whose interests can sometimes be short term in nature and be predominantly commercial in character.

Similarly, within the NGO community there will very often be a range of expertise and information which can be an invaluable resource in reaching out or providing services to children, young people, parents, guardians and educators to help promote the online safety agenda.

Law Enforcement

It is a sad fact that as wonderful as technology is, it has also attracted the attention of criminal and anti-social elements. The Internet has greatly increased the circulation of CAM. Sexual predators have used the Internet to make initial contact with children and young people, luring them into very harmful forms of contact, online and offline. Bullying and other forms of harassment can do great harm to children's and young people's lives and the Internet has provided a new way for that to happen.

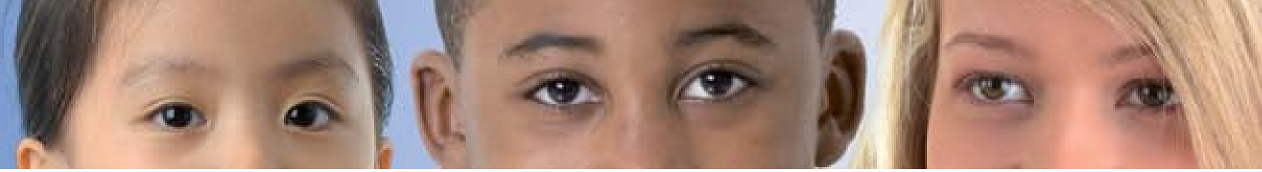
For these reasons, it is essential that the law enforcement community becomes fully engaged with any overall strategy to help make the Internet safer for children and young people. Law enforcement officers need to be appropriately trained to conduct investigations into Internet related crimes against children and young people. They need the right level of technical knowledge and access to forensic facilities to enable them to extract and interpret data obtained from computers or the Internet.

In addition, it is very important that law enforcement establishes clear mechanisms to enable children and young people, or any member of the public, to report any incidents or concerns they might have about a child's or a young person's online safety. Many countries, for example, have established hotlines to facilitate reports of CAM and similar dedicated mechanisms exist to facilitate reports of other kinds of issues, for example bullying and other kinds of threatening behavior.

Law enforcement is the primary source for CAM seized within national borders. A process should be put in place to examine this material in order to establish whether local victims can be identified. Where this is not possible the material should be passed onto INTERPOL for inclusion in the ICSE Database.

Social Services

Where children or young people have been harmed or abused online, for example by having an inappropriate or illegal picture posted of them, they are likely to need specialized and long-term support or counseling. Professionals working within social services will need to be appropriately trained to be able to provide this kind of support.



7. Conclusion

The Internet is now the indispensable nexus for an array of digital technologies which are transforming economies, opening up an array of possibilities to improve people's lives and to enrich societies in a variety of ways.

At a macro level, it is hugely important that the economic advantages which the Internet can generate are spread evenly across the world. The prospect of a digital divide growing up between the developed world and the industrializing economies, entrenching or widening existing disadvantages or imbalances, was addressed by the WSIS processes. It continues to be a major feature of policy discussions within the WSIS Forum[24] , the Internet Governance Forum (IGF)[25] and in many related international fora.

At the individual level, the Internet has become a tremendously enriching and empowering technology. Children and young people in particular have been major beneficiaries of the Internet and related digital technologies. These technologies are transforming the way we all communicate with each other and have opened up many new ways to play games, enjoy music and engage in a vast array of cultural activities, dissolving many barriers of time and space. Children and young people have very often been at the forefront of adopting and adapting to the possibilities provided by the Internet.

[24] http://www.itu.int/wsis/implementation/2009/forum/geneva/index.html

[25] www.intgovforum.org

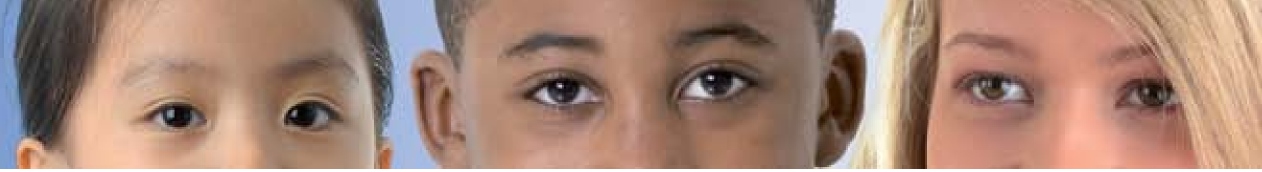
Yet, it is undeniable that the Internet has brought in its wake a range of challenges to children's and young people's safety which need to be addressed, both because they are important in their own right but also because it is important to communicate to everyone concerned that the Internet is a medium we should all be able to trust. Equally it is essential that, we collectively do not allow an apparent concern to protect children and young people online to become a platform to justify entirely unrelated assaults on free speech, free expression or the freedom of association.

It is extremely important for the next generation to feel confident about using the Internet in order that they can, in turn, continue to benefit from its development. Thus, when discussing the safety of children and young people online, it is vital to strike a balance.

It is essential to discuss openly the hazards which exist for children and young people online, so we can teach them how to avoid the risks altogether or teach them how to deal with them should they nonetheless materialize, however, we must not do so in a way which exaggerates the dangers or which is unduly frightening. An approach which deals only or largely with the negative aspects of the technology is very unlikely to be taken seriously by children and young people because hundreds of millions of them are already using it everyday and they therefore know a great deal about what it is and what it can be. In this respect parents and the members of older generations can often find themselves at a disadvantage. Here is an instance where young people will very often know more about the technology and its possibilities than their parents and teachers. But knowledge is not the same as wisdom.

National governments have an obligation to provide for the protection of legal minors in both the "real" and "virtual" worlds. In an important sense, because the new technologies are now so thoroughly integrated into the lives of so many children and young people in a number of important ways, it no longer makes sense to try to maintain rigid distinctions between "real world" events and online events. The two are increasingly intertwined and interdependent.

National governments and the policy making community have a major responsibility both to set the framework within which an appropriate national and multinational response can be developed and then to sustain it over time. In doing so the Internet industry itself and all of the relevant stakeholders will have very important roles to play, not least because the speed with which the technology can change means that many of the traditional methods of law or policy making no longer fit this purpose. As this report has shown, the new technologies are also making new demands on law makers.



Appendix 1

Contact Offences Against Children and Young People

Children and young people can be exposed to a range of unwanted or inappropriate contact on the Internet which can have dire consequences for them. Some of this contact might be sexual in nature.

Studies in Europe by EU Kids Online in 2008 reveal some disturbing results (median figures): 15-20% have been bullied, harassed or stalked online; 25% have received unwanted sexual comments; 9% have met people in real life whom they had previously only known online. Though the rates vary by country and region, these figures demonstrate that the risks are real.[26] One American Internet study[27] found that 32% of teens online have been contacted by a complete stranger, of those, 23% said they felt scared and uncomfortable during the contact; and 4% of those kids received aggressive sexual solicitation.

Sexual predators use the Internet to contact children and young people for sexual purposes, often using a technique known as "grooming" whereby they gain the child's confidence by appealing to his or her interests. They often introduce sexual topics, photos and explicit language to desensitize, raise sexual awareness and soften the will of their young victims. Gifts, money and even tickets for transportation are used to persuade and lure the child or young person to a place where the predator can sexually exploit him or her. These encounters may even be photographed or videotaped. Children and young people often lack emotional maturity and self-esteem which makes them susceptible to manipulation and intimidation. They are also hesitant to tell adults about their encounters for fear of embarrassment or of losing access to the Internet. In some cases they are threatened by predators and told to keep the relationship a secret.

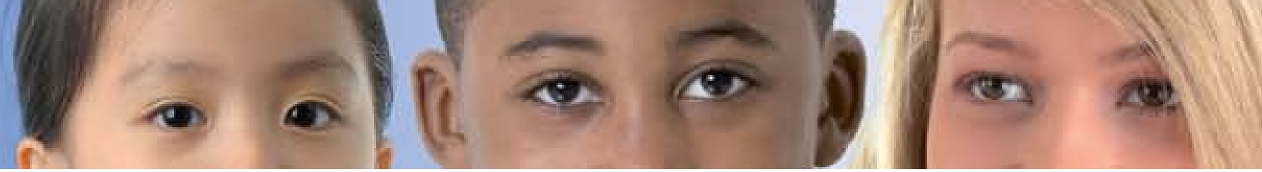
Sexual predators learn from one another through Internet fora and chat rooms. When communicating with children and young, these predators often pretend to be closer to the child's or young

[26] EU Kids Online Report, Comparing Children's Online Opportunities and Risks Across Europe, pages 29-30, June 2008.

[27] Pew Internet and American Life Project 2007.

person's age than they really are, and claim to be seeking friendship. Once they gain the child's confidence, they take advantage of his or her vulnerabilities — such as loneliness or upset over a personal loss — to create an emotional dependence on the predator. There are numerous media reports of cases where a child or a young person has agreed to meet face-to-face with someone they have been talking to online, and who they think is within their age group, only to find that the individual is an older male interested in having sex with them. Unfortunately, some of these cases have resulted in the victimization and sexual molestation of the child; in a few cases the outcomes were far worse.

A particularly disturbing trend is for predators to broadcast sexual acts with children or young people via real-time webcam video to an audience of other predators — often to solicit their approval. In such cases, the child or young person not only suffers harmful and lasting psychological (and sometimes physical) trauma from the heinous act but is victimized over and over by the posting of the images on the Internet where they become objects of collection for other predators. These new images are welcomed and used, traded and sometimes sold on the Internet to other predators who need new material to satisfy their sexual fantasies. Sadly, victims are often unable to obtain a sense of closure and to get on with their lives long after the horrible events have occurred because they live in constant fear that their image will be recognized by others. Even more contemptible is the use of these images by the predator to "blackmail" the child or young people into maintaining silence and complying with the ongoing abuse.



Appendix 2

“Child Pornography: Model Legislation & Global Review”

With the support of Interpol and Microsoft, the International Centre for Missing & Exploited Children (ICMEC) reviewed the child pornography legislation of the 187 Interpol Member Countries and made recommendations for key concepts that, when applied in national legislation, would constitute a comprehensive legislative strategy to combat child pornography.

Unfortunately, the report concluded[28] that few of the world’s countries have legislation in place that is sufficient to combat child pornography on some level.

The complete report, which is now in its 5th Edition, can be found at www.icmec.org in Arabic, English, French, Korean, Portuguese, Russian, Spanish, Thai and Turkish.[29]

Following is a listing of Interpol Member Countries and the status of their child pornography legislation.

[28] The report concluded that:

- ✓ only 29 have legislation sufficient to combat child pornography offenses (5 Interpol Member Countries meet all of the criteria set forth above and 24 Interpol Member Countries meet all but the last criteria, pertaining to ISP reporting); and
- ✓ 93 Interpol Member Countries have no legislation at all that specifically addresses child pornography.

Of the remaining Interpol Member Countries that do have legislation specifically addressing child pornography:

- 54 do not define child pornography in national legislation;
- 24 do not explicitly provide for computer-facilitated offenses; and
- 36 do not criminalize possession of child pornography, regardless of the intent to distribute.

[29] www.icmec.org

Global Review

(Reprinted with the permission of the International Centre for Missing & Exploited Children)

✗ = No ✓ = Yes

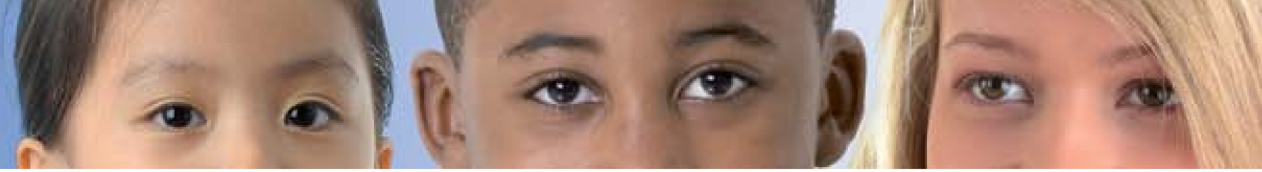
Country	Legislation Specific to Child Pornography[30]	"Child Pornography" Defined	Computer-Facilitated Offenses[31]	Simple Possession[32]	ISP Reporting[33]
Afghanistan	✗	✗	✗	✗	✗
Albania	✗	✗	✗	✗	✗
Algeria	✗	✗	✗	✗	✗
Andorra	✓	✗	✗	✓	✗
Angola	✗	✗	✗	✗	✗

[30] For the purposes of this report, we were looking for specific laws that proscribe and/or penalize child-pornography offenses. Mere labor legislation that simply bans the "worst forms of child labor," among which is child pornography, is not considered "legislation specific to child pornography."
Further, countries in which there is a general ban on pornography, regardless of whether the individuals being depicted are adults or children, are not considered to have "legislation specific to child pornography," unless there is a sentencing enhancement provided for offenses committed against a child victim.

[31] In order to qualify as a computer-facilitated offense, we were looking for specific mention of a computer, computer system, Internet, or similar language (even if such mention is of a "computer image" or something similar in the definition of "child pornography"). In cases where other language is used in national legislation, an explanatory footnote is provided.

[32] "Simple possession," for the purposes of this report, refers to possession regardless of the intent to distribute.

[33] While some countries may have general reporting laws (*i.e.*, anyone with knowledge of any crime must report the crime to the appropriate authorities), only those countries that specifically require ISPs to report suspected child pornography to law enforcement (or another mandated agency) are included as having ISP reporting laws. Note that there are also provisions in some national laws (mostly within the European Union) that limit ISP liability as long as an ISP removes illegal content once it learns of its presence; however, such legislation is not included in this section.



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Antigua & Barbuda	✗	✗	✗	✗	✗
Argentina	✓	✓	✓	✗	✗
Armenia	✓	✗	✓	✗	✗
Aruba	✓	✗	✓	✓	✗
Australia	✓	✓	✓	✓	✓
Austria	✓	✓	✓[34]	✓	✗
Azerbaijan	✗	✗	✗	✗	✗
Bahamas	✗	✗	✗	✗	✗
Bahrain	✗	✗	✗	✗	✗
Bangladesh	✗	✗	✗	✗	✗
Barbados	✓	✗	✗	✓	✗

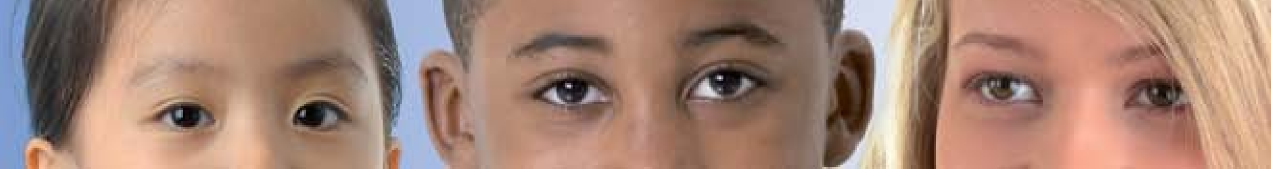
[34] Section 207a(1)(3) of the Austrian Penal Code criminalizes "mak[ing] available in **any other manner**…a pornographic depiction of a minor." *Emphasis added.*

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Belarus	✓	✗	✗	✗	✗
Belgium	✓	✓	✓[35]	✓	✓
Belize	✗	✗	✗	✗	✗
Benin	✗	✗	✗	✗	✗
Bhutan	✓	✗	✓[36]	✗	✗
Bolivia	✗	✗	✗	✗	✗
Bosnia-Herzegovina	✓	✗	✓[37]	✓	✗
Botswana	✗	✗	✗	✗	✗
Brazil	✓	✓	✓	✓	✗

[35] Article 383bis of the Belgian Penal Code, as amended on 1 April 2001, criminalizes, *inter alia*, the dissemination of child pornography, thereby including dissemination via computers. Letter from Jan Luykx, Deputy Chief of Mission, Embassy of Belgium, Washington, D.C., to Ernie Allen, President and CEO, International Centre for Missing & Exploited Children (Feb. 24, 2006) (on file with the International Centre for Missing & Exploited Children).

[36] According to Article 225(b) of the Penal Code of Bhutan, "[a] defendant shall be guilty of the defense of pedophilia if the defendant…sells, manufactures, distributes, or **otherwise deals** in material that contains any depiction of a child engaged in sexual contact." *Emphasis added.*

[37] Articles 189 and 211 of the Penal Code of Bosnia-Herzegovina reference "other pornographic materials" in addition to photographs and audio-visual tapes.



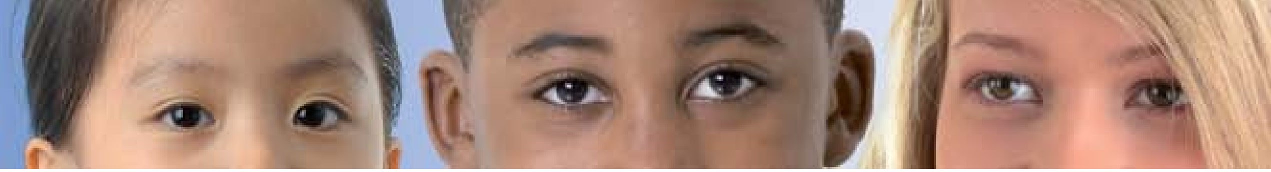
Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Brunei	✓	✗	✓	✗	✗[38]
Bulgaria	✓	✗	✓[39]	✓	✗
Burkina-Faso	✗	✗	✗	✗	✗
Burundi	✗	✗	✗	✗	✗
Cambodia	✗	✗	✗	✗	✗
Cameroon	✗	✗	✗	✗	✗

[38] While there is no mandatory-reporting requirement specific to ISPs, under the laws of Brunei all ISPs and Internet Content Providers (ICPs) licensed under the Broadcasting (Class License) Notification of 2001 must comply with the Code of Practice set forth in the Broadcasting Act (Cap 181). ISPs and ICPs are required to satisfy the Minister responsible for broadcasting matters that they have taken responsible steps to fulfill this requirement. Under the Broadcasting Act, such Minister has the power to impose sanctions. Content that should not be allowed includes, *inter alia*, that which depicts or propagates pedophilia.
The Licensee must remove or prohibit the broadcast of the whole or any part of a program included in its service if the Minister informs the Licensee that the broadcast of the whole or part of the program is contrary to a Code of Practice applicable to the Licensee, or if the program is against the public's interest, public order, or national harmony, or offends against good taste or decency.
The Licensee must also assist the Minister responsible for broadcasting matters in the investigation into any breach of its license or any alleged violation of any law committed by the Licensee or any other person; and shall also produce such information, records, documents, data, or other materials as may be required by the Minister for the purposes of the investigation. E-mail from Salmaya Salleh, Second Secretary, Embassy of Brunei, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Mar. 21, 2006) (on file with the International Centre for Missing & Exploited Children).

[39] Article 159(3) of the Bulgarian Penal Code, when read in conjunction with Article 159(1), criminalizes, *inter alia*, "**otherwise circulat[ing]** works with a [child] pornography content." *Emphasis added.*

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Canada	✓	✓	✓	✓	✗ [40]
Cape Verde	✓	✗	✗	✗	✗
Central African Republic	✗	✗	✗	✗	✗
Chad	✗	✗	✗	✗	✗
Chile	✓	✓	✓	✗	✗

[40] While there is no mandatory reporting requirement specific to ISPs, ISPs in Canada collaborate with law enforcement and work closely to facilitate the reporting of offending material. Canadian criminal law employs a very broad definition of "child pornography," which gives its comprehensive set of offenses additional scope. The specific offenses of transmitting, making available, and accessing were added in 2002 to address the Internet context and would apply to the activities of ISPs. Canada also introduced a "notice and takedown" provision for child pornography found on the Internet in that same legislation. Penalties for child pornography offences were enhanced in 2005 by: imposing mandatory minimum penalties; increasing the maximum penalties on summary conviction from 6 to 18 months imprisonment; making the commission of any child pornography offense with intent to profit an aggravating factor for sentencing purposes; making denunciation and deterrence the primary sentencing objectives in any case involving the abuse of a child; and making the abuse of any child an aggravating factor for sentencing purposes. In addition to the comprehensive protections found under the criminal law, Canada also has a national, public tipline for reporting online child sexual exploitation (www.Cybertip.ca) that performs a triage function on those reports for law enforcement. Additionally, Cybertip.ca also maintains the Project Cleanfeed Canada database that blocks approximately 90% of Canadian subscribers from accessing known child pornography sites that may be beyond the reach of Canadian prosecution. Further, Canada has a National Strategy for the Protection of Children from Sexual Exploitation on the Internet, of which the National Child Exploitation Coordination Centre (Centre) is a key component. The Centre, which is located with the Royal Canadian Mounted Police, coordinates domestic and foreign online child sexual exploitation investigation, provides training to Canadian law enforcement, and serves as a central clearing house for reports received from Cybertip.ca. Summary of letter from Carole Morency, A/General Counsel, Criminal Law Policy Section, Department of Justice Canada, to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (June 24, 2008) (complete letter on file with the International Centre for Missing & Exploited Children).



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
China[41]	✓[42]	✗	✓[43]	✗	✗
Colombia	✓	✓	✓	✗	✓
Comoros	✗	✗	✗	✗	✗
Congo	✗	✗	✗	✗	✗
Costa Rica	✓	✓	✗	✓	✗
Côte d'Ivoire	✗	✗	✗	✗	✗
Croatia	✓	✗	✓	✓	✗

[41] Child pornography legislation in Hong Kong differs from that in China. Legislation in Hong Kong:
- defines child pornography;
- criminalizes computer-facilitated offenses; and
- criminalizes simple possession of child pornography.

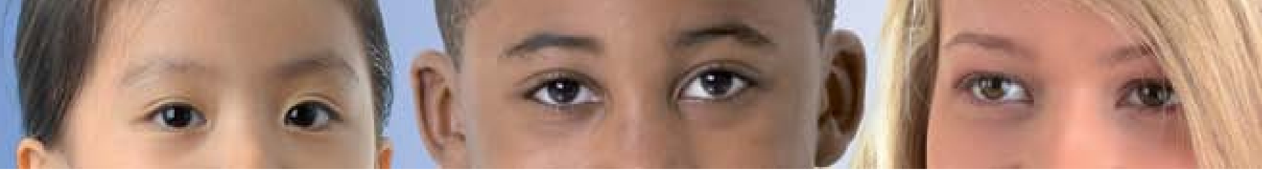
[42] While China does not have any specific child-pornography legislation, there is a general prohibition on obscene and pornographic materials in the Criminal Code. In 2004, with the aim of better protecting minors, the Supreme People's Court and the Supreme People's Protectorate promulgated an "Interpretation On Several Issues Regarding the Implementation of Laws in Dealing with Criminal Cases Involving the Production, Duplication, Publication, Sale, Dissemination of Pornographic Electronic Information Using Internet, Mobile Communications Terminals, Radio Stations." Article 6 of this Interpretation explicitly stipulates that, "whoever disseminates, duplicates, publishes, or sells pornographic electronic information that depicts sexual behaviors of adolescents under the age of 18, or provides direct linkage in the Internet server or websites owned, managed, or used by himself/herself, to the electronic information with the knowledge that such information depicts sexual behaviors of adolescents under the age of 18, shall be severely punished in accordance with Article 363 of the Criminal Law regulating the punishment of crimes of production, duplication, publication, sale, and dissemination of pornographic materials, or Article 364 regulating the punishment of crimes of dissemination of pornographic materials with serious circumstances." E-mail from Chen Feng, Police Liaison Officer, Embassy of the People's Republic of China, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Mar. 17, 2006) (on file with the International Centre for Missing & Exploited Children).

[43] The 2004 Interpretation by the Supreme People's Court and the Supreme People's Protectorate applies to computer-facilitated offenses.

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Cuba	✗	✗	✗	✗	✗
Cyprus	✓	✓	✓	✓	✗
Czech Republic	✓	✗	✓	✓	✗[44]
Democratic Republic of Congo	✗	✗	✗	✗	✗
Denmark	✓	✓	✓[45]	✓	✗
Djibouti	✗	✗	✗	✗	✗
Dominica	✗	✗	✗	✗	✗
Dominican Republic	✓	✓	✓	✓	✗
Ecuador	✓	✗	✗	✗	✗
Egypt	✓	✗	✓	✓	✗

[44] While there is no ISP-reporting requirement in Czech law, the Czech National Plan on the Fight Against Commercial Sexual Exploitation of Children, available online at http://www.mvcr.cz/prevence/priority/kszd/en_tab.html, names the Ministry of Transportation and Communications and the Ministry of the Interior as the national agencies charged with specifying the statutory obligation of Internet providers included in the Telecommunications Act (No. 151/2000) to file the necessary data on illegal websites and to hand them over to Czech law enforcement. The expected result of this measure is to secure "evidentiary facts against those who spread child pornography on the Internet."

[45] Section 235 of the Danish Criminal Code criminalizes, *inter alia*, dissemination and possession of "other…visual reproductions" of pornographic materials concerning children under the age of 18.



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
El Salvador	✓	✗	✓	✓	✗
Equatorial Guinea	✗	✗	✗	✗	✗
Eritrea	✗	✗	✗	✗	✗
Estonia	✓	✗	✓[46]	✓	✗
Ethiopia	✗	✗	✗	✗	✗
Fiji	✗	✗	✗	✗	✗
Finland	✓	✓	✓[47]	✓	✗
France	✓	✓	✓	✓	✓
Gabon	✗	✗	✗	✗	✗
Gambia	✓	✗	✗	✗	✗
Georgia	✓	✓	✗	✗	✗

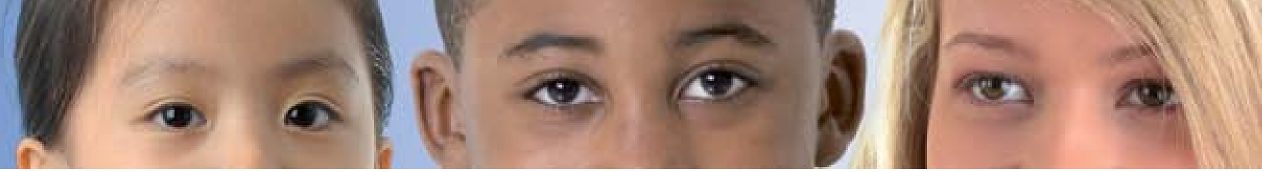
[46] Articles 177 and 178 of the Estonian Penal Code criminalize using a minor in "other works" or using "any other manner" to manufacture, store, hand over, display, or make available child pornography.

[47] Chapter 17, section 18 of the Finnish Criminal Act criminalizes "any person who…otherwise distributes obscene pictures or visual recordings depicting children."

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Germany	✓	✓	✓	✓	✗ [48]
Ghana	✗	✗	✗	✗	✗
Greece	✓	✓	✓ [49]	✓	✗
Grenada	✗	✗	✗	✗	✗
Guatemala	✓	✗	✗	✗	✗
Guinea	✗	✗	✗	✗	✗
Guinea Bissau	✗	✗	✗	✗	✗
Guyana	✗	✗	✗	✗	✗
Haiti	✗	✗	✗	✗	✗
Honduras	✓	✓	✓	✓	✗

[48] While there is no explicit obligation for an ISP to report to law enforcement or another mandated agency, in most cases ISPs will file reports with law enforcement. It is a punishable offense for an ISP that knows of child pornographic material on its websites to not delete the illegal content. Factors considered include whether it was possible and reasonable for the ISP to detect the data and to delete or block it, as there are many ISPs in Germany that offer large storage capacities for commercial purposes. E-mail from Klaus Hermann, Counselor/Police Liaison, Embassy of Germany, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 9, 2006) (on file with the International Centre for Missing & Exploited Children).

[49] Article 348a of the Greek Penal Code criminalizes various child-pornography offenses, including possession, purchase, transfer, and sale of child pornography "in any way."



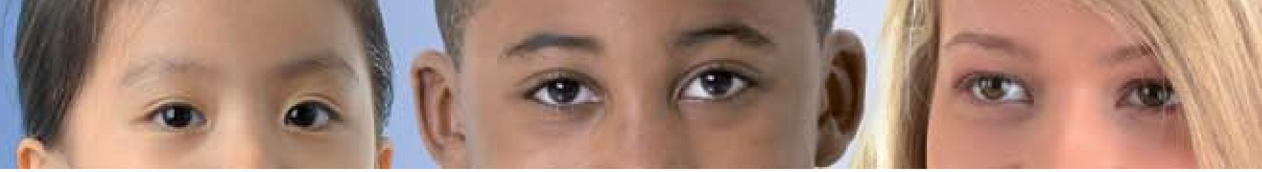
Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Hungary	✓	✓	✓[50]	✓	✗
Iceland	✓	✗	✓[51]	✓	✗
India	✓	✗	✓	✓	✗
Indonesia	✗	✗	✗	✗	✗
Iran	✗	✗	✗	✗	✗
Iraq	✗	✗	✗	✗	✗
Ireland	✓	✓	✓	✓	✗
Israel	✓	✓	✓	✓	✗
Italy	✓	✓	✓	✓	✗
Jamaica	✗	✗	✗	✗	✗
Japan	✓	✓	✓	✗	✗

[50] Under Section 195/A(3) of the Hungarian Criminal Code, a person making, distributing, or trading pornographic pictures of a minor by video, film, photograph, or "by any other means," or making such pictures available to the public, commits a felony. Further, according to a recent decision of the Hungarian Appellate Court (Nr. BH 133/2005), the reference to "any other means" and "making available to the public" includes distribution through the Internet. Letter from Viktor Szederkényi, Deputy Chief of Mission, Embassy of the Republic of Hungary, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 6, 2006) (on file with the International Centre for Missing & Exploited Children).

[51] Article 210 of the Penal Code of Iceland criminalizes the "possession of photographs, films, or **comparable items** depicting children in a sexual or obscene manner." *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Jordan	✗	✗	✗	✗	✗
Kazakhstan	✓	✗	✗	✗	✗
Kenya	✗	✗	✗	✗	✗
Korea	✓	✓	✓	✗	✗
Kuwait	✗	✗	✗	✗	✗
Kyrgyzstan	✓	✗	✗	✗	✗
Laos	✗	✗	✗	✗	✗
Latvia	✓	✗	✓[52]	✗	✗
Lebanon	✗	✗	✗	✗	✗
Lesotho	✗	✗	✗	✗	✗
Liberia	✗	✗	✗	✗	✗
Libya	✗	✗	✗	✗	✗

[52] Article 166(2) of the Criminal Law of Latvia criminalizes “the importation, production, public demonstration, advertising, or **other distribution** of such pornographic… materials as relate or portray the sexual abuse of children.” *Emphasis added.*



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Liechtenstein	✓	✗	✓	✓	✗[53]
Lithuania	✓	✗	✗	✓	✗
Luxembourg	✓	✗	✓[54]	✓	✗
Macedonia	✓	✗	✓[55]	✗	✗
Madagascar	✓	✗	✓[56]	✗	✗
Malawi	✗	✗	✗	✗	✗
Malaysia	✗	✗	✗	✗	✗
Maldives	✗	✗	✗	✗	✗
Mali	✓	✗	✗	✗	✗
Malta	✓	✗	✓	✓	✗

[53] While there is no specific mention of ISP reporting in the Penal Code of Liechtenstein, in the draft of the new Children and Youth Act, a reporting requirement is foreseen that would apply to "anyone learning of the endangerment of the welfare of a child or young person." E-mail from Claudia Fritsche, Ambassador, Embassy of Liechtenstein, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 7, 2006) (on file with the International Centre for Missing & Exploited Children).

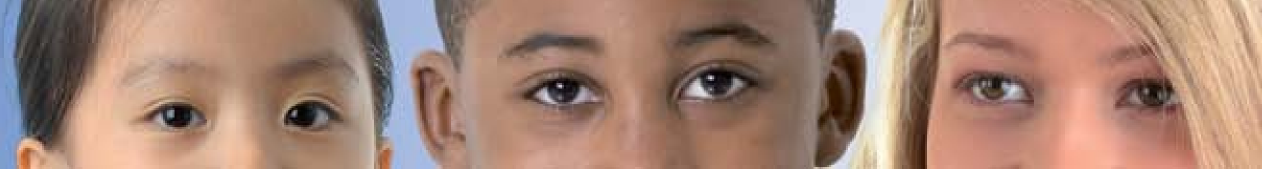
[54] Article 383 of the Penal Code of Luxembourg criminalizes not only the manufacture and possession (for trade, distribution, or public display) of "writings, printings, images, photographs, films, or **other objects** of a pornographic nature," but also the commission of a variety of other child-pornography offenses in "any way." *Emphasis added.*

[55] Article 193(3) of the Macedonian Penal Code criminalizes the abuse of a "juvenile" in the "production of…other objects with a pornography content."

[56] Article 346 of the Penal Code of Madagascar criminalizes the use of "any means" to disseminate child pornography.

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Marshall Islands	✗	✗	✗	✗	✗
Mauritania	✗	✗	✗	✗	✗
Mauritius	✓	✗	✓	✗	✗
Mexico	✓	✓	✓	✗	✗
Moldova	✓	✗	✗	✓	✗
Monaco	✗	✗	✗	✗	✗
Mongolia	✗	✗	✗	✗	✗
Montenegro	✓	✗	✓[57]	✗	✗
Morocco	✓	✗	✗	✓	✗
Mozambique	✗	✗	✗	✗	✗
Myanmar	✓	✗	✗	✗	✗
Namibia	✗	✗	✗	✗	✗
Nauru	✗	✗	✗	✗	✗

[57] Article 211(2) of the Penal Code of Montenegro criminalizes "exploit[ing] a child for the production of pictures, audio-visual, or **other items** of pornographic content." *Emphasis added.*



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Nepal	✓	✗	✗[58]	✗	✗
Netherlands	✓	✓	✓	✓	✗[59]
Netherlands Antilles	✗[60]	✗	✗[61]	✗[62]	✗
New Zealand	✓	✓	✓	✓	✗
Nicaragua	✗	✗	✗	✗	✗
Niger	✗	✗	✗	✗	✗
Nigeria	✗	✗	✗	✗	✗
Norway	✓	✓	✓	✓	✗
Oman	✗	✗	✗	✗	✗
Pakistan	✗	✗	✗	✗	✗

[58] While not specific to child pornography, section 47 of the Electronic Transaction Ordinance of 2004 does prohibit the publishing or displaying on computers, the Internet, or other electronic media, materials that are prohibited by law to be published or displayed because they are against public morality and decency.

[59] While there is no legal or contractual obligation for ISPs to report suspected child pornography to law enforcement, Netherlands-based ISPs do have a practice of reporting their findings of child pornography immediately to law enforcement and the ISPs remove the content from the concerned web site. Further, on the request of law enforcement, ISPs hand over their logs concerning the web site(s) under suspicion. E-mails from Richard Gerding, Counselor for Police and Judicial Affairs, Royal Embassy of The Netherlands, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 8, 2006) (on file with the International Centre for Missing & Exploited Children).

[60] While legislation specific to child pornography does not yet exist, a committee has been installed to revise the current Netherlands Antilles Penal Code. Specific legislation on child pornography will be introduced (Proposed Article 2.13.4). E-mail from Richard Gerding, Counselor for Police and Judicial Affairs, Royal Embassy of The Netherlands, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 22, 2006) (on file with the International Centre for Missing & Exploited Children).

[61] Proposed Article 2.13.4 would criminalize computer-facilitated offenses.

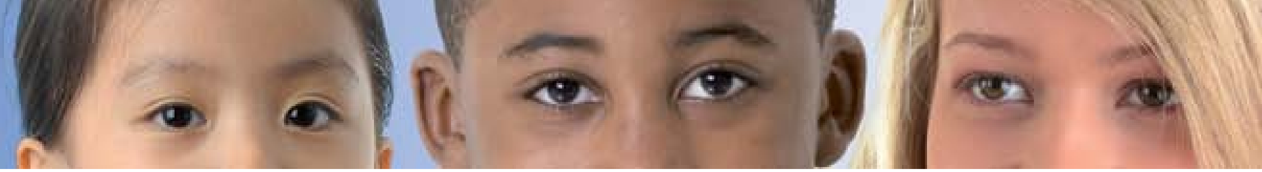
[62] Proposed Article 2.13.4 would criminalize simple possession.

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Panama	✓	✓	✓	✓	✗[63]
Papua New Guinea	✓	✗	✗	✓	✗
Paraguay	✓	✗	✗	✓	✗
Peru	✓	✓	✓	✓	✗
Philippines	✓	✗	✗	✗	✗
Poland	✓	✗	✗	✓	✗
Portugal	✓	✗	✓[64]	✓	✗
Qatar	✓	✗	✓[65]	✗	✗
Romania	✓	✓	✓	✓	✗

[63] While there is no mandatory-reporting requirement specific to ISPs, Article 231-I of the Panamanian Penal Code establishes that anyone who has knowledge of the use of minors in pornography or sexual activities, whether the person obtained such information by means of his or her duties, job, business, profession, or by any other means, and fails to report it to the authorities, he or she will be sent to prison for this omission. If the commission of the crime (child pornography or sexual activity) cannot be proved after the report, the person who reported it will be exempted of any liability with regards to his or her report to the authorities. E-mail from Isabel Fernández, Embassy of Panama, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Apr. 12, 2006) (on file with the International Centre for Missing & Exploited Children).

[64] It can be inferred from Article 172 of the Portuguese Penal Law that the expression "by any means" allows a Prosecutor to view information and communication technologies as a means to commit the crime of circulating images, sounds, or movies clearly showing minors younger than 14 years old engaged in sexual acts. Letter from Pedro Catarino, Ambassador, Embassy of Portugal, Washington, D.C., to Ernie Allen, President and CEO, International Centre for Missing & Exploited Children (Feb. 22, 2006) (on file with the International Centre for Missing & Exploited Children).

[65] Article 292 of the Penal Code of Qatar specifically mentions "books, publications, **other written materials**, pictures, photographs, films, symbols, or **other items**." *Emphasis added.*



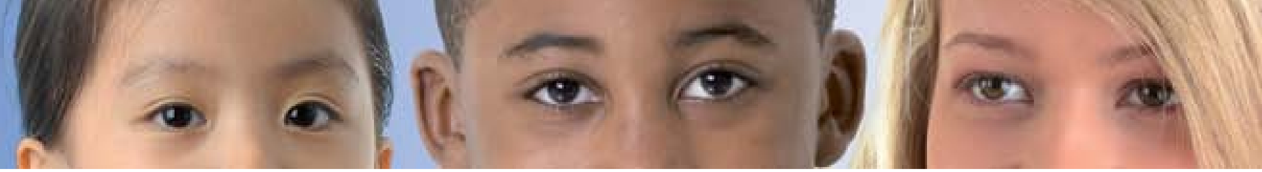
Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Russia	✓	✗	✗	✗	✗
Rwanda	✗	✗	✗	✗	✗
St. Kitts & Nevis	✗	✗	✗	✗	✗
St. Lucia	✗	✗	✗	✗	✗
St. Vincent & the Grenadines	✗	✗	✗	✗	✗
San Marino	✓	✗	✓	✗	✗
Sao Tome & Principe	✗	✗	✗	✗	✗
Saudi Arabia	✗	✗	✗	✗	✗
Senegal	✗	✗	✗	✗	✗
Serbia	✓	✗	✓[66]	✗	✗
Seychelles	✗	✗	✗	✗	✗

[66] Article 111a of the Serbian Penal Code criminalizes making a "photograph, film, or **some other picture**" of a minor for the purpose of making an item of pornographic content. Additionally, Article 185 criminalizes using a minor for producing "pictures, audio-visual, or **other items** of pornography content." *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Sierra Leone	✗	✗	✗	✗	✗
Singapore	✗	✗	✗	✗	✗
Slovak Republic	✓	✓	✓	✓	✗
Slovenia	✓	✓	✓[67]	✗	✗
Somalia	✗	✗	✗	✗	✗
South Africa	✓	✓	✓	✓	✓
Spain	✓	✗	✓[68]	✓	✗
Sri Lanka	✓	✗	✗	✓	✗
Sudan	✗	✗	✗	✗	✗
Suriname	✗	✗	✗	✗	✗
Swaziland	✗	✗	✗	✗	✗

[67] Article 187(2) of the Penal Code of Slovenia criminalizes the abuse of a minor “to produce pictures, audio-visual, or **other items** of a pornographic nature”; Article 187(3) criminalizes the actions of anyone who “produces, distributes, sells, imports, exports, … or supplies [pornographic material depicting minors] in any other way, or who possesses such material with the intention of producing, distributing, selling, importing, exporting, or supplying it in **any other way**.” *Emphasis added.*

[68] Article 189(1)(a) of the Spanish Penal Code criminalizes using a minor “to prepare **any type** of pornography material”; Article 189(1)(b) criminalizes producing, selling, distributing, displaying, or facilitating the production, sale, dissemination, or exhibition, of “any type” of child pornography by “any means”; and Article 189(7) repeats the “any type” and “any means” language previously used. *Emphasis added.*



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Sweden	✓	✗	✓[69]	✓	✗[70]
Switzerland	✓	✓	✓	✓	✗
Syria	✗	✗	✗	✗	✗
Tajikistan	✓	✗	✗	✗	✗
Tanzania	✓	✗	✗	✗	✗
Thailand	✗	✗	✗	✗	✗
Timor Leste	✗	✗	✗	✗	✗
Togo	✗	✗	✗	✗	✗
Tonga	✓	✓	✓	✓	✗
Trinidad & Tobago	✗	✗	✗	✗	✗

[69] Swedish criminal legislation is, in principle, formulated so that it will apply regardless of technical prerequisites. The criminalization of child pornography is no exception and accordingly, Chapter 16, Section 10a, of the Swedish Penal Code extends to computer-facilitated offenses. Letter from Anette Nilsson, First Secretary, Embassy of Sweden, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 23, 2006) (on file with the International Centre for Missing & Exploited Children).

[70] In 1998, Sweden enacted the Bulletin Board System (BBS) Liability Act (1998:112), which aims to prevent the spread of child pornography by obligating BBS providers to supervise BBS content. BBS providers are also obligated to remove or in some other way prevent the dissemination of messages with a criminal content, including those with child pornography. Letter from Anette Nilsson, First Secretary, Embassy of Sweden, Washington, D.C., to Jessica Sarra, Director of Global Operations, International Centre for Missing & Exploited Children (Feb. 23, 2006) (on file with the International Centre for Missing & Exploited Children).

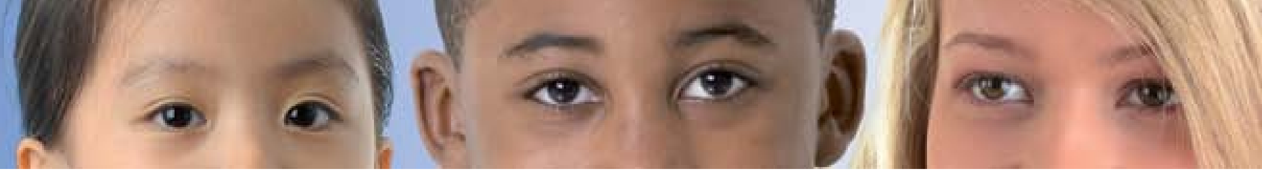
Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Tunisia	✓	✗	✓[71]	✗	✗
Turkey	✓	✗	✗	✓	✗
Turkmenistan	✗	✗	✗	✗	✗
Uganda	✗	✗	✗	✗	✗
Ukraine	✓	✗	✓	✗	✗
United Arab Emirates	✗	✗	✗	✗	✗
United Kingdom[72]	✓	✓	✓	✓	✗[73]
United States	✓	✓	✓	✓	✓
Uruguay	✓	✗	✓[74]	✗	✗
Uzbekistan	✗	✗	✗	✗	✗

[71] Article 234 of the Tunisian Penal Code criminalizes, inter alia, the use of "any visual recordings or photographs" depicting pornographic images of children.

[72] For the purposes of this report, the United Kingdom includes England and Wales.

[73] The United Kingdom operates a voluntary "notice and takedown" procedure overseen by the Internet Watch Foundation (IWF), an independent industry-funded body, endorsed by the police and government. U.K. ISPs "take down" images of child pornography when notified of them by IWF. Failure to do so could make them liable to prosecution. Letter from Tony Lord, First Secretary, Justice & Home Affairs, Embassy of Great Britain, Washington, D.C., to Ernie Allen, President and CEO, International Centre for Missing & Exploited Children (Feb. 9, 2006) (on file with the International Centre for Missing & Exploited Children).

[74] Law 17.815 of the Oriental Republic of Uruguay criminalizes certain child-pornography offenses regardless of how they are committed (*i.e.*, Article 1: "in any way makes or produces child pornography"; Article 2: "in any way facilitates the commercialization, diffusion, exhibition, storage, or acquisition of child pornography").



Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Vatican City	✗[75]	✗	✗	✗	✗[76]
Venezuela	✓	✓	✓	✗	✗
Vietnam	✗	✗	✗	✗	✗
Yemen	✗	✗	✗	✗	✗
Zambia	✗	✗	✗	✗	✗
Zimbabwe	✗	✗	✗	✗	✗

[75] In the absence of specific child-pornography legislation, such cases may be delegated to the Italian judiciary system at the request of the Holy See.

[76] "The Holy See has no Internet Service Provider external to it and the navigation from the internal provider has filters which impede not only access to any sites related to child pornography, but also online distribution of pornographic material. Given that the Holy See's web site is institutional, only those issues which are inherent to its mission…can be found there." Letter from Archbishop Pietro Sambi, Apostolic Nuncio, Apostolic Nunciature, United States of America, to Ernie Allen, President and CEO, International Centre for Missing & Exploited Children (June 5, 2006) (on file with the International Centre for Missing & Exploited Children).

Appendix 3

Child Safety Software

There are many software packages and technical tools available on the market that can help screen out unwanted and undesirable content and contacts, help limit the amount of time a computer can access the Internet or limit the applications which can run on a particular computer or device. Some operating systems also include such tools as part of their standard provision. Typically these functions will underpin or supplement the key safety messages that are common to Internet safety campaigns in all parts of the world. Safety software of this type is widely used in schools and public libraries, and is similar to those that employers may deploy on their internal networks to limit inappropriate or non-work related use of the Internet during working hours.

The effectiveness of child safety software can vary enormously and in some countries efforts have been made to introduce a "seal of approval" to give a basic level of quality assurance that will help parents, teachers, children and young people to choose a programme that best meets their needs and is likely to work in an efficient and easy to understand way.

It should always be noted that, sooner or later, every device will fail and that software can malfunction. To that extent parents, teachers, children and young people should never entirely delegate their responsibilities to safety programmes. Such programmes should always been seen as complementary to sound education and awareness programmes designed to ensure that a child or young person knows how to avoid online hazards, or knows how to deal with them should they arise.

Examples of currently available child safety software packages include:

Free Products

1. K9 Web Protection (http://www.k9webprotection.com/)
2. SafeFamilies (http://www.safefamilies.org/download.php)
3. File Sharing Sentinel (http://www.akidthaine.com/)
4. B-Gone (http://support.it-mate.co.uk/?mode=Products&p= bgone)
5. The latest versions of Windows and Mac OS also include tools which can be used without any further payment

Commercial Products

- Net Nanny Parental Controls
- Safe Eyes
- CYBERsitter
- WiseChoice.net
- CyberPatrol
- MaxProtect
- FilterPak
- Netmop
- imView
- McAfee Parental Controls
- Norton Parental Controls
- Child Safe
- ContentProtect Security Appliance
- http://www.cybersentinel.co.uk/

For a more detailed list of both commercial and free products see www.getnetwise.org.

Appendix 4

Developing a National Strategy

The Internet has made possible a range of ways of abusing children and young people, e.g., via web cams and chat rooms, which were simply impossible before its arrival as a mass consumer product. The internet has also played a singular role in expanding the scale on which CAM has become available in all parts of the world. For these reasons, when addressing online safety concerns for children and young people policy makers may wish to give particular consideration to some or all of the following:

1. Outlawing "grooming" or other forms of remote enticement of legal minors into inappropriate sexual contact or sexual activity.

2. Outlawing the possession, production and distribution of CAM, irrespective of the intent to distribute.

3. Taking additional steps to disrupt or reduce the traffic in CAM, for example by establishing a national hotline and by deploying measures which will block access to web sites and Usenet Newsgroups known to contain or advertise the availability of CAM.

4. Ensuring that national processes are in place which ensure that all CAM found in a country is channelled towards a centralised, national resource.

5. Developing strategies to address the demand for CAM particularly among those who have convictions for such offences. It is important to build awareness of the fact that this is not a victimless crime: children are abused to produce the material being viewed and by intentionally viewing or downloading CAM one is contributing directly to the abuse of the child depicted and one is also encouraging the abuse of more children to produce more pictures.

6. Building awareness of the fact that children can never consent to being sexually abused, whether for the production of CAM or in any other way. Encourage people who use CAM to seek help, while at the same time, making them aware that they will be held criminally responsible for the illegal activity in which they engaged/are engaging.

7. Ensuring that law enforcement crime prevention strategies as well as school-based and social programmes include sections on cybersafety and the risks posed by online predatory behaviour, with age appropriate advice.

8.Considering other strategies to address the demand for CAM. For example, some countries maintain a register of convicted sex offenders. Courts have issued judicial orders banning such offenders from using the Internet altogether or from using parts of the Internet which are frequented by children and young people. The problem with these orders hitherto has been one of enforcement. However, in some countries consideration is being given to integrating the list of known sex offenders into a block list which will prevent those on it from visiting or joining certain web sites, for example web sites known to be visited by large numbers of children and young people. Of course if the offender joins a web site while using a different name or fake log-in the effectiveness of such measures can be greatly reduced but by criminalising this behaviour a further deterrent can be established.

9. Providing appropriate long-term support for victims. Where children or young people have been victimized online, where for example an illegal image of them has appeared on the Internet, they will naturally feel very concerned about who might have seen it and what impact this will have on them. It could leave the child or young person feeling vulnerable to bullying or to further sexual exploitation and abuse. In that context it will be important for there to be professional support services available to support children and young people who find themselves in these circumstances. Such support may need to be provided on a long-term basis.

10. Ensuring that a mechanism is established and is widely promoted to provide a readily understood and rapid means for reporting illegal content or illegal or worrying online behaviour e.g. a system similar to that which has been established by the Virtual Global Taskforce, http://www.virtualglobaltaskforce.com. The use of the INTERPOL i24/7 system should be encouraged.

11. Ensuring that a sufficient number of law enforcement officials are appropriately trained in investigating Internet and computer-based crime and have access to appropriate forensic facilities to enable them to extract and interpret relevant digital data.

12. Investing in training for law enforcement, prosecutorial and judicial authorities in the methods used by online criminals to perpetrate these crimes. Investment will also be needed in acquiring and maintaining the facilities necessary to obtain and interpret forensics evidence from digital devices. In addition it will be important to establish bilateral and multilateral collaboration and information exchanges with relevant law enforcement authorities and investigative bodies in other countries.

Photo credits: www.shutterstock.com, Violaine Martin/ITU, Ahone Ayeh Njume-Ebong/ITU

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int/cop

Printed in Switzerland
Geneva, 2009

With the support of:

Child Helpline International

unicri
advancing security, serving justice,
building peace

International Centre
FOR MISSING & EXPLOITED CHILDREN

CHIS