Ofcom's Submission to the Byron Review

Annex 4: Online child protection – the international perspective

Submission date:
30 November 2007

Contents

1 Introduction and overview

As part of our research in preparing this submission we looked at approaches adopted in other countries to protecting children from harmful online content. The opportunities and the challenges surrounding children's use of the internet are shared around the world, so it is important to explore other countries' experiences in this area when considering options for the UK. We have therefore carried out a brief survey to identify the policy approaches and control mechanisms used in several countries around the world:

- we looked at France and Germany, with comparable market sizes and levels of internet penetration to those in the UK; we also looked at Sweden which has one of the highest broadband penetration rates in the world;
- we considered other major English-speaking markets, including the US and Australia;
- we examined the approach employed in the Republic of Korea with its advanced use of internet applications among children and teenagers; and
- we looked briefly at the use of national network-layer content blocking mechanisms in China and Saudi Arabia.

In each country we:

- identified the relevant government and regulatory bodies involved; and
- examined whether regulation has been applied to potentially harmful online content; and
- explored major initiatives in the areas of filtering, age verification and content classification.

In conducting this overview, we have relied on desk research and information from regulatory bodies and other organisations involved in online child protection in these countries. We have endeavoured to ensure that all the information is as correct; however, given the complexities of internet regulation, the lack of direct comparability between the countries' approaches and ongoing change in this area, some information may be out-of-date by the time this report is published. The report does not aim to be a comprehensive examination of internet regulation in other countries, but an overview of the range of measures adopted to protect children from harmful content online.

The overview section provides a summary of approaches adopted by the countries included in our analysis. This is followed by a summary of the tools and mechanisms adopted in each country surveyed.

We would like to thank the following organisations and individuals for information on specific countries' approaches:

Australian Media and Communications Authority (ACMA), British Embassy in Seoul, Conseil supérieur de l'audiovisuel (CSA), Family Online Safety Institute (FOSI), Freiwillige Selbstkontrolle Multimedia (FOSI), Délégation aux Usages d´Internet (DUI), John Carr, Korean Broadcasting Commission, Korean Internet Safety Commission (KISCOM), Media Partners Asia, Oxford Internet Institute (OII), and the Swedish Media Council.

1.1. Overview

The global reach of the internet – one of its greatest benefits – means that both the advantages of instant international communication and the potential harms are often experienced in similar ways around the world. The options for protecting children online from harmful content have been explored by policy-makers and the internet industry in many countries. The international challenges involved in the task are largely similar – although the differences in legal systems and policy traditions mean that different approaches have evolved, and that direct comparisons between countries are not always possible.

Our analysis of approaches in different countries suggests that the mechanisms applied vary significantly:

- some countries rely mainly on efforts to promote awareness of internet safety issues, (e.g. Sweden);
- yet others have legislated/regulated on the issue directly. In some cases this regulation is carried out by a statutory regulator (e.g. Republic of Korea), in others a co-regulatory approach is applied (e.g. Germany, France and Australia);
- a number of states exercise direct control over potentially harmful content as part of a broader government control framework for the internet which is not specifically targeted at protection of children (China, Saudi Arabia);
- Awareness-raising of internet safety and harmful content issues through information campaigns is of great importance in many of the countries we surveyed.

Figure 1: Overview of policy measures to protect children from harmful content

	France	Germany	Sweden	USA	Australia	South Korea
Legal or regulatory restrictions for online content unsuitable for minors		✓			✓	✓
Age verification/parental consent requirements		✓		✓	✓	✓
Requirements for filters in public spaces (e.g. schools, libraries)	✓	✓		✓	✓	✓
Policy measures to provide free filtering tools	✓	✓			✓	
Requirements for industry to carry out awareness-raising	✓	✓			✓	

Source: Ofcom research, ACMA, SMC, FOSI, FSM, KJM, KISCOM, Medierådet, MIC

1.2 Regulation of illegal and harmful content

There are significant differences between countries in what constitutes illegal content, and associated differences in enforcement arrangements. All of the countries surveyed have

primary legislation in place defining certain activities – such as distribution and possession of child abuse images – as illegal. As in the UK, these activities are illegal under all circumstances, independently of whether children can access this content or not. Some countries' legislation is similar to the UK's (e.g. France, Australia, Sweden) in that it seeks to ban images that are linked to criminal activities and material that may cause extreme distress both to children and adults. Other states employ a broader notion; for example in Korea, content that "infringes upon the public interests and social orders" may be defined as illegal1. Content defined as illegal generally attracts direct regulation, either by the government or in combination with co- and self-regulatory measures. The approach in other European countries surveyed is largely similar to the UK, with law enforcement and industry bodies cooperating on tackling illegal content based in the country, and aiming to restrict access to content hosted elsewhere.

In addition, several of the countries surveyed have enacted legislation in relation to content that while legal, is potentially harmful for children. For example, in Germany, the 2002 Youth Protection Act[2] distinguishes between illegal content (such as child abuse images), restricted content (such as adult pornographic content, which should only be made available to adults in closed user groups behind an age verification system) and harmful content (which may be only made available in a way that prevents, or substantially impedes, children's access to it). The national regulatory body for the protection of minors, Kommission für Jugendmedienschutz (KJM) is charged with monitoring and enforcing these regulations. The KJM has officially acknowledged the Freiwillige Selbstkontrolle Multimedia (FSM), an industry self-regulatory body which includes most of Germany's major online players. The FSM's code of conduct commits its members to implement child protection measures, including access restrictions for potentially harmful content, and aims to promote awareness of internet safety issues. In France, the Penal Code establishes a general prohibition to produce or distribute content which is violent, pornographic or which seriously violates human dignity, whatever the means, where the message may be seen or perceived by a minor. ISPs provide free filtering products to their customers as the main means to ensure protection.

Another example is the approach taken in Australia, where the Broadcasting Services Act 1992 requires classification of content unsuitable for those under 18. This responsibility was given to the Classification Board by the Classification Act 1995. Providers of internet content must prevent access for under-18s to material classified as unsuitable to them. The converged media and communications regulator, ACMA[3], is charged with defining the rules and processes for restricted online content systems. As in Germany, the implementation of these rules is based on a co-regulatory model. The content codes developed by the Internet Industry Association set out detailed legally-enforceable requirements for ISPs and content hosts. The regulator, ACMA, monitors compliance with the requirements and carries out periodical audits.

In the Republic of Korea, the legal framework is provided by the 1997 Youth Protection Law, which includes provisions on protecting the young from harmful media content. The Korean internet safety commission, KISCOM, is responsible for defining online content that may be harmful for young people. Content providers are required to introduce age verification processes, linked with national ID card information, for content designated as harmful for young people by applying uniform front pages based on a format specified by KISCOM. In addition, a real-name verification system was introduced in July 2007 on Korea's major portals. Internet users are required to fill in their national ID registration information before posting comments, and their data is cross-checked using online credit information

[1] http://www.singo.or.kr/english/report/howto/
[2] http://www.kjm-online.de/public/kjm/bogus.php?download_id=337&PHPSESSID=44196063e1d9f3074c2331c5df80f158
[3] The Australian Media and Communications Authority

databases. The system aims to reduce malicious and/or obscene commentary (i.e. it is not targeted specifically at child protection issues).

In all these examples, regulation of access to potentially harmful content focuses on national providers, as these are the only providers within the government's jurisdiction. Such rules tend to be combined with age verification and classification schemes for online content. However, these measures are likely to tackle only a small proportion of the available online content that is potentially harmful; in the absence of other measures, children are still able to view content published in other territories.

Some countries also have parental consent requirements in place in relation to children's privacy. The US and the Republic of Korea both have passed legislation requiring online content providers to gain verifiable parental consent before collecting personal information about child internet users under a certain age (13 in the US, and 14 in Korea).

Finally there is The Association of Internet Hotline Providers in Europe (INHOPE) which provides a collaborative forum for hotlines from all over the world. Through this body, Information about internationally hosted content is shared with relevant local authorities.

1.3 Several countries have adopted measures to support the use of filtering tools

As discussed in Annex 2, filtering tools provide an efficient (although not full) protection mechanism against potentially harmful content. The majority of the countries examined had some requirements or initiatives in place to promote the adoption of filtering technologies. There are several types of initiative:

Installation of filtering tools in public places where children may be accessing the internet. For example, in France, The Technology Directorate (SDICTE) supports provision of filtering tools for educational institutions as part of its national plan for the protection of students. In Australia, The *NetAlert* programme managed by the Department of Communications, Information Technology and the Arts (DCITA) coordinates the national filter scheme which provides every Australian public library with a free filter. In the US, the 2002 Child internet Protection Act (CIPA) requires all publicly-funded schools and libraries to install filtering tools. In the Republic of Korea, all cyber-cafes, schools and libraries are required to install filtering software.

Promoting the use of filtering software by parents to install on home PCs and laptops used by children. Several approaches have been applied in the countries examined. Australia's *NetAlert* programme makes free tools available to any parent. The software can be downloaded, or sent in the post. In addition, a website and a hotline are available to internet users who want advice on installation of tools and online child protection. The Australian government has undertaken a detailed assessment of filters made available via the filter scheme. In addition, the converged communications regulator, ACMA, manages a national outreach programme, continuously examines trends in internet safety and carries out research on filtering solutions.

In France the law has required ISPs to provide their customers with a filtering tool since August 2000 (the provisions were restated in legislation in June 2004). In November 2005, under the aegis of the AFA (Association of Internet service providers), French ISPs signed an agreement with the French Ministry for the Family, to supply all subscribers with free-of-charge, efficient and easy to use parental control software. The agreement states that these ISPs tools must meet some minimal quality standards agreed between ISPs, the French government and Child care associations. The standards include the provision of 'pass lists' for children and 'blocking lists' for adolescents; and restrictions on subscribers' ability to

create an Internet account without making an explicit decision about the use of the filtering tool. The software is tested under the supervision of the Ministries of Education and Research, and the Interdepartmental Delegation on Family Affairs.

The agreement between the AFA and the Ministry also committed ISPs to carry out awareness campaigns for their users and contribute to a government awareness campaign, led by the Ministry for the Family in 2006. The campaign had the core message "*On the internet, security starts with you*". Several public information films were broadcast on the largest French TV channel; one provided users with information about the new parental control tools offered by internet access providers.

AFA and its members actively support this campaign: they were involved in its creation and helped raise awareness access through their own websites.

Flexible network layer parental controls
Flexible network layer filtering enables parents to apply different levels of control and to restrict children's access to potentially harmful websites. Among the countries surveyed, only Australia is currently considering mandating such controls for ISPs. This could, in the future, serve as an alternative filtered internet service for families who prefer this protection option over home computer-installed software tools. The system may be implemented following feasibility research and input from a trial of ISP filtering currently taking place in Tasmania. An initial feasibility study carried out in 2006 found that network layer controls reduced performance significantly, especially for larger ISPs. However, the changes in performance were detected by only one in six study participants.

1.4 Some states employ mandatory blocking of 'harmful' content at the ISP layer

ISPs in many countries, including the UK, voluntarily block access to illegal websites using lists provided by law enforcement authorities, which usually cover illegal content such as child abuse images. In some countries the blocking activity extends to broader content which the authorities consider illegal to the country's population, irrespective of whether they are adults or children.

For example, in South Korea, ISPs are required to block not only illegal content but also materials deemed harmful by the Korean internet Safety Commission (KISCOM). Content categories covered in the scheme include pornographic content (the majority), violent materials and crime-related content. The legal basis is provided by the 1995 Law for Electronics and Communications Businesses which contains provisions for filtering "national illegal and harmful information" and for preventing "cyber sexual violence".

In China, an internet filtering regime is implemented by the Ministry of Information Industry (MII). According to a forthcoming report by the Oxford Internet Institute[4], filtering is performed by nine internet access providers licensed by the government. These licensed providers offer international network access to regional internet service providers. Filtering takes place at national gateway routers based on a government-maintained list of around ten content categories, including pornography, gambling, violence and terror.

Saudi Arabia's government has also put arrangements in place to block web pages containing pornographic, illegal, or otherwise objectionable content, which contains "violation of Islamic tradition or national regulations". [5] The Communications and internet Technology Commission (CITC) oversees the blocking process that is implemented by the three licensed

[4] Brown, I. (forthcoming, 2007). Internet filtering: be careful what you ask for.
[5] See the Internet Services Unit information page on http://www.isu.net.sa/index.htm

data service providers (DSPs) on their servers. The filtering takes place at the proxy servers of DSPs, between the state-owned internet backbone and servers in the rest of the world. The list of blocked sites is maintained by CITC and is updated on a daily basis. The types of content blocked, and the filtering process is transparent and users can request CITS to unblock websites stating the reasons to which the CITS has to respond.

However, the interventions described above are all aimed at controlling access to illegal content or content considered harmful by the authorities for all internet users in the country, rather than managing access by some groups of individuals (such as children).

1.5 Trust marks, content standards and child-friendly content

Some countries' activities focused on promoting services that are child-friendly, rather than restricting access to potentially harmful services, including:

- In several countries **industry trust marks** are used to indicate compliance by ISPs and/or content hosts with online safety requirements. For example, in France the AFA and its members ISP signed a Charter in June 2004, under which they made several commitments in relation to child protection and illegal content. On the basis on this Charter, the AFA has created a "Net+Sur" (safer Internet) label, that can be published on its website by compliant ISPs.

- Also in France, the Ministry for Home Affairs mandated the "Forum des droits sur l'internet" (Internet Rights Forum) to work on a "Certificat citoyen" (Certificate for citizenship) that could be gained by ISPs which contribute to a safer Internet. The FDI accepted a recommendation in 2006 that a trustmark for ISPs be created.

- In Australia, the 'Ladybird' trust mark serves a similar role – ISPs which comply with the best practice requirements of the Internet Industry Association's codes of practice have the right to display a Ladybird logo on their homepage.

- Measures to implement and enforce **content standards in online communities** which are open for children: an example of this is a recent agreement between New York's attorney general and Facebook, under threat of legal action, on monitoring and enforcement of its child protection policies. In Sweden, the Swedish Media Council has worked with the major social networking services used by children to develop website policies and to adhere to best practice in online safety.

- "Positive" content regulation or **promotion of child-friendly "pass lists**" and portals: the most direct example of a co-regulatory initiative in this area is the "*Net for kids*" initiative in Germany, announced in summer 2007. The project is coordinated by the self-regulatory body FSM, and co-funded by the government and the internet industry. The aim is to create a nation-wide database of websites suitable for, and adapted for children, in order to provide a safe and interesting surfing environment. The list is expected to contain several thousands of websites and will be used by filtering software as well as by parental control applications in operating systems.[6] In addition to policy initiatives, a wide range of non-governmental organisations and private players are active in this area. This includes work by public organisations (for example, the *KidsClick* search engine based on a meta-list of child-friendly websites compiled by public libraries in the US), children's media brands (many children's television providers offer sophisticated websites for children including video, games and online social environments), and online content providers (for example, the

[6] http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_prog/results/fsm_a423842.pdf

Yahoo! Kids portal which offers a wide range of materials and activities for children, and is available in English, Korean and Japanese).

1.6 Awareness-raising initiatives

Raising awareness among parents and children is vital both for governments and private players around the world. For example, in a recent announcement, Australia's Minister for Communications, Information Technology and the Arts, Hon Helen Coonan, stressed in relation to the free filtering tools provided by the Australian government, is important to "recognise that while the free services we are providing will be useful tools for families, parental supervision is more important than ever" and urged parents, teachers and carers to engage in dialogue about safety issues with children.[7]

To support this process, a wide outreach programme has been set up in Australia to deliver advice about online protection both for children and adults. The Government's *NetAlert* initiative provides material on its website, and operates a helpline on internet safety issues.

Awareness-raising is the key task of the Swedish Media Council, a public body charged with child protection in all media, including the internet. The Council works to encourage dialogue between children and adults and to develop and disseminate educational material about safe use of the internet among parents and educators. In France, the Interdepartmental Delegation on Family Affairs orchestrated a media campaign in 2006 with the message "On the internet, security starts with you".

In addition to these activities, co-regulatory measures to support awareness-raising have been implemented in several markets. In Germany, France and Australia, industry codes require ISPs and/or content providers to carry out awareness-raising activities, such as placing safety information prominently on their portals, and providing information of the use of software filters. In the US, the federal *On Guard Online* website is the result of co-operation between six federal agencies to offer information on secure use of the internet, while the Federal Bureau of Investigations (FBI) provides a website offering safety guidance for parents.

In addition to policy efforts, a wide range of non-governmental actors in other countries are actively engaged in awareness-raising work. One example is the *GetNetWise* initiative in the US, operated by the internet Education Foundation and supported by internet industry players, non-governmental organisations and child activists.

1.7 Conclusions

While approaches to the protection of children have evolved differently, depending on existing regulatory frameworks and different policy traditions, some general conclusions can be drawn.

Firstly**, the protection of children is recognised, in all the western countries we have looked at, as a complex issue, where solutions depend on a combination of public policy and industry activities as well as on action by parents and children themselves**. In France, Sweden, Germany, Australia and the US a combination of all of these measures is used.

Secondly, while the protection of children from potentially harmful material online is recognised as an important issue in all the countries surveyed, **the specific measures**

[7] Please see http://www.netalert.gov.au/news_and_events.html

depend on cultural background, policy traditions and the particular contexts of internet use. For example, online gaming is an area of particular concern and attracts direct regulatory intervention in South Korea and China, while this is not the case in other countries. And in Sweden, while several types of content are defined as illegal and/or prohibited, the 1992 Fundamental Law on Freedom forbids pre-screening of content in advance for regulatory purposes - any action is to be taken after if had been published. This limits the possibility of applying content regulation both to traditional and new media content. Therefore, although online protection of minors is a globally shared challenge, there is no 'one size fits all' solution. **Accordingly, any actions adopted in the UK, while taking into account the lessons from international experiences, will need to be targeted at, and relevant to, UK citizens' and consumers' expectations, and children's experiences.**

Finally, international examples show that all solutions have both pros and cons. For example, age verification requirements in Germany restricting access to content exclusively suitable for adults have had a limited effect on access to overseas-based content. As shown by the comprehensive programme of testing filtering solutions in Australia, network-layer filtering potentially offers an alternative means for parents to manage children's access, but has significant performance implications for ISP networks. For this reason any solutions must be carefully assessed in terms of their potential to deliver real improvements in protecting children from harmful content, balanced against associated costs and the costs and benefits of alternative approaches.

2 France

2.1 Introduction

France has an internet penetration rate of 55%, and around 48% of households had access to broadband at the end of 2006.[8] In France, the regulation of telecommunications markets is carried out by ARCEP (Autorité de Régulation des Communication Eléctroniques – formerly AT). Spectrum management is the responsibility of a separate government agency (Agence Nationale des Fréquences) while the Conseil supérieur de l'audiovisuel (CSA) is responsible for the regulation of the television and radio industries. The CSA does not have direct responsibilities for the regulation of internet content.

France - communications regulatory authorities

Authority	Remit
Conseil supérieur de l'audiovisuel (CSA)	Independent regulator for the television and radio broadcasting market.
Autorité de Régulation des Communication Eléctroniques (ARCEP)	Independent regulator for the electronic communications networks and services and postal activities
Agence Nationale des Frequences (ANFR)	Government agency with responsibility over spectrum management
Delegation for Internet Usages (Délégation aux usages d´internet (DUI)	The DUI reports directly to the Minister of National Education, Higher Education and Research, and is responsible for the coordination and promotion of various activities in protection of children online
Délégation interministérielle à la famille (DIF)	An inter-departmental unit within the Ministry of Employment, Social Relations and Solidarity responsible for child and youth protection on the internet.

2.2 Protection of children from harmful content

As in the UK, internet content is subject to definitions of illegal activities with content in criminal legislation (e.g., in relation to child abuse images). The Penal Code establishes a general prohibition to produce or distribute content which is violent, pornographic or which seriously violates human dignity, whatever the means, where the message may be seen or perceived by a minor.[9] Protection of children online is also subject to significant activity involving many players and including government departments, schools, NGOs, and other relevant stakeholders.

At the National Family Conference in September 2005, the French Prime Minister de Villepin called for action to protect children on the internet and for accompanying information campaigns. Possible actions included awareness raising campaigns, classification of tools,

[8] Internet take up data from Internet World Stats at http://www.internetworldstats.com/europa.htm#fr .Broadband take-up data from IDATE

[9] **ARTICLE 227-24** (Ordinance no. 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002). See: http://195.83.177.9/code/liste.phtml?lang=uk&c=33&r=3741#art16410

services and content, educational programmes, safe search tools, the creation of a 'family label' and data protection measures. The announcement kick-started an engagement process between ISPs, mobile operators, government and citizens to design online protection tools.

Major public actors in this area include:

- **The Delegation for internet Usages** (Délégation aux usages d´internet – DUI)[10] is responsible for the coordination and promotion of various activities in the online protection of minors, including the Confiance Project (French awareness node within Insafe). The DUI reports directly to the Minister of National Education, Higher Education and Research (MENESR).[11]

- **The Inter-departmental Delegation on Family Affairs** (Délégation interministérielle à la famille –DIF) within the Ministry of Employment, Social Relations and Solidarity is responsible for child and youth protection on the internet.

- **The Ministry for the Family**

In 2004 the French government obliged ISPs to provide their customers with filtering software. The law has since been reinforced by an agreement between the Ministry of Family Affairs and the Association of Internet service providers in France, AFA, committing the ISPs to supply their subscribers with the filtering software for free. As a result, all French consumer ISPs have offered free parental control software, with three different profiles (one for children, one for teenagers, and one for adults) since April 2006. Subscribers find the software included in their connection pack, and can also download the software from their access provider's site.

The software has been tested under the supervision of the DIU and DIF. Some non-governmental organisations are involved in testing and raising awareness of parental control software. For example, E-Enfance ('E-Childhood') provides filtering software comparison test results three times a year. The tests are carried out in conjunction with the Delegation on Family Affairs (Ministry of Employment, Social relations and Solidarity) and the DUI, who work with ISPs and software providers to improve protection. Action *Innocence*[12], an international organization dedicated to protecting children online, provides test results on various French parental control software options. Fact sheets and assessments are provided, with test results updated every six months.

In addition, Point de Cont@ct, the French hotline created in 1998 under the EU Safer Internet Plan offers advice for parents and children on internet protection issues, including guidance on useful filtering software.

Point de Cont@ct deals with reports of illegal activities such as child pornography, racial hatred or violence. The hotline closely co-operates with LEA and the other hotlines which make up the INHOPE network.

[10] Please see http://www.mineurs.fr/ for information on the informational materials and links to software filtering results websites such as Action Innocence France (www.filtra.info).
[11] Please see: http://delegation.internet.gouv.fr/.
[12] Please see http:// www.filtra.info

2.3 Public awareness campaigns

The CONFIANCE project is the French node in charge of implementing awareness campaigns and coordinating actions at the national level under the EU Safer internet Plus Programme, working under the aegis of the French Ministry of Education and the Délégation aux Usages de l'internet (DUI: inter-departmental internet usage unit). Other partners include the École Normale Supérieur and the technical coordinator Tralalere, which creates and distributes educational digital content. The projects principal aim is to raise awareness among children and the general public of the risks associated with internet use, to encourage responsible behaviour and to define appropriate online behaviour. A key aspect of the project is the involvement of all internet safety stakeholders (public institutions, non-profit-making, private partners) in a national awareness campaign.

The national awareness campaign ("internet sans Crainte" or **"internet without Fear"**) aims at the various target audiences: children, parents, grandparents, and educators. The core target group among children is the age range at which children start to use the internet on their own but are not yet aware of the risks: 7 to 11 years old. The intention is to disseminate initiatives already developed for other audiences, including teenagers.

AFA Point de Contact, which is in charge of the Hotline project under the Safer Internet plus programme, co-operates with CONFIANCE. Especially, AFA attends the Confiance Advisory Boards since January 2006, and The DUI attends the Point de Contact Advisory Boards since May 2007.

Examples of pilot activities and tools to raise awareness, and to train and support children and families about safety issues include:

- cartoons created by Tralalere for children between 7 to 12 years old, ready to be broadcasted on mass media;
- school-targeted support (guidelines for teachers, CD-Roms, posters, leaflets, etc);
- tools providing advice to families (guidelines, CD-Roms, leaflets etc.); and
- These are available in the CONFIANCE website which also provides information about other tools available in France.

Other relevant initiatives include:

The **Forum for internet rights** (le Forum des droits sur l'internet)[13], an independent initiative with representatives from Government, industry and civil society, covering all aspects of public policy linked to the use of content in a digital world. It is not a decision making body, but plays a strong facilitator role, in close collaboration with public authorities, and can act either at the request of public authorities or private actors, as well as on its own initiative.

A **media campaign** orchestrated by DIF with the aim of creating awareness among parents with the message: "On the internet, security starts with you". This included press and radio, with ten short films shown on television in 2006.

A **national educational plan** by the Technology Directorate (SDICTE) catering to students within schools and other institutions.[14] The programme focuses on providing

[13] http://www.foruminternet.org
[14] Please see Official Education Bulletin/BOEN of 26 February 2004.
Accessed from http://www.educnet.education.fr/eng/equip/minors.htm on 31 October, 2007.

training to students and teachers on internet usage policies and providing educators with filtering tools (based on the availability of a national 'blocking list' of inappropriate websites).

2.4 Illegal content

The framework for tackling illegal content is, as outlined above, closely integrated with that for content which is potentially harmful for children. For domestically hosted content, the Point de Cont@ct hotline collates information about content which is banned or which may corrupt minors; depending on the characteristics of the content, it will inform the criminal authorities and the content hosts. Content hosts can be required to take down content, as well as passing on to content providers information about the illegal or harmful content, and about providers' legal duties and liabilities. Content hosts are also required to keep relevant data they have which might identify the providers of illegal content they host.

For internationally hosted content, France's focus is on supporting citizens through the provision of information and free filtering products. Information about abusive images of children is shared with INHOPE, but is not used as part of a domestic filtering or blocking system. France has made a small number of requests that to Google that it remove links to international sites targeting France in relation to hate speech and holocaust denial.

3 Germany

2.5 Protection of minors: 'regulated self-regulation'

Germany has an internet penetration rate of 63%, and 38% of households had access to broadband at the end of 2006.[15] The federal government is responsible for telecommunications networks regulation, while issues of culture and media are the sole responsibility of the 16 Länder (states) and are overseen by separate regulatory authorities in each Land (Ländesmedienanstalten or LMAs). Co-ordination across the Länder is achieved via interstate treaties, which set the framework for regional public service broadcasters, the licensing regime for private radio and TV broadcasters, and the regulation of new media and via the ALM (Arbeitsgemeinschaft der Ländesmedienanstalten) – an inter-state organization comprising directors of the state regulators. The interstate treaties are subject to frequent revisions.

There have been significant developments in the area of protection of minors in Germany over the last years. A number of events, including the highly publicized massacre of school children and teachers by a computer game addict in 2002, prompted country-wide action to overcome the historical fragmentation of approaches to child protection at the state level. In 2002, a new law was passed giving the federal government responsibility for child protection across areas other than the media (such as setting age limits for the purchase of alcohol and access to discos etc).

In the media area, the Youth Protection Act 2002 (Jugendschutzgesetz) and the Interstate Treaty on the protection of minors and human dignity in broadcasting and telemedia[16] consolidated and streamlined previous legislative provisions applied to broadcasting, media services and the tele-services sector. The Commission for the protection of minors and human dignity (Kommission für Jugend Medienschutz or KJM) was established and began its work in 2003.

The KJM is a 'converged' body in which the Länder and the Federal Government participate. It has a governing body of 12 members, with ten nominated by LMAs and child protection bodies, and the remaining two nominated by federal child protection bodies. It is responsible for protection of children in all media (including broadcasting, mobile TV, the internet, videotext and online computer games).

As the national regulator, the KJM has been given the authority to oversee activities in the determination of suitable content and to monitor compliance As part of a drive towards greater reliance on self- and co-regulation, the KJM's was given the power to accredit self-regulatory bodies to carry out routine regulatory tasks.

The authorized self-regulatory body for online media is the Freiwillige Selbstkontrolle Multimedia (FSM). FSM was set up in 1997 as the self-regulatory body for Germany's online industry and gained certification from the KJM in October 2005. The FSM works to provide the public with information and advice on media youth protection, related technologies and responsible media usage. The FSM has been accredited by KJM as a competent body to carry out self-regulation for the protection of minors. It has an operationally-autonomous body, the Complaints Commission (Beschwerdestelle) to deal with complaints and to provide advice both to members and non-members on how to respond to complaints.

[15] Internet take-up data from Internet World Stats at http://www.internetworldstats.com/ , broadband take-up data from IDATE.
[16] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien – JMStV). For the English translation, visit http://www.kjm-online.de/public/kjm/downloads/JMStV2007-englisch.pdf

Currently, the FSM has approximately 40 members, including AOL, Google, MSN and Deutsche Telekom who participate in various self-regulatory initiatives. FSM members conform to the KJM guidelines, as well as the FSM Code of Conduct.[17]. Members of the FSM are also committed to the promotion of media literacy among parents and children, particularly through the dissemination of information on the safe use of the internet.

The FSM is funded through contributions of the affiliated providers, and their rulings are subject to challenge from the Länder and the KJM.

Germany - communications regulatory authorities

Authority	Remit
Bundesprüfstelle für jugendgefährdende Medien (BPjM)	Federal investigation office that Investigates and indexes print and electronic material deemed inappropriate for children
Bundesnetzagentur	The Federal Network Agency is the national regulator with responsibilities for electricity, gas, telecommunications, post and railway
Landesmedienanstalten (LMAs)	The media regulator for each Lander which enforces the content rules within the Interstate Treaties.
Kommission für Jugend Medienschutz (KJM)	The government regulator that is responsible for the protection of minors in broadcasting and online. It determines suitable content and oversees the activities of the FSM and other authorised self-regulatory bodies.[18]
Freiwilligen Selbstkontrolle Multimedia (FSM)	Self-regulatory body monitoring online content among its members and on the internet. Also serves in a co-regulatory capacity to enforce legislation.

[17] See: http://www.fsm.de/en/CoC

[18] Other KJM- authorised self-regulatory bodies include the FSF (for broadcast content), USK (games) and FSK (feature films and cinema)

2.6 Overview of online protection mechanisms in Germany

Content classification

The Interstate Treaty provides three distinct categories of content, which are reflected in the FSM's Code of Conduct.[19] They include:

- **Illegal content** is forbidden in all circumstances (covering for example child pornography; Holocaust denial, incitement to hatred, violations of human dignity)

- **Restricted content** is adult content, as defined in the Youth Protection Act 2002) and which should only be made available to adults in closed user groups behind an age verification system.

- **Harmful content** is content which might harm minors and which should be made available only in a way that prevents, or substantially impedes, children's access to it. This classification requires a KJM-endorsed filter, other technical measures or the use of time restrictions.

Age verification systems

In Germany, people under 18 are not allowed access to pornographic content ("restricted content"), and providers of such content must use an age verification system to ensure children cannot gain access.

A number of age verification tools have emerged. Identification verification must be conducted within pre-approved locations such as the post office. Once verified, the applicant's documentation is sent to the provider. Under certain preconditions, webcams are now an option for applicants to identify themselves and then present their national identification to the online service provider for verification. Successful applicants can receive free software (non-transferable and designed for a PC) or be sent a personal ID USB-chip (PID) via post for €10; the USB is used in conjunction with a password. [20]

It is important to note, however, that AVS are imposed only on providers of pornography which are based in Germany. There is anecdotal evidence that a significant proportion of providers (up to 80% and mainly those providing pornography) have moved all or part of their operations outside of Germany in order to avoid the age verification requirements. However this problem is mitigated by the fact that this type of content can be put on a blocking list by the Federal Department for Media Harmful to Young Persons. The FSM Code of Conduct for Search Engine Providers requires the list to be built into search filters that are used by the search engines affiliated to the FSM. Through the use of these filters, the websites with harmful content should not be listed in the search results, making access more difficult.

Time-related measures regarding approaches to potentially harmful content online

German online content providers can apply broadcast 'watershed' rules to the internet. These time-related measures are one of the ways that providers can limit access to content deemed harmful but not extreme enough to merit an age verification system. Oversight of these time restrictions resides with the KJM and the LMAs. The provider must classify the content and implement the necessary steps (time restriction) to ensure that the content is

[19] According to testimony by Michael Schneider (09-6/2007) at the EU Consultation on "Safer internet and online technologies for children". Statement by BOCATEL Invent GmbH. .
[20] Please see www.xcheck.de.

time-slot appropriate. Breaches are investigated by the state authorities and fines can be imposed if the restrictions not technically correct. The “time zones” include:

- 22:00 = <16
- 22:00+ = 16+
- 23:00+ = 18+ as well as other erotic material

In addition, a self-regulatory commitment to time-sensitive moderation exists for chats to ensure that someone is present during a certain time of day:

Filtering

The Interstate Treaty for the Protection of Minors and Human Dignity in Broadcasting and Telemedia envisions the use of filters (which must be authorised by the KJM) as one way to meet legal requirements. To get authorisation, filters must be easy to install, have high-blocking thresholds and low over-blocking rates, be user-friendly and allow age-differentiated content blocking.

However, recent tests done by KJM suggest that the efficiency of available web filters is still low. In particular, illegal content associated with violence, racism, drugs and gambling, in particular, is rarely blocked.[21]

Blocking at ISP level

Very little blocking of online content is conducted in at the ISP level, and lists are not blocked at this point. This is partly due to the fact that preliminary censorship is prohibited by the German Constitution. Only a few single websites including illegal content have been blocked (note that when harmful content is made freely available it is automatically deemed illegal) after judicial injunctions.

The role of search engine providers

In 2004, the FSM approved a *Code of Conduct for Search Engine Providers*[22] with the aim of improving consumer protection as well as protection of children and young persons with their use of search engines in Germany. The Code highlights the particular role that search engines play in making information available on the internet and remains purely voluntary (therefore outside the scope of the KJM co-regulatory regime). It is important to note that the Code is applicable exclusively for search engines in Germany, with companies doing business internationally for their German search engine offerings.

The Code requires signatories to endeavour, within the framework of their capabilities, to enable technical precautionary measures which are suitable to promote the protection of children and young persons from content which is harmful to them, for example, by removing URL links from search results. The Code also makes clear that absolute protection cannot be guaranteed and that children should not use the internet without the supervision of their parents.

The Federal Department investigation office for Media Harmful to Young Persons (Bundespruefstelle fuer jugendgefaehrdende Medien, BPJM), in cooperation with the FSM,

[21] Public consultation: Safer internet and online technologies for children. Official statement of jugendschutz.net. Mainz, 31 May, 2007. Accessed on 25 October, 2007 from http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_prog/results/jugendschutz.net_a423505.pdf.

[22] Please see http://www.fsm.de/en/SubCoC_Search_Engines

has developed a blocking list (also known as BPJM module), which is implemented by the search engine providers for their German versions as part of their commitment to the FSM code of conduct. As a result, the relevant URLs are not listed in the search results.

Chat moderation

In early November 2007, three German chat room providers signed an FSM-endorsed self-regulatory agreement to provide internet chat rooms accessible to minors with moderators between 10:00 a.m. and 10:00 pm. At least one moderator per chat is required. The companies (Lycos Europe, RTL, Knuddels) must also maintain a list of "bad words" and will block participants who break the rules. Implementation of the Conduct of Conduct-Chat is monitored by FSM.

Promotion of awareness and safe internet use/media literacy initiatives

Finally, there has been strong support for media literacy initiatives in Germany since the early 1990s, with responsibilities with the relevant regulators who have been very active in this area. The media authorities have established their own research and training institutions, like the European Centre for Media Competence (Europäisches Zentrum für Medienkompetenz).[23] They fund third-party projects (for example courses at the "International School of New Media") and are involved in the support of several educational initiatives. The KJM, for example, has led the development of internet ABC[24], an informational website with sections for children and parents/teachers. It includes news, advice, quizzes and interactive games such as an internet 'driving test' and internet virus awareness.

The German awareness node under the European Framework of the Safer internet Program is called "Klicksafe", financially supported by the European Commission. Klicksafe is organized through the Landesmedienanstalten of Rhineland-Palatinate and North Rhine-Westphalia.[25]

As mentioned above, the FSM Code of Conduct also requires members to engage in supporting the FSM fostering media literacy amongst parents and children, particularly through the dissemination of information. Last summer, the FSM launched the "Net for kids" initiative, a positive content portal for children comprising a "pass list" of websites.[26] The project is co-funded by the government and the internet industry. The aim is to create a nation-wide database of websites suitable and adapted for children, in order to provide a safe and interesting surfing environment. The list is expected to contain several thousand websites for use by filtering software as well as parental control features in the operating system.[27] Sections for parents and teachers are included. The list is now available at www.fragfinn.de and includes adventure comics, tasks and simulations through which children are taught about how to use the internet safely.

Another initiative is the "Internauten" at www.internauten.de, created by the FSM, MSN and the DKHW. It includes adventure comics, tasks and simulations teaching children about safe use of the internet.

[23] http://www.ecmc.de/
[24] www.internet-abc.de/kinder/
[25] www.klicksafe.de
[26] Public consultation: Safer internet and online technologies for children. Official statement of jugendschutz.net. Mainz, 31 May, 2007. Accessed on 25 October, 2007 from http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_prog/results/jugendschutz.net_a423505.pdf.
[27] http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_prog/results/fsm_a423842.pdf

2.7 Illegal content

As in France, the framework for tackling illegal content is closely integrated with that for content which is potentially harmful for children. There are hotlines operated by the FSM, and the KJM, which can both issue takedown notices to domestic hosts. In addition, the KJM can apply financial sanctions to persistent offenders.

Information about internationally hosted content from these hotlines is passed to INHOPE and the BjPM. The BjPM creates an Index of banned sites, including both illegal content and material which is potentially harmful to minors and does not have appropriate access controls in place (such as robust age verification). The index is not used directly to block access to content. It is provided to the leading search engine providers, who agree to remove the blacklisted sites from their search returns under a code of conduct created by the FSM. Google, which accounts for at least 90% of the German search market[28], is a signatory to this code. Google does remove the blacklisted sites from its index at Google.de, but they will remain available to users of the global index at Google.com.

[28] www.webhits.de August 2007

4 Sweden

4.1 Introduction

Sweden has one of the highest internet and broadband penetration rates in the world. Over 80% of Swedish households had internet access in autumn 2006, of which 68% were broadband subscribers. Take-up is higher among families with children – 92% of 9-16 year olds have internet access at home[29].

General regulation of internet services falls under the remit of the Post and Telecommunications Agency (Post-och telestyrelsen, PTS), which regulates the electronic communications market in accordance with the EU regulatory framework. Broadcasting is regulated by the Swedish Broadcasting Commission, which monitors and enforces the legal framework set out in the 1996 Radio and Television Act, issues broadcasters' licenses and enforces regulations. The Swedish media Council is a government body set up specifically with the objective of monitoring and reducing the risk of harmful effects for children and young people in all media.

Sweden – communications regulatory authorities

Authority	Remit
Swedish Radio and TV Authority (RTA)	The government authority that oversees the broadcasting market, grants broadcasting licences and issues and monitors regulations.
Swedish Broadcasting commission (GRN)	The regulator for broadcasting content; monitors and enforces compliance with the 1996 Radio and Television Act and enforces the rules set out in the broadcasting licences.
Post and Telecommunications Agency (PTS)	The independent regulator for telecommunications, IT, postal and spectrum. As in other European countries, the basic framework for telecommunications regulation is provided by EU Directives. As part of its remit, PTS regulates internet networks and services.
Swedish Media Council	A Committee of Inquiry in the Government Offices, with the objective to reduce the risks of harmful effects of the media on children and young people. The Council's remit covers all media with moving images, i.e. film, TV, video, computer games, TV games and the internet. It is also the national node for INSAFE, the EU project for safer internet use by children and young people.

4.2 No specific rules exist for protecting children from harmful content on the internet

The police and industry co-operate on tackling illegal content

Several types of activities are defined as illegal in Swedish legislation, including the making and distribution of child abuse images, racial hatred content and unlawful depictions of violence. Law enforcement activities in relation to online content have focused on child abuse images, adopting a similar approach as in the UK, relying on co-operation between law enforcement, the internet industry and non-governmental organizations:

[29] http://medieradet.se/upload/Rapporter_pdf/svenskslutrapport2005-2006.pdf

- **Police**: the IT Section of the Swedish Criminal Police has a dedicated child protection team whose remit includes tackling criminal activities connected with child abuse images online.

- **Hotline:** An internet hotline is available to report illegal content. The hotline was initially managed by Save the Children Sweden, but in 2003 the responsibility was transferred to the police.

- **ISP blocking:** Since 2005, all major Sweden's ISPs block access to sites containing child abuse images, based on a blocking list maintained by the police. This is done voluntarily by the ISPs, which also co-operate with the police on identifying websites containing illegal content. Blocking is carried out using NetClear DNS filtering software. According to a 2005 study, the ISP level blocking stopped around 30,000 hits a day trying to reach child abuse images. Users who attempt to access a website known to contain child abuse images receive a notification that their content request has been blocked and that their request has been shared with the police.

- **Search engine blocking:** The police have also started co-operation with search engines. The first initiative in this area was announced in July 2007, with the Picsearch search engine agreeing to exclude from its search results illegal child abuse websites contained in the police blocking list.[30]

- **NGO activities:** a number of non-governmental organisations are active in supporting the efforts to tackle child abuse materials on the internet. Many of these are members of ECPAT Sweden, a node of the international "End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes" campaign. ECPAT Sweden was established in 1996 with 23 NGO member organisations and individual members. Its members' work covers a wide range of activities, including training for law enforcement authorities, awareness campaigns and youth activities such as chat-conferences on child abuse images and paedophile activities on the internet.

The legal framework forbids pre-screening of content

The legal framework for content in non-print media is provided by the 1992 Fundamental Law on Freedom of Expression, which prohibits pre-screening of content. The legal framework does not set out any rules prohibiting or limiting content that may be harmful for children in the media. Any forms of speech that are prohibited under criminal legislation or the Freedom of Expression Law are to be scrutinised after they have taken place and are to be based on legal trial. Prohibited forms of speech under the Law include racial hatred material, unlawful depictions of violence and instigation of rebellion.

Electronic bulletin boards are an exception from general practice – they are subject to the 1998 Act on Responsibility for Electronic Bulletin Boards. The act requires service providers storing bulletin board content to monitor and remove or make inaccessible obviously illegal content.

There are no specific provisions for protection of children online in the Swedish legal framework.

[30] http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/

4.3 Efforts to protect children from harm focus on awareness-raising and encouragement of best practice

The regulatory authority for protecting children from media harm is vested in the Swedish Media Council (formerly the Council on Media Violence). Established in 1990, the Council oversees all media with moving images, including the internet. The Media Council's objective is to reduce the risk of harmful effects of the media on children and young people.

The Council is funded by, and reports to, the Ministry of Culture. Its principal tasks are to:

- act as an expert on developments in the media and the effects of the media on children and young people;
- follow research on the effects of the media and to spread factual information and provide guidance;
- press for self-regulation in the media industry;
- work for increased media knowledge in schools;
- protect and strengthen children and young people in the new media landscape through cooperation with other actors; and
- follow international developments and take part in international cooperation in its field.

In the area of self-regulation, the council's efforts focus on encouraging best practice among major online players whose services are popular with children. It encourages the creation and enforcement of website use policies that are child-friendly and minimise risks to children and young people. For example, the Council has worked closely with the country's largest social networking site providers such as Lunastorm[31] and Playahead[32] to develop and enforce terms and conditions and policies, and to devise informational materials for both children and parents about safe use of the internet.

The Media Council carries out a wide range of awareness-raising activities

The Council's awareness-raising activities aim to:

- raise awareness and encourage dialogue between children and adults about safe use of the internet;
- develop and implement tools and methods for safer use of the net;
- support knowledge and critical understanding, and teach children to use new media responsibly;
- co-operate with other relevant bodies to increase the awareness about internet safety; and
- provide information about filtering tools and hotlines.

[31] http://www.lunastorm.se
[32] http://www.playahead.se

The council has developed a wide range of materials for children, parents and teachers on all aspects of internet safety. It also carries out campaigns promoting information about safe internet use. As part of its *Young internet* campaign the Council developed a *Safer internet* toolkit containing 27 high-quality resources on internet safety for children. The toolkit was then sent to educators all over Sweden. The council is currently working on developing this toolkit further and arranging training for educational professionals, social workers and welfare officers across Sweden.

In addition to supporting safe internet use, these activities place indirect pressure on online content and service providers. For example, in its awareness-raising materials the Council advises parents about the features of online services that are unsafe and what kind of services should not be used.

5 The US

5.1 Introduction

According to a Pew survey in late 2006, 71% of US adults were internet users[33]. This figure was significantly higher, at 93% for those aged between 12 and 17 years of age, and 55% of 12 to 17 year olds use online social networking sites.[34]

The regulation of internet services in the US falls under the Federal Communications Commission (FCC) which treats the online services (not the underlying telecoms) as unregulated information services.

USA - communications regulatory authorities

Authority	Remit
Federal Communications Commission (FCC)	The Federal Communications Commission (FCC) is an independent United States government agency, directly responsible to Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable.

5.2 Several attempts to establish legislation for online child protection

The strong US constitutional protections of freedom of speech and the right to privacy have been applied to regulatory solutions in the area of online child safety. In recent years, a number of attempts to pass legislation to safeguard children online were challenged[35]. Most prominently:

- **The Communications Decency Act (CDA)** of 1996 was Congress' first attempt to criminalize certain types of internet speech. In the landmark case *Reno v. ACLU* (1997), the Supreme Court found the law unconstitutional since the same objective could be met with less restrictive alternatives.

- **The Child Online Protection Act (COPA)** of 1998 was an attempt by Congress to amend the CDA in the light of the Reno judgment. The Act criminalized the 'knowingly' making available of material harmful to minors, and protected commercial operators which actively restricted site access. The Act was immediately challenged in a legal battle that is still ongoing.

At present, two major pieces of legislation are in place :

[33]Pew Internet & American Life Project: http://www.pewinternet.org/trends/User_Demo_6.15.07.htm
[34] Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew internet & American Life Project, April 18, 2007, p. 3, http://www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf
[35] We are grateful to the Family Online Safety Institute (FOSI) for the information provided on developments in the US. FOSI will launch its Online Safety Report 2008 at its conference in December 2007.

- **The Children's Online Privacy Protection Act (COPPA)**[36] which came into force in 2000. The Act requires operators of websites marketed at children under 13 to specifically to get "verifiable parental consent" before allowing children to access their site. The Federal Trade Commission (FTC) has the authority to issue regulations and enforce COPPA compliance. Operators can use a variety of methods to comply with the parental consent requirement, including print-and-fax forms, follow-up phone calls and e-mails, and credit card authorizations.

- **The Children's internet Protection Act (CIPA),** adopted in 2002, was narrower in scope, applying only to schools and libraries receiving federal funding. These must have an internet safety policy and technology protection measures in place to block or filter internet access to pictures that are obscene or harmful to minors. The law was declared constitutional by the Supreme Court in 2003.

Outside the regulatory framework, there has recently been legal activity targeting the alleged failure of social networking sites (SNS) to protect users from harmful content. As a result, MySpace has, in the past year, hired a chief security officer, removed thousands of accounts of registered sex offenders, and is developing parental control software.[37] Facebook has also identified and removed an unspecified number of profiles belonging to registered sex offenders. More recently, the Attorney General of NY reached a settlement with Facebook under which a third party will monitor Facebook's security procedures for the next two years. Facebook also agreed to a mandatory 24-hour response time for dealing with user complaints about nudity, pornography or harassment. This has triggered calls for action in other states in search of more protective measures for children, including age verification, content controls, access restrictions and parental consent.[38]

In addition, industry-led coalitions have been launched to explore solutions which link financial services with other identity-driven service providers on the internet. They include:

Financial Coalition Against Child Pornography (2006). Managed by, and sitting within the National Centre for Missing & Exploited Children (NCMEC)[39]. An initiative by the credit card issuers, banks and internet services companies to eradicate commercial child pornography on the internet by 2008. Members include Google, Yahoo!, Bank of America, and Visa, among others. .

Technology Coalition Against Child Pornography. This is also managed by NCMEC, and members include, but are not limited to, AOL, Google, Microsoft and Yahoo.

[36] Federal Register Vol. 64, No. 212. 3, November 1999. p. 59888. Accessed from http://www.ftc.gov/os/1999/10/64fr59888.pdf on 17 October, 20007.
[37] http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=68772
[38] CT Attorney General statement on Facebook settlement. Accessed 18 October, 2007 from http://www.ct.gov/ag/cwp/view.asp?A=2788&Q=397458
[39] In 1996, the U.S. Congress established the Exploited Child Division within NCMEC, and serves as a resource centre on issues re sexual exploitation of children. Visit www.missingkids.com.

5.3 Overview of protection mechanisms

Age verification

Age verification systems (AVS) are largely clustered around preventing under-age minors (<18 years) from online content and services specific to adult entertainment, alcohol and tobacco products. Such requirements usually demand a date of birth or credit card, the primary means of verifying age online. However, this identity-driven approach has proved largely unsuccessful. According to one study, 31% of 7th – 12th grade schoolchildren provided false age information in order to access a website.[40]

Filtering

Current filtering legislation is in place in 21 states, mandating that school boards and public libraries install filtering software to prevent minors from accessing "sexually explicit, obscene or harmful materials". The degree of use of internet filters, or content-controlled software, varies partly due to legal concerns regarding First Amendment protections.

Utah, for example, introduced legislation which requires ISPs, on the request of the citizen, to install in-network or filtering software to protect minors from the transmission of harmful content.[41] Texas requires interactive computer service providers to place a link to free or shareware filtering software, conspicuously on the first accessible web page of the service provider. There is a penalty of $2,000 for each day that the provider fails to comply.

A broad range of technological solutions are available to the US internet users for dealing with potentially harmful content , ranging from operating system filters and web browser controls (used increasingly by companies like Microsoft and Apple) to PC-based filtering software and search engine filters. Many of these tools are also available in the UK.

Standalone filtering solutions are available for purchase from a wide array of providers. These are increasingly sophisticated: in addition to allowing the filtering of content many tools now allow parents to monitor content accessed by children (for example, by offering periodic reports on sites visited by children, and monitoring of potentially dangerous online chats). An extensive list of software tools offered to consumers in the US is available at the GetNetWise.org website[42]. In addition to these stand-alone solutions, filtering tools are also increasingly available from ISPs, typically as part of a package of security tools that comes with internet connection, and are often offered free of charge. Many search engines, such as Google and Yahoo! also offer an option to block potentially harmful content.

Child-friendly content initiatives

In addition to efforts aimed at limiting access to potentially harmful content, there are many initiatives in place looking to provide safe content that is targeted at children and young people. These include child-friendly search engines and portals (a few of many examples

[40] The Henry J Kaiser Family Foundation, Generation M study: Media in the Lives of 8-18 year-olds, March 2005, p. 30.
[41] "Children and the internet: Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries". National Conference of State Legislatures. Last updated 23 April, 2007. Accessed 20 October, 2007 from http://www.ncsl.org/programs/lis/cip/filterlaws.htm.
[42] Please see http://kids.getnetwise.org/tools/

include AOL for Kids US[43], Ask Jeeves for Kids[44], Education World[45], and Surfing the Net with Kids[46]). Numerous websites also provide dedicated services for children.

5.4 Awareness-raising and other initiatives

A wide range of diverse educational and awareness-building efforts in the US are led by the industry and non-profit organizations. The Government has had a relatively limited involvement at the national level to date, and there is little media literacy instruction carried out within America's educational system. One major Government-led project has been ***On Guard Online*** [47] involving six federal agencies. The website set up by the initiative provides a broad range of information about online safety, and includes videos and tutorials on child online safety, as well as a section advising parents on children's use of social networking sites[48]. A number of legislative measures were introduced in the Senate over the past year, which, if adopted, would increase national co-ordination of awareness-raising activities, and promote online safety education in the US.[49] In addition, there are state-based initiatives, such as activities led by the Virginia Department of Education, on improving internet safety education in Virginia's schools.

A significant number of public awareness campaigns and educational initiatives are conducted by industry-led partnerships. Some of the major initiatives include (please note that this is a very small selection of a much broader range of activities):

- **ConnectSafely.org[50]** is a project of the non-profit organisation Tech Parenting Group and provides a web portal for parents, teens, educators and advocates to discuss online safety issues. It also provides a wealth of resources on youth online safety, including articles, videos, safety tips, interactive forums, and commentaries. The effort is supported by a wide variety of high-technology companies, including Bebo, AOL, Facebook and Google.

- **Internet Keep Safe Coalition[51]** is a coalition formed by the US State Governors and/or their spouses, formed in partnership with crime prevention organizations, law enforcement agencies, foundations and corporate sponsors. The initiative's *iKeepSafe* website provides parents, educators, and carers with tools and guidelines to teach children about safe use of the internet. It also offers a wealth of interactive materials for children, including games, videos and books.

- **GetNetWise.org[52]** is a public service website operated by the non-profit internet Education Foundation,[53] bringing together a wide range of internet industry corporations and public interest organizations to "help ensure that internet users have safe, constructive, and educational or entertaining online experiences". [54] The

[43] http://kids.aol.com
[44] http://askforkids.com
[45] http://www.education-world.com
[46] http://www.surfnetkids.com
[47] http://onguardonline.gov/index.html.
[48] http://onguardonline.gov/socialnetworking.html
[49] For example, the "Protecting Children in 21st Century Act", and the "Safeguarding America's families by enhancing and reorganising new and efficient technologies (SAFER NET) Act".
[50] www.connectsafely.org
[51] www.iKeepSafe.org
[52] www.getnetwise.org
[53] www.neted.org
[54] Major corporate supporters include Dell, Microsoft, Verizon, Amazon.com, Yahoo!, AOL, AT&T, Comcast, EarthLink, Visa, Wells Fargo, and the RIAA. Key public interest organizations include the Centre for Democracy and Technology, the American Library Association, the Children's Partnership, People for the American Way Foundation, the National Consumers League, Net Family News, ProtectKids.com, SafeKids.com, and Wired Patrol.

website offers a dedicated section on children's safety, which includes guides for parents and children, lists of websites suitable for kids and links for reporting suspicious illegal activities. It also offers a comprehensive "*Tools for Families*" section which helps parents select the tools most suited for their and their children's needs.[55]

- **i-SAFE Inc**.[56] is a non-profit foundation founded in 1998 with a mission to "educate and empower youth to make their internet experiences safe and responsible". The goal is to educate students on how to avoid dangerous, inappropriate, or unlawful online behaviour. *i-SAFE* develops and implements community outreach programmes to parents, law enforcement, and community leaders. The *i-SAFE* website offers online interactive tutorials about internet safety for children and youth, as well as a wide range of materials for parents and educators.

- **Pause-Parent-Play**[57] is a campaign designed to "empower parents to choose what their kids watch, hear and play - from TV and movies to video games and music" based on a partnership between many major communications companies, entertainment companies and family groups. The *PauseParentPl*ay website provides Interactive materials for parents on all aspects of children's use of the internet, audio-visual services and video games, and safety mechanisms.

- **Project Online Safety**[58] is an initiative aiming to "educate parents and children about the importance of online safety and empower children to have safer experiences online". The project's online portal offers one point of access to a wide range of online safety tools and educational materials developed by technology companies, media organizations and non-profit organisations.

- **Wired Safety**[59] was founded in 1995 and provides one-to-one help, extensive information, and education on all aspects of internet and interactive technology safety issues, with a focus on children and teenagers. The organisation's website provides educational materials and assistance for parents, educators and children. These services are offered through a worldwide organization comprised entirely of volunteers who administer specialized websites and programmes.

The websites described above are only a few of many US-based websites offering parents and children online safety advice[60]. For a more comprehensive overview of awareness-raising initiatives in the US, please see the forthcoming report by the Family Online Safety Institute (FOSI), to be launch in December 2007[61].

5.4 Illegal content

In the US, the CyberTipline provides a centralised resource for reporting child abuse content, run by the National Centre for Missing and Abused Children. CyberTipline is also a member of INHOPE, providing information about such content hosted outside the US, and receiving reports about US-hosted content.

[55] See http://kids.getnetwise.org/safetyguide and http://kids.getnetwise.org/tools
[56] www.iSafe.org
[57] http://pauseparentplay.org
[58] www.projectonlinesafety.com
[59] www.wiredsafety.org
[60] Other major websites include Blogsafety.com, Netsmartz.org, Pointsmartclicksafe.com, Safekids.com, Safeteens.com, Staysafe.org, StopCyberbullying.org, Cyberbully.org, Stoptextbully.com, Takeparentalcontrol.org, Wiredkids.org, Wiredcops.org, Protectkids.com, and Chatdanger.com.
[61] http://www.fosi.org

CyberTipline can issue takedown notices to hosts which have registered with the service, in the event that domestically hosted illegal content is identified. Although the leading ISPs, such as Verizon, AT&T, or Comcast are all registered, there are thousands of US hosts which are not part of the scheme, and where is therefore no formal takedown process in place. CyberTipline does not collate the information it gathers about domestic or internationally hosted illegal content into a blacklist for service providers.

6 Australia

6.1 Introduction

According to the Australian Bureau of Statistics, over 60% of Australian households had internet access in March 2006, with around half of these subscribing to broadband.[62]

The communications sector in Australia is overseen by the Australian Communications and Media Authority (ACMA). ACMA is a converged regulator, and as part of its remit is responsible for licensing and content regulation in broadcasting as well as online.

Online content regulation in Australia is carried out by ACMA based on a national classification framework, administered by the Classification Board. The framework distinguishes between content that is illegal ('prohibited'), and content that should not be made available to minors (both 'R18+' and 'X18+'). The enforcement of the regulatory framework is carried out by ACMA in co-operation with the internet industry and the public. In addition to these measures, a major Government initiative, *NetAlert*, has been launched to make free filtering tools available to all Australian households and to raise awareness of internet safety issues.

Australia – relevant regulatory authorities

Authority	Remit
Australian Media and Communications Authority (ACMA)	The government authority that oversees licensing and content regulation in electronic media. It directly oversees *NetAlert-Outreach and Research, part of* the Government's internet safety initiative.
The Classification Board	A federal government body that classifies films, computer games and publications. It also provides classifications to ACMA of internet content.

6.2 Internet content regulation scheme

In Australia, a national scheme for regulating internet content was established in 2000 under the provisions of the 1992 Broadcasting Services Act. The Act sets out the procedures for regulating online content, and grants the Australian Communications and Media Authority (ACMA) responsibility for monitoring and enforcing controls. Under the regulatory scheme, ACMA:

- investigates complaints about internet content and internet gambling services;
- encourages the development and registration of legally enforceable codes of practice for the internet industry;
- provides advice and information about internet safety issues, especially those relating to children's use of the internet; and
- undertakes a range of supporting activities including research and international liaison.

[62] http://www.abs.gov.au/Ausstats/abs@.nsf/0/acc2d18cc958bc7bca2568a9001393ae?OpenDocument

- ACMA also enforces Australia's anti-spam law and makes rules about accessing the internet through premium mobile phone services.

Definitions of prohibited and harmful internet content

Online content regulation operates under a national classification scheme, which applies to online content, and also to other media forms such as publications, films and video games. The National Classification Code defines categories of content which is prohibited (RC or 'refused classification') or unsuitable for minors (R18+, X 18+)**.** The classifications apply to content on the internet, which is defined as the World Wide Web; postings on newsgroups and bulletin boards; and files that can downloaded via 'peer-to-peer' software. The regulatory scheme does not cover ordinary email, chat services that are not stored, voice over the internet, audio/video content that is streamed 'live' or other content accessed in real time without being previously stored.

The RC classification includes content that contains:

- child pornography;
- bestiality;
- excessive violence or sexual violence;
- detailed instruction in crime, violence or drug use; and/or
- material that advocates the doing of a terrorist act.

The X18+ classification includes internet content that:

- contains actual sexual activity;
- depicts high-level violence;
- shows implied or simulated sexual activity; or
- other high impact material.

Providers of content hosted in Australia that falls into the classification R18+ must ensure that a restricted access system in place. The procedures for gaining access to content that is likely to be classified R18+ are defined by the Classification Board. The process relies on credit card validation as a means to check that a person is 18 or older. If no access restriction is in place for content likely to be classified as R18 content, it is treated as potentially prohibited content under the regulatory scheme.

Public complaints about potentially prohibited content

ACMA administers a complaints system on its website, allowing Australian residents to submit complaints about potentially prohibited content. ACMA may seek a formal decision from the Board on classifying the content reported to it, or it may make its own assessment.

If content is hosted in Australia and is prohibited, or is likely to be prohibited, ACMA will direct the internet content host to remove the content from its service.

If content is not hosted in Australia and is prohibited, or likely to be prohibited, ACMA notifies the suppliers of approved filters, in accordance with the internet Industry Association's code of practice. If the content is deemed to be sufficiently serious (for example, illegal material such as child pornography), ACMA will refer the material to the appropriate law enforcement agency or INHOPE accredited hotline.

For both Australian and overseas content, ACMA prepares a report stating the reasons for its decisions and describing the actions taken in relation to the reported content.

ACMA is a member of the International Association of Hotline Providers (INHOPE) and runs Australia's hotline.

6.3 The role of industry

Industry codes of practice

The co-regulatory scheme for internet content is implemented though codes of practice adopted by the internet industry. The matters that must be dealt with in the codes are specified in Schedule 5 to the Broadcasting Services Act. The three codes were developed by the internet Industry Association (IIA) and apply to all Australian ISPs and internet content hosts (ICHs). The ACMA may direct an ISP or ICH to comply with a code, if they are not satisfied that they are not already doing so. Failure to comply with such a direction may amount to an offence under the Act.

- Content Code 1 sets out obligations for content hosts in Australia.
- Content Code 2 contains requirements for ISPs to Australian-hosted content.
- Content Code 3: contains requirements for ISPs to overseas-hosted content.

Codes 1 and 2 aim to improve internet users' access to tools and information on internet safety. They require ISPs to display relevant links prominently on their home pages, and to provide regular updates during the year.

Content Code 2 also contains rules for content delivered to mobile phones with audio-visual capabilities. This code prohibits mobile content that is, or would be, classified RC or X 18+, and requires access to content classified R18+ or MA15+ to be restricted to users who 'opt in' to such services and verify that they are 18 or older. The content codes use the National Classification Code categories that apply to films, DVDs and computer games. This will help ensure consistent treatment of content across fixed and mobile entertainment platforms.

Content Code 3 contains a process for dealing with overseas-hosted internet content that has been the subject of a complaint to ACMA and found to be prohibited. Such content is notified to the makers of selected internet filter products, which ISPs must make available to their customers at the time an account is opened, either directly or via a filter software portal maintained by the IIA.

Figure 2: Key ISP requirements set out in the codes[63]

Clause	Requirement
10.1	Take reasonable steps to ensure that internet access accounts are not provided to minors without the consent of a parent, teacher or other responsible adult
11.1. (a)	Encourage those subscribers who are content providers to use appropriate warnings/labelling systems about content unsuitable for children
11.1 (b)	Take reasonable steps to inform subscribers who are also content providers that they must not place on the service content that contravenes state, territory or Commonwealth law
2.1/12.2.	Provide a prominently displayed and easily accessible online safety button or ladybird seal on the homepage
19.3	Make available one or more IIA Family Friendly Filters
19.4	If the ISP seeks to charge for the provision of a filter, the charge must not exceed the total cost incurred by the ISP in obtaining, supplying or supporting that filter
19.6	Inform users every four months of the role of filters and where to obtain them.

ACMA carries out audits of industry compliance with the code. The latest audit was completed in April 2006, and found a high level of industry compliance. All internet service providers were found to be compliant with the codes' consumer protection obligations, including the enhanced provisions relating to online safety information. A small number of ISPs needed to adopt further measures on ensuring that internet access accounts were not provided to minors without parental knowledge. In all of these cases, full compliance was achieved by 31 March 2006.

The IIA Family Friendly programme

ISPs, content hosts and mobile service providers which are compliant with the relevant sections of the content codes are eligible to advertise their compliance with the IIA *Family Friendly* programme, by displaying the 'Ladybird Seal' on their safety web page and on their products and services.

Suppliers can also show that their products or services have met the minimum criteria, as set out in the relevant Code, by displaying the 'Ladybird Seal'.

The IIA maintains a public register on its website of IIA *Family Friendly* filters and all ISPs and mobile service providers which comply with the *Family Friendly* programme.

6.4 Extended regulatory framework to apply from 2008

The Communications Legislation Amendment (Content Services) Act 2007 was given Royal Assent in July this year. This introduces a new Schedule ('Schedule 7') to the Broadcasting Services Act 1992. The regulatory framework will apply to stored content services and also to 'live' content services, such as chat services, that are delivered via a carriage service. It will also apply to user-generated content and content on social networking sites. Schedule 7 will take effect from late January 2008.

[63] Please note that this is only a selection of requirements. For more detail, please see the Codes as well as ACMA's 2006 Audit Report. The documents are on ACMA's website at http://www.acma.gov.au/WEB/STANDARD/pc=PC_90080

The key features of the regulatory framework are:

- a prohibition on X18+ and RC content;
- a prohibition on R18+ content, unless it is subject to appropriate access restrictions;
- a new prohibition on MA15+ content, unless it is subject to appropriate access arrangements;
- 'take down' or 'access cessation' notices to remove access to content that is the subject of a complaint; and
- a co-regulatory approach that provides for the development of industry codes to address issues including the assessment of content, procedures for handling complaints about content and increasing awareness of potential safety issues associated with the use of content.

6.5 NetAlert: promoting filtering and safe internet use

In August 2007 the Australian Government introduced *NetAlert*, a major internet safety initiative consisting of a wide range of activities. The initiative includes two major components:

- The **Protecting Australian Families Online (PAFO)** scheme is managed by the Department of Communications, Information Technology and the Arts (DCITA)[64]. Under this initiative, the National Filter Scheme has been set up to provide every Australian household and public library with access to a free internet content filter. The scheme also foresees the provision of network-layer parental control services by ISPs in the future.
- The **Outreach and Research programme** is managed by AMCA and includes major awareness campaigns and ongoing research into filtering technologies. In August 2007, the government announced that over $11.7 million over four years will be provided to ACMA to increase its outreach activities to all Australian states and territories.

Filtering tools

The National Filter Scheme was set up to provide free filtering software to all Australian residents via internet download or by post. The Scheme also operates a website that allows the download of free filters, and contains information about all aspects of internet safety. It also offers a national helpline to provide advice about protecting children online and on the use of filtering tools.

The take-up of filtering tools has been growing in Australia over the past few years. According to a 2005 study of Australian families, 35% of parents used software to filter out inappropriate websites – double the take-up level recorded by the 2001 ABA study. The provision of free filters also stimulates take-up: data shared with Ofcom by the communications regulator ACMA show that over 100,000 households had opted for free filtering tools provided by the *NetAlert* initiative by November 2007.

[64] Please see http://www.dcita.gov.au

The options for implementing network-layer filtering nationally are currently being considered, based on a trial carried out in Tasmania. An initial feasibility study[65] commissioned jointly by the Australian government and by an internet safety body in 2006 found that the use of filters significantly reduced network performance, with degradation levels ranging between 18% and 28%. This was especially an issue for larger ISPs, due to network architecture and design issues. However, the study found that only one in six participants in its study noticed a slowing down of the service.

Accuracy testing showed that the filters gave reasonable results against a restricted content list, although only one filter tested achieved 100% blocking. In addition, blocking performance against a category list of sites was variable and generally less effective, with the highest scoring filter blocking 76% of the sites, and two filters only blocking 59% of restricted URLs. Only two of the filters provided 100% blocking of redirectors, suggesting that redirectors could provide a means of bypassing filtering tools for those wishing to do this. The study noted in its conclusions that, as filtering technologies continue to improve, an ongoing testing regime was essential to keep pace with changes.

Awareness-raising initiatives

ACMA's work in publicising online safety programmes has recently been augmented as part of the *NetAlert* suite of initiatives and now includes:

- research into current trends in internet safety;
- undertaking targeted awareness campaigns and activities, including programmes in schools and in the community; and
- establishing links with industry, and with other similarly focused agencies, to enable consistency in messaging, adoption of best practice, and general exchange of information.

A number of major awareness-raising projects are being undertaken as part of the *NetAlert* initiative, for example:

- **The Cybersafe Schools programme** aims to educate and empower students on safe use of the internet. It provides teaches with curriculum support materials to enable them to deliver effective education programmes. It provides students with learning activities that are relevant, effective and created specifically for their level of education. The programme includes three elements: the *CyberNetrix* programme aimed at secondary schools, the *CyberQuoll* programme for primary schools, and a programme of professional development for teachers.
- **Cybersmart Detectives** builds on the Net Detectives programme initially developed by UK-based agency Childnet International, and now independently operated by E-ngage*live*. The activity is an online game that teaches children key internet safety messages in a safe environment. Children work online in real time liaising with community professionals to solve an internet-themed problem. The activity is based in the school environment, and brings together a number of agencies with an interest in promoting online safety for young people, including state and federal police, internet industry representatives and child welfare advocates. ACMA supports the activity by registering the teams, moderating real-time interactions in the online

[65] http://www.netalert.gov.au/advice/publications/reports/a_study_on_server_based_internet_filters/overall_findings.html

environment, and providing additional materials for teachers and schools and follow-up activities to reinforce the safety message.

- **Netty's World** is an interactive learning environment designed for young children (aged 2-7) to learn about internet safety issues. *NetAlert* encourages parents to take their children through the online storybook, '*Netty's Net Adventure*' in which internet safety messages are revealed through five adventures. Children can also join "*Netty's Club*" where offline internet safety activities (such as bookmarks, stickers and pencil holders) are sent free by post. The offline activities help remind children of the five 'forget-me-nots' they learned in *Netty's World*.

6.6 Illegal content

As in France and Germany, the systems for managing illegal content and potentially harmful (adults-only) content are integrated. The ACMA operates a hotline for complaints about illegal content and harmful content which is not access-controlled (e.g. through age-verification tools).

For domestically hosted content which is in breach, the ACMA can direct the host take content down. In addition, the ACMA compiles a blacklist of internationally hosted content, which is distributed the providers filtering software. While this use of a blacklist model will help improve the effectiveness of filters, and their consistency with Australian content standards, it will not directly affect the availability of illegal content such as child abuse images for adults who do not use a filtering product. However, if Australia succeeds in imposing the requirement that ISPs offer network layer filtering, the blacklist could have a wider impact

7 The Republic of Korea

7.1 Introduction

The Republic of Korea has one of the highest internet and broadband penetration rates in the world. In June 2007, there were 14.4 million households with broadband subscriptions, suggesting a 90% penetration rate, according to government statistics.[66]

The Ministry of Information and Communications (MIC) is the regulatory body for the Korean communications sector, including the internet. A number of regulatory bodies reporting to the Ministry are responsible for different types of content. The Korean Broadcasting Commission is in charge of television, while the Korean Media Rating Board oversees the film sector. The Korean internet Safety Commission (KISCOM) is responsible for regulating internet content, including issues relating to child protection online. Finally, the Korea Information Security Agency (KISA) is responsible for information security frameworks, with particular focus on internet security breaches, spam, privacy protection and general information security education.

Korea - communications regulatory authorities

Authority	Remit
Ministry of Information and Communications (MIC)	The Government ministry that oversees all Korean media, including the internet
Korean Internet Safety Commission (KISCOM)	Under the supervision of MIC, it is charged with protecting children online through a variety of awareness, monitoring and enforcement activities.
Korea Information Security Agency	Responsible for information security frameworks, with particular focus on internet security breaches, spam, privacy protection and general information security education
Korean Broadcasting Commission (KBC)	Authority responsible for regulation of the broadcasting sector, including administration of channel performance, broadcasting programmes and advertising, ownership regime, authorisation of broadcasting services.
Korean Media Rating Board (KMRB)	Rating of films, phonograms, video products, games, performing works and advertising products.

Several pieces of primary legislation relate to online content. The National Security Law forbids dissemination of materials that can harm national security, including materials or speech that "will endanger the national security and the democratic freedom." The Telecommunications Business Act criminalises the transmission of content that compromises public safety, order, or morals. In addition, the Election Law was amended in 2004 to make illegal the internet dissemination of information that defames politicians, during their election campaigns.

KISCOM the key government body for online protection

[66] http://eng.mic.go.kr/eng/secureDN.tdf?seq=12&idx=2&board_id=E_04_03

South Korea's regulation in relation to harmful content dates back to 1992 when the Information and Communication Ethics Committee (ICEC) was established by the Government, and the national centre for reporting illegal and harmful online content was set up. The Korean internet Safety Commission (KISCOM) was then established in 1995 under the Telecommunications Business Act, with the main mission to "prevent the circulation of harmful materials and to promote a more ethical information communication culture".

The categories of online content that are regulated are defined as:

- Illegal content: defined as any content violating the positive law of the Republic of Korea, that is, information that infringes upon the public interests and social order.
- Harmful content: defined as content which can be harmful in a broad sense, and in particular, immoral, violent, obscene and speculative content.

KISCOM is a member of INHOPE, the international network of hotline providers, and APIC, the Asia-Pacific hotline network.

In 1992, KISCOM founded the Harmful Information Report Centre as a channel for internet users to report any information harmful to youth. It was renamed in 2002 as the Illegal and Harmful Content Information Report Centre, with key functions to:[67]

- receive and deal with reports from the public on illegal and harmful content;
- consult with those who have suffered from illegal and harmful content;
- operate the Cyber-Patrol community (a voluntary web monitoring scheme) and support its activities;
- co-operate with domestic and foreign organizations against illegal and harmful content;
- provide information for content use; and
- offer the "*Internet Bluebird*" automated reporting system.

7.2 Overview of control mechanisms

Content classification

KISCOM is responsible for designating content that is illegal, as well as harmful, both for society in general and for young people in particular. It also maintains a 'pass list' of websites considered beneficial for young people. Established in April 2000, the list is based on KISCOM's own research and public reports. Every recommended site for young people is entitled to display a specially-designed logo.

Filtering

According to a recent study of internet filtering[68], KISCOM operates a monitoring system for "illegal and harmful contents on the internet." It also defines and administers a voluntary "Internet Content Rating Service". The service consists of two elements: a rating system for

[67] Accessed on 28 October, 2007 from http://www.internet119.or.kr/english/internet119/history/.
[68] http://opennet.net/research/profiles/south-korea

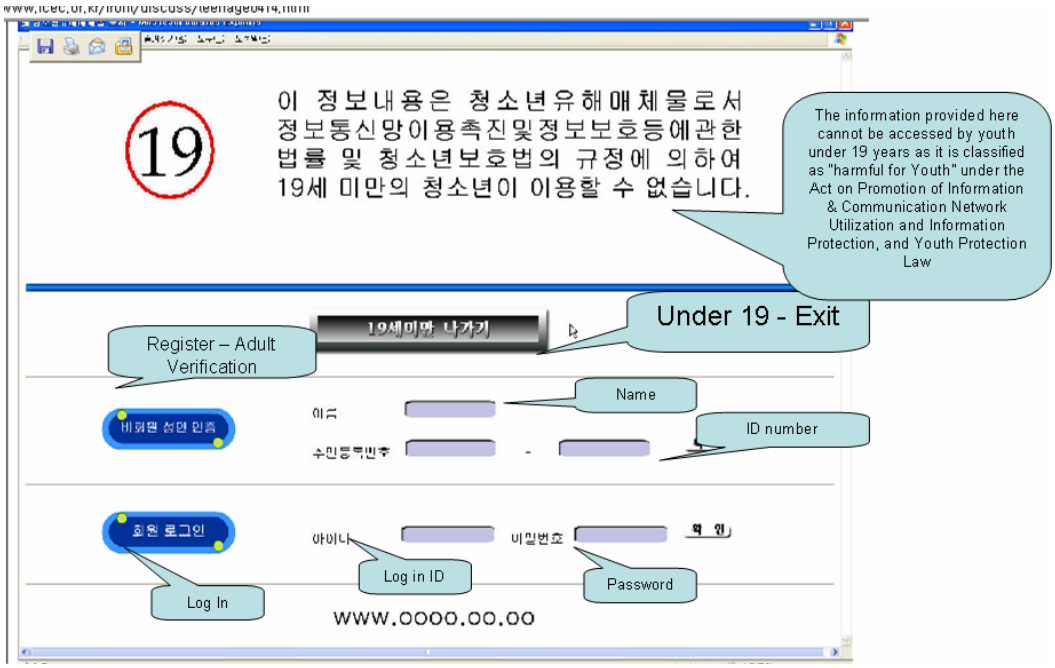
website providers to assess their sites' levels of appropriateness for minors, and filtering software for parents and schools that is compatible with the rating system.

According to the 2001 Internet Content Filtering Ordinance, Korean ISPs have a responsibility to block websites based on a content rating system provided by KISCOM. The Youth Protection Act of 1997 makes ISPs officially responsible, as "protectors of juveniles," for making inappropriate content on their networks inaccessible to children.

Age verification and parental consent requirements

The Youth Protection Act requires Korean providers of content defined as harmful for young people to restrict children's access by applying uniform front pages based on a format specified by KISCOM and based on the national ID and name information of the user, and real name information of the user, as shown in figure below.

Figure 3: The age verification interface specified by the regulator, KISCOM



In addition, the 1999 Act on Promotion of Information & Communication Network Utilization and Information Protection" provides guidelines for personal information protection in the private sector. It includes guidelines for information technology service providers to request parental consent via email, fax before recording any personal information about website users who are under 14 years of age.

Online abuse and real-name verification systems

A number of high-profile cases have led to a growing focus on the potential harm associated with the use of the internet and other new media in the recent years. Korean celebrities have endured invasions of privacy due to cyberbullying[69], raising awareness of the potential abuses inherent in new media.[70] The popularity of online gaming among Korean youth has also been an area of concern, and in 2006, the Government introduced a game addiction hotline as part of its broader counselling service for citizens.[71]

[69] http://www.asiamedia.ucla.edu/article.asp?parentid=20039.
[70] http://www.asiamedia.ucla.edu/article-eastasia.asp?parentid=68938.
[71] http://www.asiamedia.ucla.edu/article.asp?parentid=52984

More recently legislation for enacting a real-name online verification in Korea has been adopted. The initial public discussion of the issue started in 2003, and the legislation requiring the country's major portals to implement the system was formalised in December 2006, with half a year window for implementation, starting in July 2007. The system – called 'the limited personal identity verification system' - aims to prevent people using popular portals and forums from posting malicious messages or obscenities which would be available to a large number of people.

The law requires 35 selected service providers – online media sites with more than 200,000 users per day and portals with more than 300,000 users per day– to implement the new Limited Personal Identity Verification System. The service providers are required to add software to their sites that requests users to enter their name and ID registration number. This identity information can then be cross-referenced to the credit agency databases (there are four such databases in Korea, covering the vast majority of the population) which confirm whether the information is valid. Implementation of the system is monitored by KISCOM, and failure to comply results in a fine. Some other sites – for example on-line game companies – were already using similar systems to ensure payment and to prevent minors from using their sites without permission from their parents.

As identify theft was one of the concerns about the scheme, the Korean government brought in an 'I Pin' system. The "I Pin" allows an individual to register a PIN number and this number instead of their official identity registration details.

According to a survey by the Ministry of Information and Communications, these measures have lead to a slight reduction in the volume of malicious comments on the nation's major online bulletin boards in the first months since implementation. [72]

Awareness- raising

KISCOM also works to promote a "sound cyber culture" by disseminating materials about communications ethics, acting as an educational institution to raise awareness of internet safety issues, and carrying out information campaigns about internet safety. It provides support for victims of cybercrime and encourages industry self-regulatory activities.

[72] Accessed on 14 October 2007 from http://www.korea.net/news/news/newsView.asp?serial_no=20071004013