Guidelines for Industry on Child Online Protection

www.itu.int/cop

ACKNOWLEDGEMENTS

These Guidelines have been prepared by ITU and a team of contributing authors from leading institutions active in the ICT sector. 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 Marco Obiso (ITU)
- John Carr (Children's Charities' Coalition on Internet Safety)
- Natasha Jackson and Jenny Jones (GSMA)
- Nerisha Kajee and Rob.Borthwick (Vodafone)
- Giacomo Mazzone (EBU) based on documents provided by Marc Goodchild & Julian Coles (both from the BBC)
- Michael Moran (Interpol)
- Brian Munyao Longwe (AfrISPA)
- Lorenzo Pupillo and Rocco Mammoliti (Telecom Italia)

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

Foreword

Executive Summary 1

Guidelines for Industry 2

- Key areas for consideration by the Whole ICT industry
- Key areas for consideration by Broadcasters
- Key areas for consideration by Internet Service Providers
- Key areas for consideration by Mobile Operators

1. Background 6

- Collaborating as an Industry

2. Classifying Content and Services 8

- Broadcasters

Case Study: British Broadcasting Company (BBC) – United Kingdom **10**

- Internet Service Providers

Case Study: MySpace's "Big Six" safety practices for social networking services **17**

Case Study: Wireless Content Guidelines Classification Criteria – USA **19**

3. Content Control Mechanisms 21

Broadcasters
Internet Service Providers

Case Study: Telecom Italia and the Protection of Children, Italy 26

Mobile Operators
Age-Verification mechanisms
Parental Controls

Case Study: NTT DoCoMo Parental Controls – Japan 31
Case Study: ATT MEdia™ Net Parental Controls – USA 31

4.Customer Communications and Education 32

Broadcasters

Case Study – CBBC Media Literacy Skills, UK 33
Case Study – Once Upon a Cyberspace Series, MDA and Okto, Singapore 35

Internet Service Providers

Clarity about nature of content, Terms and Conditions, Acceptable Use Policies Awareness raising through specific web areas dedicated to the Internet threats and the available tools for children protection Collaboration, through on-line report forms Information for parents and teachers Education of children on safer Internet use

Using Terms and Conditions

Mobile Operators

Case Study: Wireless Application Service Providers' Association (WASPA) Code of Conduct relating to Premium SMS – South Africa 45

Case Study: Vodafone "Top Tips" for Parents – UK 45

Case Study: Using Customer Communications to Support Efforts to Combat Spam and Scam SMS 46

5. Illegal Content 48

Terms and Conditions, User Guidelines

Notice and Take Down (NTD) processes

Case Study: Abuse Desk Service and Notice and Take-Down Approach - Telecom Italia 50

Hotline Organisations

Industry Collaboration

6. Other Issues 52

User Generated Content: The Broadcaster Approach

Case Study: How Broadcasters Can Protect Cchildren Against Inappropriate, Non-in House Material: the Example of BBC 55

7. Conclusions 56

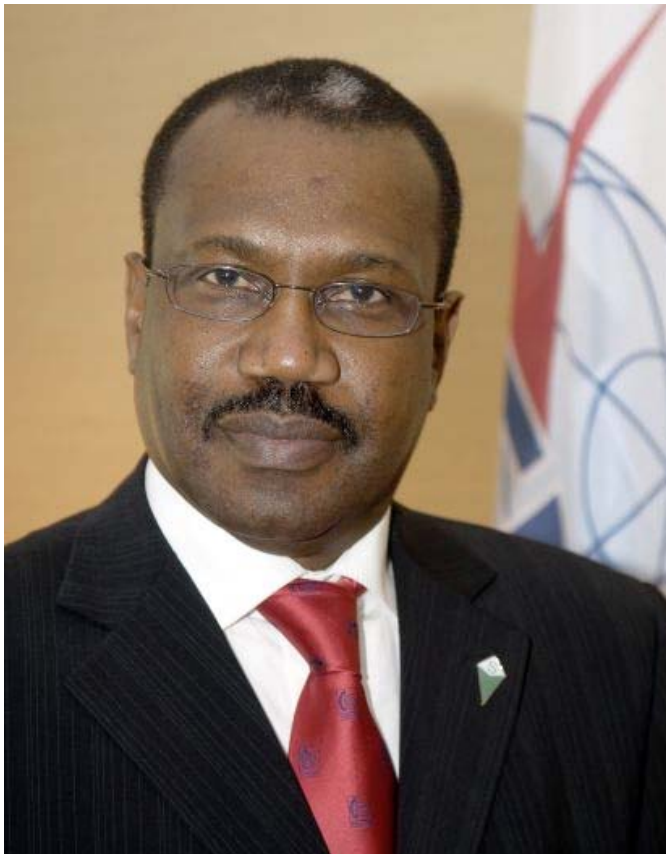
8. Further Information and Reading 58

Children and young people can benefit greatly from being online, but they also face increasing dangers in cyberspace.

As a result, a global response is needed from all segments of society in order to address what has become a global issue.


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

Foreword

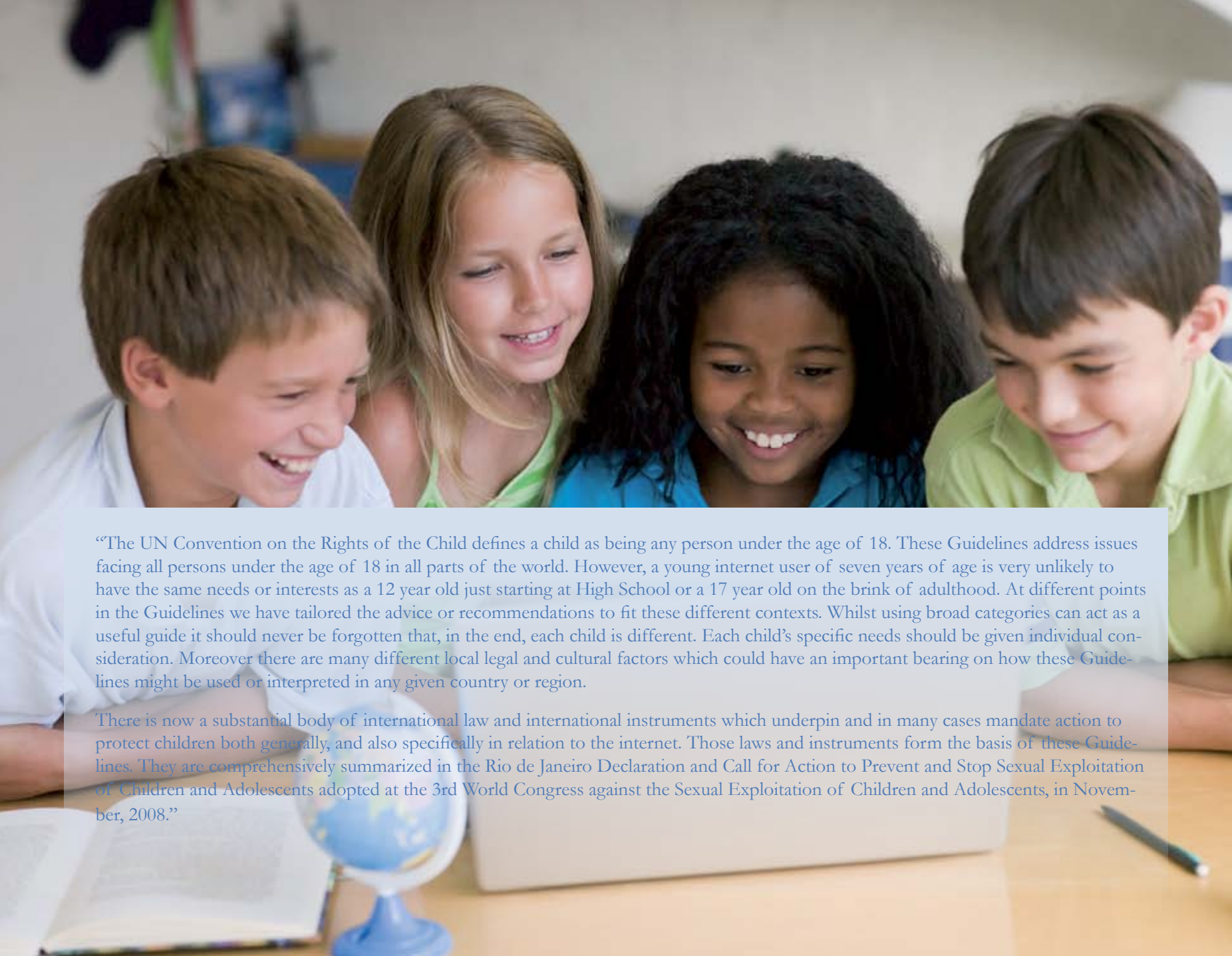


I welcome this opportunity to share with you these preliminary guidelines which have been developed with the invaluable help of multiple stakeholders.

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.

Industry players – whether broadcasters, ISPs, or mobile operators – 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)



"The 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 seven 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 we 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. Each child's specific needs should be given individual consideration. 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 underpin and in many cases mandate 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."

Executive Summary

These Guidelines have been prepared in the context of the Child Online Protection (COP)[1] Initiative in order to establish the foundations for a safe and secure cyberworld not only for today's children but also for future generations.

The information presented in these Guidelines has been developed by ITU and a team of contributing authors from leading institutions active in the ICT sector, namely, the GSMA, Interpol, Afrispa, the EBU, Telecom Italia, the Children's Charities' Coalition on Internet Safety and Vodafone.

The range of partners brought together to collaborate in the production of this document is itself a testament to the rapid changes which have been happening around the Internet as the digital revolution continues to pick up speed.

Convergence is now an established reality in many countries, and there is no doubt that it is bringing with it a host of new challenges. Cooperation and partnership are the keys to progress. No one sector of the industry has a monopoly on knowledge or wisdom. We can all learn from each other.

ITU, together with the other authors of this report, is calling upon all stakeholders to promote the adoption of policies and standards that will protect children in cyberspace and promote their safe access to online resources.

It is hoped that this will not only lead to the building of a more inclusive information society, but also enable Member States to meet their obligations towards protecting and realizing the rights of children as stated in the United Nations Convention on the Rights of the Child, adopted by UN General Assembly resolution 44/25 of 20 November 1989 and the WSIS Outcomes Document.

[1] www.itu.int/cop

Guidelines for Industry

This section provides guidelines for industry on child online protection. In order to formulate a national strategy focusing on online child safety, industry leaders should consider the following strategies in the areas mentioned below:

		Key areas for consideration
ICT Industry as a Whole		There is an urgent need for a common action that goes beyond individual ICT organizations. These include:
	1.	Developing interoperable standards and related recommendations to protect children online. The aim would be to develop a widely shared approach which could be promoted across the whole industry.
	2.	Evaluate what options and possibilities exist for real global coordinated and consistent action to protect children online. Attention should be given to the elaboration of those capabilities (e.g. watch and warning and incident management) that would facilitate the gathering of threats and information sharing among different players.
	3.	Identify the commonalities that span the different sectors (broadcasters, Internet, mobile) with the purpose of developing Codes of Conduct, or code of practices to help ITU Member States collaborate more effectively with the private sector/industry.
	4.	Establish cooperative arrangements between government and the private sector/ industry for sharing information and developing specific capabilities aimed at mitigating the risks and extending the potential of ICT usage by children.

		Key areas for consideration
Broadcasters	5.	Developing common rules regarding complaints systems. The aim would be to avoid a situation where external complaints functions are added to broadcasters' own internal systems and potentially create more confusion with users or risk overloading police and other agencies with a large number of queries which their services are not designed or equipped to handle.
	6.	Developing common standards and recommendations. The aim would be to develop a widely shared approach to protecting children online. This would be promoted across the whole industry.
	7.	Establish a pan-industry project to produce more robust procedures for obtaining parental consent for their children accessing age sensitive content at least on regional basis.
		Key areas for consideration
Internet Service Providers (ISPs)		The following recommendations provide guidance to the Internet Industry & Internet Service Providers (ISPs) to support a safer environment for young users. Each of the areas for consideration below should be included as part of a larger focus on user protection by responsible online providers.
	8.	The strategic objectives for the Internet Industry for child Internet safety should be to reduce the availability of and restrict access to harmful or illegal content and conduct. ISPs should also equip children and their parents with information and easy to use tools to help manage their use of the Internet in ways which minimize the potential dangers.
	9.	On Internet sites and on Web 2.0 services, language and terminology should be accessible, clear and relevant for all users, including children, young people, parents and caregivers, especially in relation to the site's Terms and Conditions, privacy policy, safety information and reporting mechanisms.
	10.	Reporting concerns, abuse and illegal behaviour: It is very important for Service providers to have in place robust procedures for handling complaints. In particular, complaints about harassment and inappropriate content should be assessed speedily, and, if appropriate, the offending content should be removed promptly. To the extent possible, service providers should consider having mechanisms, such as links to report abuse or flag profiles that may be inappropriate or that place the child or young person at risk, in place, and should be able to escalate any report to law enforcement if necessary.

		Key areas for consideration
	11.	Service providers should consider making the ability to report a default presence on all web pages and services offered by the ISPs by means of a "report abuse button" to the extent possible. A common, recognisable button could be developed which will be always in the same location on every screen. The reporting mechanism could be enhanced by offering technical solutions to the reporting user such as the ability to attach screen shots, connection statistics, running process lists etc, as well as by informing the user what information they need to include with any report to make it effective.
	12.	Service providers should consider emphasising, in accessible and easily understood language, 'what behaviour is and is not acceptable on the service', particularly for young users and for their parents and caregivers. It is suggested that this information should be provided in addition to its inclusion in the Terms and Conditions.
	13.	Service providers should continue to evaluate the effectiveness of technologies that identify and verify the age of customers. The goal should be to implement a suitable solution appropriate to their individual service (this will be particularly important where the service in question is subject to legal restrictions based on age), to the extent that the solution is legally and technically feasible, and most importantly creates a safer, more secure Internet services. Such solutions might variously seek to prevent under age access and exposure to age-inappropriate content or services, or work to keep services provided exclusively for children adult-free. .
	14.	Service providers should consider proactively communicating with local or national law enforcement agencies to report illegal child abuse at soon as the provider is aware of it. They should have additional internal procedures in place within their organisation to ensure that they comply with their responsibilities under local and / or international laws with regard to illegal content. They should also consider actively assessing commercial content hosted on their own servers (either branded content or content from contracted third party content providers) on a regular basis to the extent possible in order to ensure that illegal or potentially harmful content is not accessible through their network. Tools such as hash scanning and image recognition softwares are available to assist with this. .

		Keys areas for consideration
Mobile Operators		The following is a "checklist" of suggested areas for mobile operators to consider when reviewing their approach to child protection, both in terms of providing a safe and appropriate mobile environment for their younger users and in terms of combating the potential misuse of their services for the hosting or distribution of illegal child sexual abuse content:
	15.	If offering content and services that are not age-appropriate for all users, ensure that content is classified in line with national expectations, is consistent with existing standards in equivalent media, and is offered together with age-verification, where possible
	16.	If possible, work with other operators in your market to agree and promote a set of industry-wide commitments on offering age-sensitive content appropriately.
	17.	Provide tools which enable access to content to be controlled by the user or a parent/ caregiver. Again, these should be consistent with national expectations and standards in equivalent media.
	18.	Clearly signpost the nature of content and services offered, so that users are empowered to make informed decisions about their content consumption and any commitment (e.g. minimum subscription period) that they may be undertaking
	19	Support parents in understanding the full range of mobile content services that their children may be using so that they can guide their children towards appropriate mobile usage
	20.	Educate customers on how to manage concerns relating to mobile usage generally – including areas such as Spam, theft, and inappropriate contact e.g. bullying – and ensure that you offer customers a means of raising any concerns
	21.	Use your customer Terms and Conditions to explicitly state your company's position on the misuse of its services to store or share child sexual abuse content, and its commitment to support investigations by law enforcement of any abuse consistent with national legislation; have Notice and Take Down (NTD) - or equivalent - processes in place; support national hotlines or equivalent, where they exist..

1. Background

Today's digital world has transformed individual lifestyles the world over. The computing industry has long been all-digital, the telecommunications industry is almost fully digital and the broadcasting sector is well on the way to becoming digital. Always-on Internet access has become the norm, with people spending more and more time consuming digital media than any other medium.

Daily lives from China to Italy are brimming with SMS, e-mail, chats, online dating, multiplayer gaming, virtual worlds and digital multimedia.

Although these technologies mean added convenience and enjoyment for many, regulators and users alike are often one step behind the fast-paced innovations in this field.

Moreover, as the number of channels for service delivery diversifies, the sector's traditional and less traditional businesses face a number of new dilemmas.

Collaborating as an Industry

In the converging media world of today traditional distinctions between different parts of the telecommunications and mobile phone industries, between Internet companies and broadcasters, are fast breaking down or becoming irrelevant. Convergence is drawing these hitherto disparate digital streams into a single current that is reaching out to billions of people in all parts of the world. Against this background the ITU, in collaboration with

GSMA, Telecom Italia, European Broadcasting Union, Interpol, Children's Charities' Coalition on Internet Safety, Vodafone and Afrispa, has prepared these Guidelines for Industry on Child Online Protection. Its aim is to provide a common framework for all parts of the industry to work towards the shared goal of making the Internet as safe as possible for children and young people, for example, by producing codes of conduct or authoritative sources of advice and guidance.

Internet Service Providers in particular have long accepted that they have a distinct responsibility with regards to child online protection. This is largely due to the fact that ISPs act as both a conduit, providing access to and from the Internet, and a repository because of the hosting, caching and storage services which they provide. The same is true for the mobile phone networks, many of whom now extend their functionality well beyond the original business of connecting voice and data exchanges. Broadcasters similarly have become major players in the Internet space, providing many of the online services which previously were only associated with ISPs or online hosting companies. However, because of their enormous brand presence, typically established for many years prior to the arrival of the Internet as a mass consumer product, broadcasters' sites frequently attract enormous followings.

Each of the sectors working together in this collaborative project brings its own history and its own particular areas of expertise. By working together in this way, by pooling that knowledge and experience, the industry as a whole is delighted to be able to advance the wider promotion of a safer Internet for everyone, but above all for children and young people.

2. Classifying Content and Services

The notion that not all content and services are suitable for a universal audience is well-understood in the "offline" world – for example, films and games have age-ratings, and TV programmes with content of a violent or sexual nature are subject to time-based restrictions.

Where online content is exactly the same as the "offline" version (e.g. a game or film which differs solely in terms of the access channel), it is possible to re-use existing ratings or classifications. However, where content is new or modified, online content and service providers have to find methods of communicating the nature of that content and the target age-range to their customers.

With more traditional content (e.g. video clips) it is often possible to apply an age-rating by benchmarking standards against existing frameworks from equivalent national – or potentially regional, depending upon the degree to which social sensitivities are shared - media, such as games or films. However, the growing range of exciting interactive services including message boards, chat rooms, social networking and user generated content services, whilst being harder to "classify" in the traditional sense, can also pose potential risks to younger users relating not just to the consumption of age-inappropriate content, but also inappropriate conduct (e.g. bullying) and contact (e.g. grooming).

All of these issues are dealt within the sub-sections below. The Broadcasters sub-section deals with the issue of making traditional content available through a new medium, the Internet Providers sub-section looks at the content, contact and conduct issues relating to managing non-traditional online services, and the Mobile Operators sub-section provides an overview of how operators across the globe are approaching the issue of classifying and managing mobile content and services.

Broadcasters

Television broadcasters have traditionally been able to use the linear 'broadcast' nature of television viewing to manage concerns about age-sensitive content through time-based scheduling – for instance, by broadcasting content that is only suitable for older teenagers or adults later in the evening or at night (after the "watershed"), when younger children will be asleep.

However, as broadcasters increasingly make their content available online on a non-linear "on demand" basis, where direct parental supervision cannot be relied upon and time-based scheduling no longer applies, broadcasters have been exploring ways to make their content available in an age-appropriate fashion.

Research indicates that in general parents want to know about the types of content that may cause concern (such as strong language or violence) rather than being presented with simple age ratings.

Because of this, some broadcasters have developed a labelling system e.g. the BBC developed the 'G' for Guidance labelling system where a 'G' is displayed when a piece of content contains challenging material and the nature of the content is spelt out in text alongside the programme synopsis. The presence of the 'G' is used to trigger parental PIN control systems, if enabled.

Note: unless otherwise stated, the term 'broadcasters' in this document refers specifically to providers of traditional broadcast-type content, in the sense that the 'broadcaster' has creative and editorial control over the content made available, whether 'on air' or, as is the focus of this document, online. The term is not intended to include providers of services which enable the publishing of content created by others – such organisations fall within the Internet Service Providers category.

Case Study: British Broadcasting Company (BBC) – United Kingdom

Through its iPlayer proposition, which provides online access to BBC programming on a non-linear (or "on demand") basis and also currently contributes 9% of total Internet traffic in the UK, the BBC has build up significant experience in managing the responsible delivery of age-sensitive content.

On the current BBC iPlayer, installation is restricted to those aged 16 and over – Users are also informed about PIN protection during the registration process and have to make a decision about whether to enable it there and then. If they choose not to, they are told how they can enable it later. If a programme is not suitable for a universal audience (i.e. all ages), it carries a Guidance warning – in this case, a 'G' sign and text label explaining the nature of the content are displayed at the point the user decides to download the content. At the point of viewing, the text label is also displayed and the user has to enter their PIN number, if enabled, before they can view the content. Anyone using the iPlayer without the correct PIN code receives an explanatory message stating that they do not have permission access to the 'G' rated content.

The BBC will shortly introduce streamed content to the iPlayer and, where appropriate, programmes will also display the 'G' and text label before content can be viewed. A PIN protection system will be available from launch and the BBC is currently looking into ways to strengthen this even further as streaming and downloading are integrated into one system.

The BBC's 'G' for Guidance system has also been adopted by other terrestrial broadcasters in the UK including ITV, Channel Four and FIVE for their online On Demand offerings.

The BBC has a very clear strategy of supporting children from birth through to early adulthood, with three sites that reflect the varying age-appropriate levels of protection, computer literacy, independence and maturity as they grow up, as well as specific educational services offered by BBC Learning.

1. The CBeebies (www.bbc.co.uk/cbeebies) and CBBC (www.bbc.co.uk/cbbc) websites enable children and their parents or carers to interact with us and each other in a safe, trusted and accessible environment. The sites provide high quality, engaging and relevant interactive content and experiences for children, as well as acting as a springboard to the best appropriate external websites for the under-12s.

2. The focus is on empowering children and giving them the opportunity to gain a deeper relationship with the BBC, the brands and characters,

increasing the value they receive, the ownership they feel, and the impact they have on CBeebies and CBBC. To achieve this, the sites offer a range of innovative interactive tools and creative opportunities aimed at all British children, of every ability and background, giving them the space to publish their own content, thoughts and opinions. We also provide a dedicated 24/7 news service for children online as part of Newsround and through the PressPack section we can actively engage children in the topical issues that matter to them.

3. BBC Switch provides an online space for all teenagers, with content aimed at engaging young people, addressing their interests, and encouraging interaction. The site contains both supporting TV and radio programmes and free-standing content. (www.bbc.co.uk/switch)

4. BBC Learning provides output for school-aged children across a broad range of subjects and skills. The following are linked to curriculum or specific skills.

Bitesize – revision and recap service for all major subjects for children aged 5-16 (www.bbc.co.uk/schools/ks3bitesize)

Blast – creative development for teenagers, currently focused on creative arts, including partnership with youth arts organisations (www.bbc.co.uk/blast)

Some services are designed for use in the classroom; others are increasingly used directly by learners at home or at school, without the need for tutor mediation.

The BBC works closely with Ofcom (the UK's media and telecommunications regulator) and a number of broadcasters and platform providers to promote best practice on labeling; the BBC has also been an active participant in the BSG Content Information Group. The BBC is also an associate member of the Association for Television on Demand (ATVOD), the self-regulatory body for On Demand services.


Social
Networking

Internet Service Providers

Generally Internet content and Web 2.0 services are terms referring to the increasing use of the Internet by individuals to create and distribute their own content, in audio-visual as well as in written form. Specific examples of Web 2.0 services include:

- **User generated content** sites such as wikis, blogs and image-sharing sites, which are designed specifically for users to upload, share or view content.
- **Social networking sites** where users display their personal 'profile', including information such as where they live, interests and tastes (for example in music, films or books) as well as photos or videos, music tracks and links to friends' profiles. They may also include facilities for chat, file sharing, blogging and discussion groups.
- **Online communities and social worlds** where participants select, customise or create characters, called 'avatars'. Their avatars can build houses, furnish environments, interact with others and even exchange virtual money while purchasing and selling items in a multi-player virtual world.
- **Online gaming** where players play with other, often in complex and extensive 'game worlds' and where they can interact and talk to each other during play.

Frequently, these categories overlap and these networking sites are increasingly being seen as part of youth culture, as reported in the complete and independent UK review looking at the risks to children on the Internet and in video games.

It can be useful to make distinctions between potential risks based on "content", "contact" and "conduct", according to a structure put forward by EU Kids Online project[2]. With Web 2.0 and with the relevant increasing interactivity, communication is now possible on one-to-one, one-to-many and many-to-many bases. This clearly increases concerns about unwanted contact and, in some cases, illegal conduct. Making the distinction between contact and conduct is useful in order to understand differences, overlapping and possible countermeasures. The key distinction is that: 'contact' refers to a situation in which the child is the receiver of the communication/message (the 'victim'); whereas 'conduct' refers to a situation where the child is the instigator of the inappropriate behaviour (the 'perpetrator')[3]. Other commentators have added a further two categories which it is worth bearing in mind: "commerce" – which refers to the possibility of children and young people being exploited by

[2] www.eukidsonline.net/

Note: Sections on Internet Service Providers discuss approaches available to the Internet industry as a whole. This includes Internet access providers, as well as electronic service providers / providers of content and services – these are referred to collectively in this document as Internet Service Providers (ISPs). As such, it should be noted, that not all recommendations will be applicable to all ISPs.

[3] Safer Children in a Digital World: the report of the Byron Review, (http://www.dcsf.gov.uk/byronreview/).

unscrupulous companies that take advantage of young people's inexperience or it refers to problems such as phishing where, again, younger people might be more vulnerable; finally there can be issues of "addiction", which refers to the way in which some children and young people can become obsessively engaged with technology in such a way as to present an obstacle or a barrier to them developing normal relationships with other people or taking part in healthy physical activities.

From the Internet Industry point of view, there are three key strategic objectives for child Internet safety, which require industry and parents/caregivers to take joint responsibility for increasing children's safety online:

- **Reduce Availability**: reduce the availability of harmful and inappropriate content, contact and conduct (industry);
- **Restrict Access**: equip children and their parents with effective tools to manage access to inappropriate content (industry and family);
- **Increase Resilience**: build children's resilience to the material to which they may be exposed; equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children (parents).

An important consequence of the nature of the Internet is that there is no obvious single point at which editorial control can be exercised, unlike broadcast media where the channel exercises editorial control. Editorial controls exist (e.g. moderators of user generated content sites) but they are widely dispersed across the 'Internet value chain'. This value chain contain content producer, content aggregator, Internet Service Providers (ISPs) and Web host, search, directory and web providers, consumer device, etc.

At each point of the value chain, there are a range of technical tools that can help parents manage their children's access to the Internet (e.g. parental control software, safe search, and age verification on websites).

An example of the role of Internet Industry working in co-operation with families is the following:

1. User generated content websites take down harmful and inappropriate material uploaded to their sites.
2. Children and parents report harmful and inappropriate material to host websites when they find it.
3. ISPs block access to illegal material such as child abuse images.
4. Parents install software to filter out harmful and inappropriate content.

5. Websites provide clear and easily visible advice about how to stay safe.

6. Parents talk with their children and children talk with their friends and siblings about e-safety.

Reducing availability:

The objective of reducing availability of harmful and inappropriate content, contact and conduct can be met by service providers undertaking the following:

- Adopt an effective **moderation process** of user generated content – for example, MySpace conducts a post-upload review of every image and video posted on its site
- Base the moderation process upon reports from the user community - responding effectively to reports from more than one user, and from long-standing users (based on their level of activity or rating or reputation they have been given by other users), can help create an active community which "self-polices" and seeks to keep themselves and others safe online.
- Provide a mechanism for reporting inappropriate content, contact or behaviour as outlined in their Terms of Service, Acceptable Use Policy and / or User Guidelines - mechanisms should be easily accessible to users at all times and the procedure should be easily understandable and age-appropriate. Reports should be acknowledged and acted upon expeditiously. Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled.
- Link reports of abuse to "Notice and Take Down" processes – with a public service level agreement on the response or take down times.
- Avoid harmful or inappropriate **advertising content online.**

Restricting access:

The objective of restricting access to in appropriate content can be dealt with in the following ways:

- **Parental control software**, which enable parents to manage their children's access to Internet resources.
- **Safer Internet tools**, including parental controls, ideally would allow the following types of categories: White Lists, Content filters, Usage monitoring, Contact management, Time/ program limits.
- Deliver new computers or Internet services access with **parental control software enabled by "default"**, linked to prominent safety messages which explain what the default settings do.

- Adopt **"safe search"**: most search engines offer a safe search option, which does not return results containing images or keywords which would be considered inappropriate for children.
- Adopt appropriate age verification methods to prevent children accessing age-sensitive content, sites or interactive services, such as chat rooms, etc. where risks of inappropriate contact and conduct exist.
- **Content labelling**: Providers of professionally produced content (i.e. games, broadcast-style editorially controlled content) should provide a clear external label describing the content on their sites to indicate its suitability for children.
- **Network level blocking**, where, on a national-based criteria, some material on the Internet, such as child abuse images, is clearly illegal.

Increasing Resilience:

Increasing the resilience of children in managing risks is an important objective and is interdependent and complementary with the other two objectives of reducing availability and restricting access.

Although parents and children have a role in reducing the availability of harmful and inappropriate material (e.g. by reporting abuse to host sites), this is mainly a task for industry. And although industry does have a role in building children's resilience (e.g. by providing safety advice), parents and others working with children are likely to have the most impact here and so have the greater responsibility.

These overlapping, but differing, roles for industry and families across the three objectives are very important and suggest a need for a national-base and shared strategy to keep children safe online, that is capable of influencing and empowering both industry and families.

By looking at the strengths and weaknesses of existing arrangements to improve child Internet safety, and looking to the different country-based existing laws, the Internet Industry can usefully develop self-regulatory national Code of Practices; these Codes would be more transparent than good practice guidelines, provided that the body that oversees/coordinates them is effective in monitoring them and publishing the results. Mechanisms could also be developed within these frameworks to give parents and children a voice.

Mobile Operators

As growing numbers of mobile operators offer their customers access to a rich and compelling range of content services, including games, music, video and TV programming, they are faced with the challenge of how to manage customer access to commercial content which would have been subject to age-

Case Study: MySpace's "Big Six" safety practices for social networking services

- **Image and Video Review:** Sites should find ways to review hosted images and videos, deleting inappropriate ones when found.
- **Discussion Groups Review:** Social networking sites should review discussion groups to find harmful subject matter, hate speech, and illegal behavior, deleting that content when it is found.
- **Removing Registered Sex Offenders:** Social networking sites should ban registered sex offenders from setting up accounts on their sites using technology that already exists today.
- **Meaningful Efforts to Enforce Minimum Age Requirements**: Sites should enforce their minimum age requirements and take steps to identify and remove underage users who have misrepresented their age to gain access.
- **Protection for Younger Users From Uninvited Communication:** Social networking sites should implement default privacy settings that prevent adults from contacting teens under 16 who they do not already know in the physical world.
- **Cooperation with Law Enforcement:** All sites should have law enforcement hotlines available at all times to assist law enforcement during emergencies and on routine inquiries.

restrictions if accessed through different channels.

The increasing range of new community and interactive services available to users also come with concerns about users' age. For example, many major Social Networking Sites have minimum age-requirements stated in their Terms of Service, as there are concerns that younger users face risks – such as identity theft or inappropriate contact – relating to posting too much information about themselves, and so on.

In order to provide a shared and transparent approach, mobile operators and content providers in a number of countries are responding to this challenge by working together to agree classification systems. The classification systems are typically designed to manage commercial mobile content – i.e. content which mobile operators produce themselves or where they have a commercial involvement with third parties – and are based on accepted national standards and consistent with approaches taken in equivalent media (e.g. games, film).

Indeed, where possible content classifications from other industries should be re-used. An example might be of a film or film trailer or a PC game (assuming that the images are repeated in the re-purposed for mobile version) so that customers' experiences of the same content are consistent across national media.

However, given the practical challenges involved in mobile operators establishing the age of the end user, a number of markets (for example, Australia, Denmark, New Zealand) have currently committed to operating a simple two-tier classification system: content which is suitable for adults only, and other / general content.

For example, the Australian code has simply mapped across criteria and ratings from the existing Classification Board to the 'restricted' (adult 18-rated) and 'unrestricted' (general) categories used in the mobile arena, while operators in the USA - under the auspices of their trade association, CTIA - have created a grid which maps existing standards from TV, film, music and games into either the 'Cellular Accessible' (general) or 'Cellular Restricted' (18-rated) categories, the results of which are summarised by the CTIA as follows:

This binary approach allows the sale of a full range of legal commercial content by mobile operators and third parties whilst meeting national acceptability tests; it ensures that the area of greatest risk is managed, and also reflects that the age of majority is the point at which it is most practical to age-verify (for example, through presence on the electoral role or credit card ownership).

Some markets, however, are moving towards a more granular approach. Germany has

Case Study: Wireless Content Guidelines Classification Criteria USA

adopted a three-tier system for classifying commercial content which is broadly based on the German 'FSK' film classification system:

- General content / services: available to all by default
- 16-rated content / services: available to all by default, parents can choose to apply a block
- 18-rated content / services: blocked by default to all users, adults must be age-verified

In France, a recommended four-tier classification system ('all users', 12-rated, 16-rated, 18-rated), created in consultation with a broad spectrum of stakeholders under the auspices of Le Forum des droits sur l'Internet, was announced in

Mobile content will be classified as Restricted Carrier Content or Generally Accessible Carrier Content based on existing criteria used to rate movies, television shows, music and games.

Content is generally considered "Restricted" if it contains any of the following restricted content identifiers:

Restricted Carrier Content:

- Intense Profanity
- Intense violence
- Graphic depiction of sexual activity or sexual behaviors > Nudity
- Hate speech
- Graphic depiction of illegal drug use
- Any activities that are restricted by law to those 18 years of age and older, such as gambling and lotteries

Any content that has not been classified as "Restricted Carrier Content" will be considered "Generally Accessible Carrier Content" and will be available to all consumers.

Further details of the Wireless Content Guidelines can be found on the CTIA website: http://www.ctia.org/advocacy/index.cfm/AID/10394

October 2006. The four different levels will facilitate the handling of challenges relating to managing access to interactive services and user generated content – much of which is suitable for older teens but is neither 'adult rated' nor is it appropriate for younger teens and children.

To access 18-rated content, users will have to age-verify; the 12-rated and 16-rated tiers will correspond to two levels of parental controls as follows:

- Contrôle parental de premier niveau: blocks access to 16-rated commercial content, user-generated / interactive services that facilitate meetings (e.g. dating sites), the Internet.
- Contrôle parental renforcé: blocks access to 12-rated and 16-rated content, all user-generated / interactive services, the Internet.

Content classification systems are either defined by the operator community itself or outsourced to a third party organisation with relevant expertise. Many countries (including Denmark, Malaysia, Singapore, and New Zealand, for example) have simply defined the classification boundaries within or as an appendix to their national Code of Practice itself.

Others, including France above, have had classification criteria defined through a third party organisation. The UK's two-tier classification system was launched by the industry-funded Independent Mobile Classification Body (IMCB: http://www.imcb.org.uk/) in 2005. In addition to formulating the classification criteria, the IMCB can provide advice or act as an arbiter in (the extremely rare) disputes over classification of individual items of content.

It should be noted that not all content classification systems relate to age-sensitivities: Malaysia and Singapore use a binary content classification system based on existing national standards, however this is based on 'acceptable' versus 'unacceptable' content, and there is no distinction based on age.

Shared content classification systems simplify self-classification for content partners and therefore reduce costs and increase efficiencies for the industry as a whole. They also make the classification system more transparent for customers, particularly for third party services promoted independent of the operator portal (for example, in magazines), and allow for the consistent introduction of tools such as pre-determined adult short codes for premium SMS services, which can facilitate the implementation of age controls.

3.

Content Control Mechanisms

Providers of online content and services are developing a range of approaches for enabling the age-appropriate control of content in the online world. These include mechanisms to restrict access to content until the user has proven his or her age ("age-verification") as well as controls made available to parents to enable them to place restrictions on their child's consumption of online content and services.

Broadcasters

Broadcasters offer a range of content and services online, including some which is only suitable for users above a certain minimum age. To ensure that younger users are only consuming age-appropriate content and services, broadcasters use a range of techniques such as:

- Single Sign On processes – For example, at BBC online services, when children sign up to the message boards, they are asked to provide their date of birth. This is then used to determine whether they are old enough to access the service – and they are not able to change the original date of birth at a later date if they discover that certain content is unavailable to them because of their age.

Note 1: mechanisms to combat the presence of illegal online content, in particular child sexual abuse content, are discussed separately in the next section.

Note 2: more detailed information regarding broadcasters and user generated content can be found in section 6.

- Parental Consent via email - For example, the BBC is presently engaged in a range of trials to review the use of parental consent by email, and a registration system that would allow parents to decide what activities their children could engage in on PSB websites and what level of reporting they would receive. The BBC is also reviewing what rules should apply for teenagers up to 16, and whether they should have access to greater levels of interaction before they need to ask for parental consent".
- Many public service broadcasters, at the moment, whilst waiting for better regulation[4], have adopted a more drastic approach on the web, than on their air-waves. RAI Italy, for instance, has a restrictive policy and doesn't publish on its web sites any content that has not received the "clearance for all the family" classification, (distinguishable by a white butterfly). All content with a yellow butterfly (to be seen with an adult) or a red one (restricted only to adults) are not currently available on the Internet.

Internet Service Providers

It is important for Internet Service Providers to offer controls which prevent access to certain types of content and service.

In many countries the national law will specify that certain types of content, or services should not be made available to children (ie. those users who are below the legal age of majority / adulthood). Where such content services are being offered on commercial terms by ISPs, a method for verifying adult status should be implemented. Alternatively if the law does not require it, there may be well-established expectations that children and young people should not be able to access adult content. In that connection ISPs and others may wish to consider developing or using age-verification systems as a means of ensuring legal compliance.

Internet Service Providers should keep in mind that simple click-through age-confirmations, which require the user to state they are over 18, are not reliable because they rely solely on the user's integrity.

However, it is also important to be aware that even solutions which seek to confirm the age

[4] It is worthwhile to note that the BBC has expressed some caution about how to allow users to activate a "red button" if they come across material that is harmful, explicit or worrying to them. The main concern is that in by having too many options, this may drive users to other less reputable, unregulated sites. It is essential that broadcasters maintain their reputation as a safe environment and so ensure that critical safety alerts are not off-putting.


“
The industry is demonstrating commitment to developing a responsible approach to children’s use of online ICT and communications
”

of the user – for example, by requiring credit card or ID details – cannot be entirely guaranteed: an underlying concern for all age verification methods is that identity verification on the Internet is difficult because it is virtually impossible to know whether the individual user supplying the information is indeed the individual whose information is being supplied. Although a user may provide certain information when registering with a website, there is no efficient or effective way to ensure that this information has been entered truthfully. For example, the use of government-issued national ID cards with associated PINs cannot necessarily be relied upon for age-verification as these details are often known by others (e.g. family members).

Such approaches could also potentially infringe on the user's right to privacy – for example, ID cards disclose personal details (e.g. date of birth) beyond those which are strictly necessary to confirm that the user is above the age of majority.

ISPs are becoming increasingly creative about managing challenges relating to age-sensitive content. For example, MySpace requires in its Terms and Conditions of service that all users are 13 years or older and, to combat a situation where a user under the age of 13 lies about his or her age, employs a search algorithm, using terms commonly used by underage users, to find and delete underage profiles. MySpace's site is scanned for such terms and the database of search terms is updated to reflect changes in user behaviour and terminology.

Many major Internet Access Providers now offer parental control solutions which help parents to manage which sites, content and services their child can access.

Case Study: Telecom Italia and the protection of children – Italy

To allow children and adolescents to surf the web safely, Telecom Italia has taken steps to inhibit content that offends their psycho-physical integrity, described on the Group's portal[5], and has provided its customers with protective services and instruments, capable of fostering safe surfing[6].

The most important tool for children is the software **Alice's Magic Desktop** which is a simplified operating system, running on normal PCs. Alice Magic Desktop allows children to use PCs and the permitted Internet functionalities in a secure, amusing and educational way, under the granular and detailed control of the parents. The targets for this service are children of 10 years and under.

The principal characteristics of the product are:

- **PC protection** from improper use by the children (avoiding damage of files, configurations, installed software of the parent, etc.);
- **Safe Internet surfing**, based on a white list of preferred websites provided by the parent;
- **Email client**, specific for children, with a dedicated Graphical User Interface and a pre-defined address book by the parent;
- **Web games and tools** for children, dedicated to playing, learning and use a lot of instructive materials;
- **Global Parental Control** Interface, that allow to the parent to control and to define the children's "walled garden".

The safe environment can be used by the children in a very easy way, with different desktop themes, a personalized Internet browser ("My first Browser") where the child can only visit the "preferred" web sites approved by the parent; a Magic email program with which email coming from not allowed email addresses are posted to a "quarantine" folder for parent's verification prior to being passed to the child.

Source: Telecom Italia

In addition, Telecom Italia, in order to comply with the very restrictive national Italian Law[7] about child protection, and to ensure a global response for the security and safety of citizens who use its commercial services, has launched a programme of close collaboration with the Italian police forces and with the specialized National Center for combating Child Pornography Online (CNCPO)[8], by making highly specialized technological infrastructure available and implementing a filter system to block sites communicated by CNCPO.

[5] www.telecomitalia.com, Sustainability->Hot Topics-> Protection of Children and Abuse

[6] Alice Total Security and Alice Magic Desktop, http://adsl.alice.it/servizi/index.html

Moreover, in order to combat and prevent the diffusion of child sexual abuse content (child pornography) and protect children, Telecom Italia has made a helpline/reporting mechanism available on the web for reporting illicit content encountered by users while navigating the Internet. These reports, which can be made anonymously and by filling out a web standard form, are analysed and promptly forwarded to the Postal Police (CNCPO), which will investigate the alleged crimes since this type of activity is entrusted exclusively to police force.

Although parental controls solutions are improving all the time, they cannot be expected to provide complete safety – however, in conjunction with teaching children responsible Internet practices (see Customer Communications and Education, below), parental controls can help provide younger users with a safer online experience.

Mobile Operators

Mechanisms for controlling access to age-sensitive content fall broadly into two categories:

- Age-verification mechanisms
- Parental controls

Age-verification mechanisms

The "age-check" tools available to more traditional retailers and broadcasters of media and content are not readily transferable to the mobile content environment. For example, with mobile content there is no opportunity to do a visual check at the "point of sale", such as can be used in cinemas and shops; nor, given the personal nature of the mobile device, can mobile operators rely on parental supervision in the same way that TV broadcasters have traditionally been able to do.

However, a number of operators across the globe are addressing this challenge through the development of age-verification systems. To date, these typically focus on age-verifying adults who wish to have full access to all content and services. It should be noted that where operators are offering commercial content and services that are subject to legal age-restrictions this is of particular importance.

[7] Italian law 38/2006, to combat the sexual exploitation of children and pedopornography, including over the Internet; Italian Legislative Decree 70/2003, which regulates e-commerce and ask Telco Operators such as Telecom Italia to provides reporting to the competent authorities of cybercrimes involving the network infrastructure and child's sexual abuse notices; EU Convention on Cybercrime, signed at the Council of Europe on 23 November 2001, ratified in Italy with Law 48/2008

[8] http://www.poliziadistato.it/articolo/10232-Centro_nazionale_per_il_contrasto_alla_pedopornografia_sulla_rete

Different operators are taking different approaches to age-verification, based on leveraging existing options such as:

- National ID schemes
- Credit cards
- Tax / fiscal codes
- Electoral rolls
- Face-to-face ID check in-store or through e.g. post office
- Contract status / existing relationship with billpayer

Once age-verified at adults, users are either given an 'adult PIN' which needs to be entered whenever the user wishes to access adult-rated content or services, or an 'adult profile' is applied to their account and any restrictions on content and services are removed.

Due to the difficulties of verifying age prior to adulthood in the virtual / 'online' environment, operators enable parents to control younger users' access to content and services through the application of parental controls rather than attempt to verify the age of every end user.

Parental Controls

Whilst age-verification mechanisms mean that operators are proactively implementing systems to ensure that individual customers are above the minimum age required to access given items of content, parental controls rely upon parents taking the initiative and applying parental controls as they deem appropriate for their child.

Many operators, from a range of countries, have already introduced parental controls systems – some propositions focus purely on blocking access to age-inappropriate commercial content, others are combined with additional features such as time or spend controls.

With some exceptions, including operators in France, who have already allowed for two levels of access, and a few other operators across the globe who have developed different multi-tiered parental control, most systems tend to be either 'on' or 'off' options, with access to a set level of age-sensitive commercial content or services (e.g. 18 or 16-rated) blocked when switched on.

Most parental controls systems currently focus purely on commercial content, reflecting the area where the operator has the greatest degree of control and, therefore, responsibility. Operators in Japan use a black / white list approach to websites when parental controls are applied and some operators in other markets have Internet filtering systems in place, but most operators have to yet to introduce Internet filtering as part of their parental controls proposition.

As an interim measure, a number of operators are simply blocking access to the Internet when parental controls are switched on.

It is likely, however, that the growing trend towards using mobiles to access Internet-based services will speed the roll-out of Internet filtering tools.

Naturally, given the onus that is placed upon parents or caregivers to apply the controls, promotion and awareness-raising of this option is key to the overall effectiveness of the proposition in terms of protecting younger users. Similarly, operators must ensure that parents understand that they can only control content carried by their own networks

Other options for consideration include mobile operators installing parental controls on branded handsets as a default and, potentially, mobile phone manufacturers putting software on their phones which can empower parents to control usage and restrict who their child can contact, and who can contact their child.

Case Study: ATT MEdia™ Net Parental Controls – USA

AT&T's parental controls proposition is made available to customers free of charge. It enables parents to restrict their children's access via mobile to mature content as well as offering the option to restrict the purchase of downloads, such as games and ringtones.

Controlling Content: parents can set Content Filters to "On" or "Off." When the content filter is "On", access to sites with mature content (e.g. chat, dating) on AT&T's MEdia™ Net portal is restricted and access to the broader mobile Web via the search function is shut off. "Off" has no restrictions and all content is visible and accessible. The default content filter setting is "Off".

Controlling MEdia™ Net Purchases: parents can set Purchase Blocker to "On" or "Off." When the Purchase Blocker is "On" children will be prevented from purchasing premium content, including ringtones, downloads, games and graphics. "Off" allows all purchases. The default Purchase Blocker setting is "Off." .

Case Study: NTT DoCoMo Parental Controls – Japan

DoCoMo provides various levels of content filtering (e.g. 'Kids' i-mode filtering and i-mode filtering) plus a 'time restriction' option which can be used alone or in parallel with the other levels of content filtering. All three options are offered to customers free of charge:

1. Kids' i-mode filtering: allows access to sites on i-mode menu only (content providers on the i-mode menu are contractually forbidden from offering 'harmful content', including adult and sensitive content, gambling, violence, dating, chat services and discussions boards); the "Kids' i-menu", which contains sites specifically designed for children, becomes the default menu setting.
2. i-mode filtering: allows access to sites on the i-mode menu and also to independent sites which do not contain harmful content.
3. Time restriction: prevents access to any site (whether i-mode or independent) between 22.00 and 6.00.

4. Customer Communications and Education

In order to enable users to make informed decisions about the content and services they may choose to use, as well as empowering parents and teachers to guide children and teenagers towards a safe, responsible and appropriate online experience, telecommunications and content companies are increasingly investing in education and communication programmes.

This section provides a range of potential approaches taken by providers of online content and services.

Broadcasters

Broadcasters who make programmes that are popular with children and younger users are likely to have a correspondingly younger online "audience", and therefore have a particular responsibility for promoting messages about keeping safe online.

Broadcasters are also well-positioned to exploit the popularity of their content to deliver simple messages that will help younger users fight issues such as "cyberbullying" or invasion of privacy.

Other approaches that can be adopted by broadcasters include encouraging children to seek parental consent before using particular services. When creating a user account, children can be advised to ask their parents' permission, and make sure that their parents are aware that they will be using services such as message boards. The Terms and Conditions of use can also make it clear that children should have a parent or guardian's permission before using message boards.

If a child posts a message which suggests that their parents don't know or don't want them to use broadcasters on/line communities, usually the webmaster will message the user making it clear that they must have parental/guardian permission to use the message boards.

Some organisations require parental verification by return email for added security. However, for instance, the BBC's own user testing experience suggests that many children share their parents' email addresses which would undermine the efficacy of the system, and that a proportion of BBC audience only access CBBC through after school clubs, either because they don't get that support at home or because they don't have access to the Internet.

Therefore, a tick-box solution or email verification is not sufficient to acknowledge that an informed parent / guardian / teacher is actually monitoring the child's activities and does little to help those children who fall on the wrong side of the digital divide. Some pan-industry exploration into more robust parental consent procedures that are socially inclusive and not open to abuse is welcomed in this area.

Internet Service Providers

The Internet industry has a responsibility to review the role and importance of communicating with customers in terms of:

- **Clarity** about nature of content, Terms and Conditions (T&Cs) and Acceptable Use Policies (AUPs);
- **Awareness raising**, through specific web areas dedicated to Internet threats and the available tools for children protection;
- **Collaboration**, through on-line reporting forms;
- **Information** for parents and teachers about child online safety;
- **Education** of children on safer Internet use;

These areas are each dealt with in greater detail below.

Clarity - *about the nature of content, Terms and Conditions, Acceptable Use Policies*:

ISP are increasingly recognising the importance of communicating clearly about the nature of contents and services, so that all users – including younger users – can make informed decisions about their consumption.

Clarity for Internet Industry means:

- Signposting age-sensitive content;
- Communication with regard to pricing of content, terms of subscription, how to cancel subscriptions, and so on;
- Definition and communication of clear Acceptable Use Policies, and Terms and Conditions;
- Definition and updating of policies to comply with any relevant national code, as regards safer use of Internet by younger teenagers and children.

Awareness raising - *through specific web areas dedicated to the Internet threats and the available tools for children protection*:

ISPs can facilitate the raising of awareness concerning children's protection by displaying clearly visible information about safe use of the Internet and about tools for children's protection on their website. This specific web area would be intended to::

- Promote awareness and discussion about Internet threats and the protection of children , and the tools available for them to use, such as blocking and privacy settings;
- Share online security tips for users;
- Contain educational resources;
- Describe the national and international regulatory background;
- Provide customer with information about available tools for children' protections (parental control, etc.).

ISPs can also contribute to customers' awareness by adopting a self-regulatory code that allows minor protection through specific rules and tools, and also by applying a visible brand that certifies the adhesion to the code.

Collaboration - *through on-line report forms*:

In order to combat and prevent child sexual abuse content and protect children, ISPs should:

- Offer a space available on the web for reporting illegal content encountered by users while navigating the Internet; these reports could be made anonymously by filling out a standard form;
- Provide customers with details of how to report safety concerns;
- Promptly contact the relevant police / law enforcement agency, which will investigate the alleged crimes; the ISPs customer services staff should be equipped to handle and forward customer reports to the appropriate authority.

Information *for parents and teachers:*

Service providers are realizing that it is very important to provide parents and teachers with the necessary information to understand how their children are using ICT services (e.g. including issues such a bullying) and be well-positioned to guide them towards responsible usage.

- Parents and teachers should be made aware of all Internet risks in order to better protect their children. Messages should be positive and empower parents to take action.
- This information should be transmitted through multiple media channels as many parents do not use Internet services. For example through collaborating with school districts to provide on line safety curricula for children and educational materials for parents. Where possible, ISPs should also promote national support services where parents and carers may report and seek support in the case of abuse and exploitation.

Parents and teachers should:

- Educate themselves about the Internet and the ways in which their children use it, as well as about technology in general;
- Explore and evaluate the effectiveness of available technological tools for their particular child and their family context, and adopt those tools as may be appropriate;
- Be engaged and involved in their children's Internet use;
- Be conscious of the common

risks youth face to help their children understand and navigate the technologies;

- Be attentive to at-risk children in their community and in their children's peer group;
- Recognize when they need to seek help from others.

Education *of children on safer Internet use*:

For "baby navigators" the virtual world is a useful and amusing resource, but it is also a place where they can access material that is not suitable for them.

Children' use of the Internet varies with their age and level of development; on their own the youngest are unable to understand the advantages and dangers of navigating on the web, so it is preferable that they are accompanied at all times by an adult (parent and/or teacher), who can assist and guide them in the choice of content, as well as helping to establish appropriate rules of behaviour for them to follow.

For adolescents, however, the task is more difficult. They are more independent and more informed about the opportunities offered by the web, often knowing much more than their parents and teachers about software for the Internet, instant messaging, chat-rooms, and online games, etc. Nonetheless, it is a good idea for parents to lay down rules for them, as well and to teach them to be vigilant, well-mannered and responsible while they are navigating.

It is also very important that ISPs provide information directly to children on safer Internet use. Children should be educated on how to detect and respond to inappropriate behaviour. The following is a suggested check-list of advice for ISPs to provide to their younger users:

- "Never give away your physical contact details";
- "Never agree to meet anyone you have met online in person, especially without consulting an adult first";
- "Do not respond to inappropriate (bullying, obscene, or offensive) messages and save the evidence, don't delete it";
- "Tell an adult if you are uncomfortable or upset about something or someone";
- "Never give away your account password or username; and be aware that other players may give false information about real-world characteristics."

Where possible, ISPs should also promote national support services where children may report and seek support in the case of abuse and exploitation.

Using terms and conditions

It is very important that ISPs and the Internet industry in general highlight the "Terms and Conditions" (T&Cs) pages of the Internet services they provide, with a clear policy for any breach of T&Cs. For example, typical messages of "Terms and Conditions" pages note that the customer must not use the website or the service to:

- Upload, post, transmit, share, store or make available any content that could be harmful, unlawful, defamatory, infringing, abusive, vulgar, obscene, invasive of privacy or public rights, hateful or racist;
- Impersonate any person or entity, or falsely the age, the affiliation with any person or entity;
- Upload, post, transmit, share, store, make available on the websites any private information relating to any third party, including addresses, phone numbers, email addresses, credit card numbers;
- Solicit personal information from anyone under 18, including, but not limited to: name, e-mail address, home address, phone number, or the name of their school;
- Upload, transmit, share any materials that contains viruses;
- Upload, post, transmit, share or make available content that would constitute, provide instruction for a criminal offence, violate the rights of any party or any local, state, national or international law;
- Harm or exploit children in any way;
- Stalk, defame, defraud, intimate, degrade an individual or group of individuals for any reason, including on the basis of age, gender, disability, ethnicity, race, religion or sexual orientation;

Terms and Conditions should be supported by a clear statement of the company's policy with regard to any infringement – typically, including messages such as the following:

- [Company X] has adopted a policy of terminating accounts of those customers who are deemed to be repeat infringers. It reserves the right to review and remove user-created services and content at will and without notice and delete content and accounts;
- [Company X] may also, at its sole discretion, limit access to the sites or terminate the membership of any users who infringe the rules.

ISPs should echo key messages from their Terms and Conditions in user-friendly language in community guidelines and 'reminders' that sit within the service itself – for example, by reminding users of the types of content which are considered inappropriate at the point of uploading content.

Mobile Operators

Education and customer communication play a key role in ensuring that children and younger users can enjoy an age-appropriate and safer mobile experience.

Operators are increasingly recognising the importance of communicating clearly about the nature of content and services on offer, so that all users – including younger users – can make informed decisions about their consumption. This includes signposting age-sensitive content, but also requires clarity of communication with

Case Study: Wireless Application Service Providers' Association (WASPA) Code of Conduct Relating to Premium SMS – South Africa

The WASPA Code contains a number of commitments specifically providing for clear communication with customers. Examples of these commitments include the following:

- **Promotional material for all subscription services must prominently and explicitly identify the services as "subscription services"**
- **Once a customer has subscribed to subscription service, a notification message must be sent to the customer containing the following information:**

a) The cost of the subscription service and the frequency of the charges;

b) Clear and concise instructions for unsubscribing from the service;

c) The member's contact information.

- **Subscription customers must be sent a monthly reminder message containing the same information listed in (a, b, and c above)**

The full Code of Conduct can be found on the WASPA website: http://www.waspa.org.za

regard to pricing of content, subscription terms and how to cancel subscriptions, and so on – not least because lack of absolute clarity in this area risks younger users in particular inadvertently signing up for a subscription, for example, when they originally intended to buy a single ringtone.

As with other media, mobile operators cannot take full responsibility for ensuring that children and teenagers use their mobile devices appropriately – parents, caregivers, and educators all have a role to play as well. The challenge is that parents are often less aware of the capabilities of new mobile devices than children themselves, so educating this demographic is key.

Case Study: Vodafone "Top Tips" for Parents – United Kingdom

As part of its child safety customer education initiatives, Vodafone devised a high level "top tips" pocket guide for parents. The guide provides recommendations on a number of areas including chat, games, premium rate services and bullying.

The following "top tips" relate to downloading content on mobiles:

- **Discuss with your child what services they use on their mobile, for example they might download ringtones, wallpaper or games directly from their mobile.**
- **Find out whether they share any downloaded content with friends.**
- **Discuss with your child the types of content you would be unhappy for them to download, receive or share with others.**
- **Stress the importance of not responding to any messages from strangers, or messages that are funny, or offer to sell products cheaply. These are invariably, 'too good to be true'.**
- **Make sure any phones which have had the Content Control bar lifted are kept away from children**
- **You can reapply the content control bar by calling Vodafone Customer Care on 191, visiting a Vodafone retail store or on-line at www.vodafone.co.uk**

The "Staying in Touch: A Parent's Guide to Mobile Phones" top tips can be downloaded at: http://online.vodafone.co.uk/dispatch/Portal/SimpleGetFileServlet?dDocName=VD007645&revisionSelectionMethod=latestReleased&inline=0

To this end, a number of operators have invested in education programmes and guidelines targeting parents and covering a full range of relevant issues, such as:

- Content and services: explaining to parents the types of service now available

(e.g. explain what are social networking sites? What are Location Based Services? How is the Internet accessed via mobile?) and, where relevant, the options available to parents to apply controls;

- Inappropriate contact: how to avoid "stranger danger"; what to do if their child is being bullied through so-called 'cyber-bullying' or SMS;
- Steps to take if a phone is stolen or if your child is receiving spam;
- Managing privacy – not sharing information online, keeping profiles on SNS private, etc.

By educating parents, operators are empowering them to guide their children towards safe and responsible usage of mobile services themselves. Some operators have joined together with other players in their markets to produce and promote shared parents guides (e.g. France[9], Ireland[10]) whilst others promote their own company guides to their customers specifically.

Equally, raising awareness of the availability of parental control tools is vital, particularly in markets where they are not applied by default. In recognition of this, operators are increasingly communicating about parental controls options on websites, in-store, through bill inserts and by offering parental controls at point of sale as part of the sales process.

Operators are also engaging with younger users directly through online education programmes and partnerships with NGOs in their local markets, as well as indirectly by providing teachers with resources to educate and inform pupils about appropriate usage - see, for example, the Teach Today (www.teachtoday.eu) website which was created by a consortium of mobile and Internet providers in Europe.

As content and services grow ever richer, all users will continue to benefit from advice and reminders about the nature of a given service they are using and how to enjoy it safely. For example, many operators also build community guidelines into their interactive services (e.g. chat rooms) reminding users of appropriate and safe behaviour – for example, by reminding users not to give out their contact details, and so on (see "Education of Children " in the Internet Providers section above for further examples). Similarly, as a matter of best practice, many operators will now send out regular reminders to users of Location Based Services (LBS) which post their location, letting them know that the service is on and reminding them how to change their profile or turn the service off.

[9] http://www.sfr.fr/media/pdf/offre-sfr/maj-240107/att00013578/701.09Guideparents2007.pdf
[10] http://www.vodafone.ie/download?id=ICIA_PARENTS_GUIDE.PDF

Case Study: CBBC Media Literacy Skills United Kingdom

CBBC (Children's BBC) has a media literacy section called Stay Safe, presented by an animated cartoon rabbit called Dongle. Research has shown that children of primary school age respond very well to the character. The section includes an interactive quiz, a 'pop video', and links to other resources such as 'thinkuknow'. The material covers online and mobile safety, and the content is built around the Stay Safe smart rules:

S = Keep Safe
M = Don't Meet Up
A = Accepting emails can be dangerous
R = Reliable? People may not be who they say they are.
T = Tell an adult if you feel scared or uncomfortable

The Stay Safe section is linked to from all the community pages and these messages are reinforced by the hosts as they encourage the right sort of behaviour from users. But it is important to note that although the SMART rules are widely used and recognised, several different versions of it are being used across the industry, which may confuse some children.

Case Study: Once Upon a Cyberspace Series, MDA and Okto, Singapore

Singapore's Media Development Authority (http://www.mda.gov.sg/) supported the creation of a series of six animations, telecast by MediaCorp's Okto channel over six weeks, which were designed to promote the benefits of the Internet and new media, whilst highlighting the need to be cautious online. The initiative was created in line with the Singapore government's focus to step up Cyber Wellness and Cyber Safety public education.

The animations target 10 – 14 year olds, and feature characters from well-known fairytales, but in a modern day setting and with storylines which revolve around new media and the Internet.

For example, in the first episode, Instant Messaging Little Red Riding Hood, Little Red Riding Hood comes online to find a message from an unfamiliar girl living in another part of the woods. Little Red Riding Hood starts chatting with the girl, and ends up saying that she's going to visit Grandma, and even reveals Grandma's address. The animation goes on to reveal that the 'girl' is in fact the Big Bad Wolf in disguise.

Outlines of the five other episodes – Snow White and Online Gaming, Pinocchio goes on a Blind Date, The Three Little Pigs and the Attack of the Internet Virus, Sleeping Beauty and her Mobile Phone, and The Big Bad Internet Bully – can be found on the MDA website: http://www.mda.gov.sg/wms.file/mobj/mobj.1334.Annex.pdf

Case Study: Using Customer Communications to Support Efforts to Combat Spam and Scam SMS

Customers, including younger teenagers and children, may encounter two forms of potential SMS scam which, with the correct information, can be readily managed.

SMS can be used to send a message inviting a call or message back to a premium rate service. A typically message might be: "Congratulations you have won a prize. Call XXX XXX XXX [a premium rate number] to receive more details". This type of scam or "micro-fraud" is designed to remove money from a phone user's pre-pay balance or account.

In a variation on phishing, customers may also be targeted via their mobile in identity theft scams. For example, a customer may receive a text message or voicemail which is ostensibly from the tax collector saying the individual is owed a rebate – and when the customer calls they are persuaded to divulge their bank details.

In such cases, operators should use education campaigns to help customers understand how to recognize, and therefore avoid being duped by, such scams (e.g. by knowing the national premium rate code and not calling numbers beginning with that code in response to an unknown source). Where available, operators should promote resources which keep an up to date view on current scams - see, for example, SCAMwatch (http://www.scamwatch.gov.au/) which is maintained by the Australian Competition and Consumer Commission, aims to "help you recognise, report and protect yourself from scams" and has a section specifically on "mobile phone scams".

The other key form of abuse is based on premium SMS used to offer subscription services. Subscription services are legimately offered for repeated transactions such as purchasing the same information service each week. Subscription SMS abuse is where an information service provider gives a customer the impression a charge is on a one-off or single payment basis, but it is for a repeat or subscription service. An example might be an advertisement in a magazine where the impression is a one off charge but the reality is of a subscription service. Customers should cancel further payments to the service

Where customers encounter scam SMS they should be able to complain to their network operator and /or to the national communications or premium rate regulator - for example by being able to forward SMS to a specific, published mobile number. Repeated complaints help industry to identify the unscrupulous providers and take appropriate action, ultimately making it unprofitable to engage in such practices.

By emphasizing the following

types of messages to their customers, operators can help to protect their customers from SMS spam and scams:

- Do not reply to invitations to call high-priced premium rate numbers - people who SMS you to call them use normal mobile numbers. Even if you do not recognize a calling mobile number you can avoid these scams by identifying and remembering the national premium rate codes in your country (they often begin with 09).
- Competition organizers do not send out winning notifications at random – if you do not recognize a competition notification it is probably a scam.
- If you purchase a ring tone or other service and find that you are being sent repeated tones you may have agreed to a subscription SMS scam. Cancel future payments (by referring to the original advertisement) and complain to your operator and to the relevant national regulator.
- Similarly, where operators have introduced additional mechanisms for reporting spam, these should be widely communicated to customers. Mobile operators in France, for example, have supported the launch of their SMS shortcode for consumers to report spam SMS with a dedicated website: http://www.33700-spam-sms.fr/

5. Illegal Content

With the same priorities in mind, the mobile operators from over 70 countries, and representing over 900 million customers, who have signed up to the GSMA Code of Practice on Spam have all committed to ensuring "that the processes they use to obtain consent [to receive a marketing message] are clear and transparent" and to providing customers with "obvious, clear and efficient means to opt-out of receiving further operator mobile marketing communications sent via SMS or MMS".

Communication is, of course, a two-way process, and many operators now provide options for customers to contact them to report issues or discuss concerns – whether these relate to the discovery of inappropriate content or contact on a mobile service, the theft of a mobile device, the receipt of spam or a request to apply / remove parental controls, with staff being trained to respond effectively.

As will be discussed below, correctly managing customer reports of potentially illegal content is a key part of combating the presence of illegal content, including child sexual abuse content, in the mobile environment.

All Internet providers (both fixed and mobile) must work with law enforcement authorities to execute their legislative obligations with regard to illegal content. However, many Internet service providers take advantage of additional approaches to help combat the misuse of their services for the illegal hosting and / or distributing of illegal content, including child sexual abuse content (child pornography). Common additional measures include:

- Term and Conditions and "User Guidelines" which explicitly forbid illegal activity;
- Notice and Take Down (NTD) or "cease-and-desist" processes;
- Working with and supporting national hotlines

Terms and Conditions, User Guidelines

Internet providers who offer interactive services which enable users to store and share content (e.g. photo albums, social networking sites), can use the Terms and Conditions of their customer contracts to make explicit their position on the misuse of their services for hosting or distributing illegal content, in order to underline their commitment to working with law enforcement and to reserve all appropriate rights, including the right to remove illegal content and freeze user accounts.

Many Internet providers also echo and re-emphasise the content of their Terms and Conditions in easy to understand, customer-friendly language within a set of "user guidelines" which outline the kinds of behaviour expected by users of their service. Such user guidelines can typically be accessed directly from the relevant service or at the point of creating a service account.

Service providers can also actively assess commercial content hosted on their own servers (either branded content or content from contracted third party content providers) on a regular basis, in order to ensure that illegal or potentially harmful content is not accessible through their network.

Notice and Take Down processes

Whether as a voluntary measure or as a legal requirement, "Notice and Take Down" (NTD) or "cease-and-desist" type processes are a key defence for operators and service providers seeking to keep their services free of illegal content: as soon as providers are alerted to their services being used to host illegal content, they then take steps to have it removed.

For NTD measures to work effectively there needs to be legal clarity on the nature of content which is illegal and law enforcement authorities (or delegated organizations) should be able to confirm where individual items of content are illegal.

Case Study: Abuse Desk Services and Notice and Take-Down Approach – Telecom Italia

In compliance with the applicable local and EU laws concerning child protection, prevention of cybercrime, and fight against child sexual abuse content (child pornography), Telecom Italia has created operational centres for handling abuses, known as Abuse Desks (specialized for different types of customer: retail, business and top client). These centres are the interface between users of services (and in general an Internet user) and the Company for the managing of abuses and the improper use of services.

With the specialized work done by the Abuse Desk's operators, Telecom Italia is able to manage different types of cyber-crimes, reporting all relevant facts or significant events to the competent local authorities, such as the presence of child sexual abuse content on the Group's networks or sites.

Two very important prevention schemes are in place: first, a NTD (notice and take-down) mechanism, where either customers or police notify to Abuse Desk Operators the illegal content or sites to be obscured, second, a web filtering system, used for all Telecom Italia networks, based on DNS and IP filtering methods, able to provide denial of access to a certain domain sites or to a list of different IP addresses; the DNS or IP lists to be blocked are provided in Italy by the public organization CNCPO (Centre National for combating Child Pornography On Line) and the lists are downloaded automatically each day.

Operators and service providers can adopt or support an Internet Abuse Desk, help lines or specialized websites, in order to manage, reduce or eliminate cybercrimes and illegal material on its web sites or infrastructures. In this manner, they can be notified of illegal content by customers, members of the public, law enforcement or hotline organisations (see below). If the report comes from a member of the public (e.g. via customer care), operators / ISPs pass information on to law enforcement or the national hotline as appropriate – for example, to confirm whether the content is illegal or to take any further legal action.

Hotline Organisations

By 1995, as the Internet began to grow in popularity, it became apparent to the industry, as well as to governments and law enforcement agencies, that the Internet was being used to publish and exchange illegal content, in particular child sexual abuse content. Discussions began as to the various means of combating this problem, including the creation of dedicated hotlines for people to report illegal online content.

The first hotline for reporting child sexual abuse content was set up in the Netherlands in June 1996 as a joint initiative between industry, government and law enforcement. This was followed by similar initiatives in Norway, Belgium and the UK.

Since then, many countries have created hotlines and INHOPE (the International Association of Internet Hotlines), an umbrella organisation for Hotlines, now has around 30 full member Hotlines from across the globe.

Beyond standard NTD approaches for managing illegal content hosted on operators' own services, supporting and promoting local hotlines provides customers and members of the public with means of reporting illegal content should they discover it, and is an important step towards helping to combat illegal content, including child sexual abuse content.

Industry Collaboration

There are also a number of collaborative industry initiatives – such as the Technology Coalition, the Financial Coalition Against Child Pornography and the Mobile Alliance against Child Sexual Abuse Content – underway. These initiatives bring together a number of leading players within each industry with the aim of sharing knowledge and developing technical expertise on new ways of combating the presence of online child sexual abuse content on behalf of the wider industry, including, for example, by blocking access to URLs known to contain child sexual abuse content.

6. Other Issues

User Generated Content (UGC): The Broadcaster Approach

This section outlines the approaches that Broadcasters can take in order to deal with User Generated Content (UGC) on their services.

To ensure that inappropriate content is not published on message boards, it is recommended that broadcasters put in place a number of procedures to protect online users against inappropriate User Generated Content. These are:

a) Automatic filters – inappropriate words can be blocked from user names and messages at the point of posting. This filter includes swearing, sexual terms and racist or homophobic language. Non in-house URLs can also be blocked, along with email addresses.

b) Pre-moderation – for instance, all message boards can be pre-moderated by a team of specialised children's moderators who screen for content that is in contradiction to the published House Rules. Each message can be checked before it is published, and moderators will also spot and flag suspicious users, as well as users in distress.

c) Hosting – in addition to the moderation team, there can be a team of community hosts. The community hosts manage message boards from the public perspective, and they can be the first point of contact for the moderators when they have concerns about a user.

All moderation should be performed by an office-based team who have undergone advanced checks to determine if they have existing criminal records from a single external agency. In addition, moderation teams can adopt the following rules:

- Working from home should not be permitted in order to ensure that no one has access to children's information.
- Moderation should be team-based so that moderators can share concerns about posts or users, and can build up their knowledge of users' behaviour as a group.
- Moderation should be performed according to strict moderation guidelines, built up over time.
- Moderators should have set hours and message boards should only be open within those hours. Therefore, when the boards are open for posting, there is always a moderator on duty.

However, this is a very labour-intensive process and the more popular and successful the community, the more resources it takes to moderate it.

The ultimate sanction is to block those who persistently disregard the published House Rules. However, in the future broadcasters may want to move towards a more "trust and reputation" based system so as to harness good behaviour and enable peers to teach best practice to each other by example.

Those who are key and central to the community would be rewarded for their good behaviour and disruptive members would have privileges removed. All submitted user generated content should be pre-moderated before it can go live.

Exclusive pre-moderated public chat sessions with, for example, children's favourite authors and presenters, are an incentive already in use for the target age group to participate in broadcasters online communities. Offering these exclusive events and other premium content discourages users from lying about their age and registering for services aimed at older users.

Increasingly, broadcasters' online services are encouraging users to send photos and videos as well as text. All these should be pre-checked in order to make sure that the material is suitable for publication on broadcasters' websites and to check that children do not publish sensitive personal information about themselves or others eg. school signs, road names, door numbers which could put them at risk, for example through 'jigsaw id'.

In particular, when videos are submitted by children, broadcasters should require the telephone number of a guardian or parent, to get formal adult consent before publication. (This is in line with TV policies and protects children, for example, against being traced by estranged parents who may have court orders against them).

Case Study: How Broadcasters Can Protect Children Against Inappropriate, Non-in House Material: the Example of BBC

All external content linked to via Cbeebies and CBBC is pre-approved by an editorial expert and put on a "green" list which can then be searched via BBC Search services.

Cbeebies specifically searches out content on the Cbeebies site and approved sub sites created by Independent producers supporting their own Cbeebies programming.

The CBBC Search tool is a more complex resource to help users find the best CBBC and Newsround content, as well as carefully selected sites from around the BBC and the wider web. All the sites must be editorially valuable and relevant to the 7-12 year old UK audience and must not:

- **Carry, link to or advertise pornographic material or other sexually explicit material (unless it forms part of tailored sexual education for this audience group)**
- **Carry, link to or advertise explicit violence or content inciting violent behaviour (including online games and game reviews with fighting, shoot 'em ups or other use of weaponry)**
- **Incite anything illegal**
- **Include discrimination of any kind**
- **Promote poor health / poor eating**
- **Use unsuitable language**
- **Exist solely to sell products or services**
- **Promote gambling**
- **Restrict features to paying subscribers**

BBC do not allow linking to any social networking sites from CBBC. If any external sites include message boards, they must be pre-moderated at all times. Is not possible to link to live chat rooms from BBC children's sites.

The CBBC search database is constantly checked with an automated tool which 'sweeps' all the sites in the database, looking for changes according to key words e.g. 'message boards' or 'chat room'. If such changes are detected, the site is flagged to a researcher, who checks the site again for suitability, and removes it from the database if necessary.

Similarly, PSB Switch operates a rigorous policy when it comes to protecting the users from inappropriate content online. Whilst Switch's presence on third party sites is a key part of the offer to teenagers, allowing Switch to reach out to an audience that may not always be very familiar with the PSB offer, all ventures in this space are fully moderated and carefully monitored. BBC include prominent links to features about online safety wherever possible and never link to live chat rooms from Switch.

7. Conclusions

For ISPs and other online providers to engage effectively in the Child Ondine Protection Initiative, it is crucial that they have a clear understanding of how content and services are classified in the jurisdictions within which they operate.

Collaborating with local broadcasters should be very helpful in terms of developing such an understanding. It is also important to understand how the local legislation perceives the 'location' of content and determines the 'place' at which a service is delivered or received.

Each country has a responsibility to develop their own legislation that they can apply to Internet content and services within their jurisdiction.

Unfortunately, as several studies have shown, many countries have insufficient or inadequate legislation to deal with the issue of online child protection.

Additionally different jurisdictions hold differing views. These differences can be abused or exploited to the detriment of children. Criminals and child abusers will know which countries have the weakest laws or the least developed mechanisms for dealing with these sorts of issues and they will naturally gravitate towards them unless counter-vailing measures are taken.

Given this inconsistency in the legislative and policy frameworks across different countries, it is imperative that

the Internet industry at large embrace best practice guidelines and adopt global standards and codes of practice that allow them to exercise a socially responsible effort towards dealing with the issue of child online protection.

In many countries around the world, industry is taking a lead and adopting voluntary and self-regulatory approaches that demonstrate commitment to developing a responsible approach to children's use of online ICT and communications. It is very much in the industry's interests to take action, to get ahead of the curve, not only because it is the right thing to do from a moral perspective, but also because, in the longer run it will help develop public confidence in the Internet as a medium.

Without that confidence and trust, the technology will never deliver or fulfill its enormous potential both to enrich and empower individuals but also to add to the economic prosperity and well being of each country.

8.

Further Information and Reading

Collaborating as an industry

European Framework for Safer Mobile Use by Younger Teenagers and Children: http://www.gsmeurope.org/documents/safer_children.pdf

Links to national Codes of Practice for safer mobile use by European mobile operators (in English and their original language): http://www.gsmeurope.org/safer_mobile/national.shtml

GSMA, Code of Practice on Spam: http://www.gsmworld.com/our-work/public-policy/protecting-consumers/mobile_spam.htm

Safer Internet Programme: Empowering and Protecting Children Online, http://ec.europa.eu/information_society/activities/sip/index_en.htm

Telecom Italia on child protection: www.telecomitalia.com, Sustainability->Hot Topics-> Protection of Children and Abuse

Study on Safer Internet Program Benchmarking of Filtering software and services:

http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/sip_bench/index_en.htm

Home Office: Internet Taskforce for Child Protection (UK) – industry good practice documents: http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Content Classification

UK's industry funded Independent Mobile Classification Body: http://www.imcb.org.uk/

EU Kids Online project: http://www.eukidsonline.net/

Safer Children in a Digital World: the report of the Byron Review: http://www.dcsf.gov.uk/byronreview/

Education and Customer Communications

Industry funded resource for teachers to help them understand younger people's use of technology: http://www.teachtoday.eu/

Illegal Content

International Association of Internet Hotlines: https://www.inhope.org/

Mobile Alliance against Child Sexual Abuse Content

http://www.gsmworld.com/mobilealliance

The Financial Coalition Against Child Pornography

http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703

Self Regulation of the Media

All BBC online services are subject to the BBC Editorial Guidelines (http://www.bbc.co.uk/guidelines/editorialguidelines/edguide)

and the BBC Online Services Guidelines (http://www.bbc.co.uk/guidelines/editorialguidelines/onguide)

National Reports

UK: Safer Children in a Digital World: the report of the Byron Review, (http://www.dcsf.gov.uk/byronreview/

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

Printed in Switzerland
Geneva, 2009

With the support of:

TELECOM ITALIA

AfrISPA
African Internet Service Provider's Association

EBU·UER

GSMA

CHIS

vodafone