

**Term of Reference**  
on  
**Child Pornography on the**  
**Internet**  
for the  
**Advisory Council of Jurists,**  
**Asia Pacific Forum of National**  
**Human Rights Institutions**

**Background**  
**Paper**

Prepared by  
Secretariat of the Asia Pacific Forum of National Human Rights Institutions

July 2000

# Contents

---

<b>Preface</b>	<b>1</b>
<b>Introduction</b>	<b>3</b>
<b>Chapter One</b>	<b>6</b>
<b>Chapter Two</b>	<b>22</b>
<b>Conclusions</b>	<b>45</b>
<b>Appendices</b>	

## Preface

---

At a meeting held in Darwin, Australia in July 1996 representatives of the national human rights commissions of Australia, India, Indonesia and New Zealand agreed to the establishment of the Asia Pacific Forum of National Human Rights Institutions. The national human rights commissions of the Philippines, Sri Lanka<sup>1</sup> and Fiji<sup>2</sup> have since also become members of the Forum.

The objectives of the Forum as set out in the *Larrakia Declaration*<sup>3</sup> include:

To respond where possible with personnel and other support to requests from governments in the region for assistance in the establishment and development of national institutions,

To expand mutual support, co-operation and joint activity among member commissions through:

- information exchanges;
- training and development for Commission members and staff;
- development of joint positions on issues of common concern;
- undertaking joint projects;
- sharing expertise;
- periodical regional meetings;
- specialist regional seminars on common themes and needs.

To establish themselves for these purposes as an informal Asia-Pacific regional forum of national human rights institutions.

At the Third Annual Meeting of the Forum in Indonesia in September 1998, Forum members established an Advisory Council of Jurists to provide national human rights institutions in the region with jurisprudential guidance on contemporary human rights issues.<sup>4</sup> At the Fourth Annual Meeting held in Manila, the Philippines in September 1999 the members of the Forum:

- *affirmed* that there is a clear legal obligation under international human rights law to take all necessary measures against child pornography, including on the internet;
- *took* the interim view that relevant international treaties permit reasonable restrictions on the exercise of freedom of expression and that these restrictions justify action to combat child pornography; and

---

<sup>1</sup> Admitted at the Second Annual Meeting of the Asia Pacific Forum of National Human Rights Institutions, New Delhi, India, 1997.

<sup>2</sup> Admitted at the Fourth Annual Meeting of the Asia Pacific Forum of National Human Rights Institutions, Manila, the Philippines, 1999.

<sup>3</sup> 'Larrakia Declaration: Conclusions, recommendations and decision', First Asia Pacific Regional Workshop of National Human Rights Institutions, Darwin, Australia, 8-10 July 1996.

<sup>4</sup> 'Report of the Third Meeting of the Asia Pacific Forum of National Human Rights Institutions', 7th to 9th September 1998, Jakarta.

- *agreed* to make a reference on this issue to the Advisory Council of Jurists for its considered opinion and requested the Secretariat to develop a draft reference for Forum members for consideration between meetings.<sup>5</sup>

In March 2000 a draft term of reference was distributed to Forum members for comment. The term of reference subsequently adopted by Forum members is as follows:

The Asia Pacific Forum members call upon the Advisory Council of Jurists to advise and make recommendations as to the validity of measures taken to regulate child pornography on the Internet.

The Council is asked to have particular regard to whether such regulatory measures can be reconciled with national and international laws guaranteeing the rights to freedom of expression, privacy and freedom of information.

On the basis of this term of reference this background paper has been prepared to aid in the consideration of this issue by the Advisory Council of Jurists at the inaugural meeting of the Council in Rotarua, New Zealand, from 7-9 August 2000.

---

<sup>5</sup> Asia Pacific Forum of National Human Rights Institutions, 'Report of the Fourth Annual Meeting', Manila, 6 - 8 September 1999, p. 15.

## Introduction

---

There is no doubt that children used in the production of child pornography are harmed by the experience.<sup>6</sup> The children can be sexually abused and desensitised into believing that pornographic activity is normal. These children often experience a multitude of symptoms including emotional problems, withdrawal, anti-social behaviour, mood swings, depression, fear and anxiety. It has been reported that the children are also more likely to become perpetrators of child abuse themselves.<sup>7</sup>

The advances in recent years in various electronic technologies have had a profound impact on the production and distribution of child pornography. The increasing sophistication, availability, and cheapness of camcorders, videocassette recorders, microphonic devices, cameras and various kinds of software for home editing of pictures and videos have all had an impact on the production of child pornography. Special expertise is no longer a prerequisite in the production of child pornography for distribution on the Internet.

Advances in digital technology have had an influence on the images themselves, as it is now relatively easy to digitally manipulate photographs or computer generate images to produce what are known as pseudo-images.

The difference in using the Internet as a means to communicate and transmit child pornography, instead of the traditional means, is that there are no geographic boundaries, and that the receiver/user can easily become a potential supplier. The Internet can also be used to establish contact with the potential victims of child pornography – via, for example, on-line chat rooms.

---

<sup>6</sup> In the World Congress Against Commercial Sexual Exploitation of Children, Stockholm, August 1996 Declaration, section 9 it is stated: “ The commercial sexual exploitation of children can result in serious, lifelong, even life threatening consequences for the physical, psychological, spiritual, moral and social development of children, including the threat of early pregnancy, maternal mortality, injury, retarded development, physical disabilities and sexually transmitted diseases, including HIV/AIDS. Their right to enjoy childhood and to lead a productive, rewarding and dignified life is seriously compromised.”

<sup>7</sup> Background Document prepared for the Experts Meeting on Child Pornography on the Internet, Lyon, 28 May-29 May 1998.

It is difficult to estimate, with any degree of accuracy, the growth in the production and distribution of child pornography. This is due to the sheer volume of data being transmitted by the millions of people worldwide who are on-line at any one time. There is little doubt though, that the cheap, fast and secure way of distributing and storing child pornography the Internet offers, has lead to an increase.<sup>8</sup>

It must be kept in mind that the Internet technology is advancing at a blistering pace. Examples are the use of chat programs such as the Internet Relay Chat (IRC) where communication between two users is discrete and cannot be monitored, Invisible Mode (IM) which makes communication invisible to anyone not involved, and encryption systems.<sup>9</sup> This means that measures to combat child pornography on the Internet must constantly be adapting to also keep pace.

### **Scope of the report**

A function of this paper is to explain the difficulties, in terms of national and international law, of defining 'children' and 'child pornography'. Another function is to discuss child pornography in relation to the Internet. To gain an understanding of child pornography on the Internet it is first important to gain a basic understanding of the Internet itself. This background paper therefore provides details of not only the technological genesis of the Internet, but also the parallel evolution of the Internet ethos.

The paper gives a critique of the numerous technological measures to prevent access to child pornography on the Internet. This information highlights the technological issues regulators must be aware of. It is hoped that this will assist in deciding whether to regulate against content on the Internet, and if so, how to go about it. The paper also details additional non-technological, and non-legal measures taken to prevent child pornography on the Internet. It highlights that a

---

<sup>8</sup> The president of World Citizens' Movement to Protect Innocence in Danger, Homayra Sellier, has recently stated: "... there are only some fifty sites identified so far that reveal child pornography, torture of children and other forms of sadomasochism. But they are there. There are probably another hundred still lurking in virtual space and yet to be found. But these few sites deal in several hundred gigabytes of trafficked, illegal images", in UNESCO, World Citizens' Movement to Protect Innocence in Danger, paper by Homayra Sellier, President, 18 September 1999.

major problem of legislating against content on the Internet is the speed with which Internet technology is progressing.

The background paper provides some information on national and international legislation and regulation. It is beyond the scope of this paper, however, to go into detail on the national regulations of child pornography on the Internet in the Asia Pacific Region. This paper does, however, focus on some of the most important issues concerning the regulation of the Internet vs. freedom of expression, privacy and freedom of information.

It is beyond the scope of this paper to give details of every relevant Internet technology or discuss every issue relevant to child pornography. However, for further general information and discussions on the subject of child pornography on the Internet, please see the report to the Asia Pacific Forum of National Human Rights Institutions Fourth Annual Meeting in Manila, 6-8 September 1999, "Child Pornography on the Internet" and the numerous articles referred to in Appendix D of this paper.

---

<sup>9</sup> W. Bruggeman, Child Pornography – Police and justice cooperation, p.3., paper presented at the International Conference on Combating Child Pornography on the Internet, Vienna, 29 September to 1 October 1999.

# Chapter One

---

## 1. Definitions

### 1.1 Children and child pornography

In order to better understand the issues discussed in this paper it is important to have a clear comprehension of the definitions of 'children', 'child pornography' and the 'Internet'.

There is no definitive international definition of a 'child'. The International Labour Office (ILO) has defined a child as any person under the age of 18 in the Worst Forms of Child Labour Convention 1999. Article 2 of the Convention states that "the term child shall apply to all persons under the age of 18."<sup>10</sup>

However the United Nations Convention on the Rights of the Child (CROC) Article 1 defines a child as a person "below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier." Therefore in many countries the threshold age of a child for protection against exploitative use in pornography is determined by the age of consent.<sup>11</sup>

In addition there are several different definitions of child pornography in international treaties and in national legislation – so what constitutes child pornography in one jurisdiction may not be classified as child pornography in another.

The United Nations General Assembly<sup>12</sup> defines child pornography as

... any visual or audio material, which uses children in a sexual context. It consists of the visual depiction of a child engaged in explicit

---

<sup>10</sup> The Convention explicitly includes "the use, procuring or offering of a child ... for the production of pornography or for pornographic performances" within the definition of the worst forms of child labour.

<sup>11</sup> Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, *Macarthur Law Review*, (3) 1999 p. 147.

<sup>12</sup> World Congress Against Commercial Sexual Exploitation of Children, Stockholm, 27-31 August 1996 Background Document, p. 3.

sexual conduct, real or simulated, or the lewd exhibition of the genitals intended for the sexual gratification of the user, and involves the production, distribution and/or use of such material.<sup>13</sup>

The new Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography defines child pornography in Article 2 (c) as

... any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child, the dominant characteristic of which is depicted for a sexual purpose.<sup>14</sup>

However the draft Convention on Cybercrime, the UN Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, Interpol, the Council of Europe and others all use differing definitions of child pornography.<sup>15</sup>

The difficulties of adequately defining child pornography are illustrated when one considers the creation of 'pseudo-images' (i.e. images that are totally computer-generated) and animations of children. It has been argued that if an image is completely computer-generated then no child has suffered and accordingly no criminal act has taken place.<sup>16</sup>

To ensure there is no further proliferation of child pornography on the Internet, it is essential that international law adopt a clear and unambiguous working definition of both children and child pornography.

---

<sup>13</sup> UN General Assembly Document A/50/456, page 6.

<sup>14</sup> The Representative of Portugal on behalf of the European Union, said that the European Union understood the term "any representation" to mean visual representation and so did the representative of Japan, cf. UNESCO, E/CN.4/2000/75, 28 March 2000, Commission on Human Rights, Fifty-Sixth session, Agenda item 13, Rights of the Child paragraph 23-24.

<sup>15</sup> For these definitions and a discussion on the definitions please refer to Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, Macarthur Law Review, (3) 1999 p. 148ff.

<sup>16</sup> For a discussion on regulation of pseudo-images and animations, please see Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, Macarthur Law Review, (3) 1999 p. 158ff. Note that in the United Kingdom Section 1 of the Protection of Children Act 1978 outlaws the distribution of 'indecent pseudo-images' of children under the age of 16.

## 1.2 The Internet

The Internet is a global collection of networks connected and sharing information through a common set of protocols. Perhaps its most powerful feature is that it allows computers attached to networks to communicate openly and effectively regardless of make, architecture, operating system or location. Resources and network management are widely distributed throughout the world. There is no central point of control.

No one can completely own the Internet. Each network in the collection of interconnected networks is in charge of its own area, each is owned by distinct stakeholders and all work together according to common sets of rules and standards.<sup>17</sup>

In the late 1950s and early 1960s, paranoia of the Soviet bloc in general, and nuclear armament and other technological advances in particular, gave the impetus to significant advances in computer network technology. This resulted in the establishment in 1958 by the United States Department of Defence of the Advanced Research Projects Agency (ARPA) and a project to develop a military research network, or specifically, the world's first decentralised computer network.<sup>18</sup>

At that time the world of computers consisted of giant mainframes which required climate-controlled environments, rather than today's desktop PCs. In the event of a nuclear strike the Americans were concerned to maintain lines of communication. In theory, if an independent mainframe was bombed, communication would be lost, but if a network existed, communication could be maintained by 'detouring' information around the destroyed portion of the network.

---

<sup>17</sup> *Regulation of the Internet – A Technological Perspective*, G Miller, G Sinclair, D Sutherland & J Zilber, March 1999.

<sup>18</sup> ARPA is now known as DARPA, the Defence Advanced Research Projects Agency. DARPA's mission is as follows – 'The DARPA mission is to develop imaginative, innovative and often high-risk research ideas offering a significant technological impact that will go well beyond the normal evolutionary developmental approaches; and, to pursue these ideas from the demonstration of technical feasibility through the development of prototype systems' Source - Advanced Research Projects Agency; <http://www.arpa.mil>

By the means of packet switching technology information flows between two points without a direct fixed connection or circuit. This is a major advance on the telephone system. Data is broken into packets which contain addresses. The network delivers these packets to their destination by routing them through a succession of interconnected computers, called routers. Data is reassembled into its original form at the final destination. Each packet may take a different route, and if part of the network is slow or unavailable, the packet is sent through a different route. In 1968 ARPA issued a request for a proposal to build a network prototype. ARPAnet was the resulting network.

In the 1970s, many research agencies and universities recognising the potential advantages of such a network, decided to join the growing network. UCLA, MIT, Stanford and Harvard were all forerunners, and in 1973, the network crossed the Atlantic and was joined by such institutions as University College London and Norway's Royal Radar Establishment. Internet-related technology exploded from that time on with the introduction of electronic mail, File Transfer Protocol (FTP) and Newsgroups.

The 1980s saw the introduction of Transmission Control Protocol/Internet Protocol (TCP/IP), the protocols that provide reliable connectionless transmission of data over the Internet, the Domain Name System (DNS), the European UNIX Network (EUnet) and the Janet Academic Network (JANET). By this time ARPA had evolved to handle research traffic and MILnet had taken over the US military intelligence traffic. In 1986 the US National Science Foundation established NFSnet by linking five university super-computers. This now formed the infrastructure for a national Internet, and regional networks sprang up around these five nodes to allow other institutions to connect to the US national backbone. This allowed for an explosion of connections, especially from universities. The speed of connection increased at a rapid rate, allowing many more countries to join the network. This is seen to be point in time when the Internet became truly international.

In 1990 ARPA's role was reviewed. It had proved successful in theoretically being able to cope with a nuclear strike, but concurrently it created an additional military

weakness, namely espionage. Security was an issue, and in the final years of the Cold War there were rumours that Soviet agencies were hacking the Internet for military research data. ARPA ceased to operate and administration of the Internet was taken over by NFSnet.<sup>19</sup>

Today, the first level of provider is the Internet Service Provider (ISP). Users can have a contract with the ISP for a dial-in or dedicated connection to the ISP's equipment, which then gives them access to the Internet. Users may be clients or hosts, in that they may be accessing information or supplying it.

ISP's come in many different forms. They may be one of the following:

- a private profit making organisation;
- a public non-profit making organisation;
- an educational institution;
- a government department.

ISPs may then connect to a Regional Network Provider (RNP) that operates a wide area network and provides Internet connections across a geographic area. RNPs then connect to the Internet backbone through Network Access Points (NAPs). These backbones are operated by service providers who operate the networks that route the TCP/IP packets from point to point.

## **2. Technological Measures to Prevent Access to Child Pornography on the Internet**

### **2.1 Client-side filtering software**

Filtering software on the user's computer is one of the most common ways to restrict access to undesirable content such as child pornography. The user of the computer is in control of the filtering software and its use and whom any restrictions are going

---

<sup>19</sup> For further information on the history of the Internet please see the definitive work on key events and technologies in Hobbe's Internet Timeline © 1993-9 by Robert H Zakon. The current version is available at <http://www.isoc.org/zakon/Internet/History/HIT.html>

to affect (for example, other users of the same computer). Basically, filtering software compares some or all of the contents of a data file<sup>20</sup> retrieved by a user against a pre-defined set of rules, and determines whether to permit the file to be received and/or displayed by the user's computer. Common rules used for filtering include:

- blocking of selected files (e.g. web pages and newsgroups) or sites by comparing the URL,<sup>21</sup> name, or IP<sup>22</sup> address of each item against a list of prohibited files or sites (commonly called 'blacklisting');
- blocking of all files except pre-approved files or sites by comparing the URL, name or IP address of each item against a list of permitted files or sites (a less common practice, this is sometimes called 'whitelisting');
- filtering of selected files by scanning the header information of each file and comparing the contents of the header against a list of prohibited text strings (sequences of text characters);
- filtering of selected files by scanning the full text of each file and comparing the contents against a list of prohibited text strings;
- filtering of selected files or sites by comparing a 'rating label' included in the header information of each file or site against a pre-defined set of rating criteria.

All of the different types of filtering software are labour intensive. Human intervention is required to (i) determine whether blacklisting or whitelisting is necessary, (ii) create a list of prohibited words or phrases, after which the screening process is automated and (iii) establish a rating criteria and rate each file or site, after which rated files and sites can be screened in accordance with their ratings.

Some client-side filtering software can restrict the disclosure of personal information such as addresses and phone numbers. In this way parents and schools can ensure

---

<sup>20</sup> A file may be a document, a newsgroup, or any item that is stored in digital form and can be accessed on the Internet. Web sites generally consist of a large number of linked files.

<sup>21</sup> Universal Resource Locator, the address of a document on the World Wide Web.

<sup>22</sup> A unique address assigned to each Internet host. The IP number is used to identify the host in order to make a connection.

that children do not reveal personal information to paedophiles which may put them at risk.

The accuracy of filtering software is often questioned. Given the difficulty in its design and implementation, all filtering software prohibits access to a wide range of acceptable content, but also allows unacceptable content to slip through. When filtering is done on the basis of partial or full-text scanning of documents the first scenario tends to occur. Perhaps the best-known example of this problem was when AOL decided to use the word 'breast' as a criterion for filtering out pornography sites. This resulted in a whole range of legitimate sites being blocked. The content matter of these sites ranged from dealing with breast cancer to cookery sites containing recipes for chicken breasts. As a result of the public complaints AOL were forced to remove the word 'breast' from their filtering criteria.

Unacceptable sites slipping through the filter tends to occur when the filtering software blocks documents using a predetermined list of prohibited sites. In 1998 the World Wide Web had an estimated 300 million sites. The growth rate at that time was estimated to be 40,000 new sites per day. These figures indicate the volume of work that would be necessary to maintain a comprehensive and timely list of unacceptable sites. If attempted the quantity of reviewers necessary to fulfil such a task would no doubt prove to be prohibitively expensive. Even if this were not the case this approach ignores the constantly changing nature of the Internet. The content of books and movies are fixed upon publication. In theory, the contents of an Internet site can be updated hourly. Basically, if a URL or site is put on the banned list, the content is simply moved to another address. This increases the difficulty of keeping up-to-date records.

Yet another limitation of filtering is that users can request and receive web pages as email attachments or in encrypted form that defies filtering. Numerous on-line services exist that allow a user to request a web page via email. Others, such as 'Anonymizer', allow a user to anonymously request a web page by adding the URL of the web page to the URL of the Anonymizer web site. The Anonymizer then obtains and forwards the page to the user with an unidentifiable URL attached. Initially, services such as the Anonymizer were developed to defeat software that

records the sites visited by a user. However another application is to circumvent filtering software. As quickly as you can block access to such sites, new ones spring up as replacements, due to the ease with which sites can be copied and moved.

Other than filtering software using labelling systems, all filtering software currently available uses text-based criteria to determine which materials to block. Therefore there is currently no screening of Internet content consisting of graphics, audio and video. Work has begun on writing software to encompass the screening of such content, but it is in its infancy.

## **2.2 Server-side filtering at ISP Level**

Filtering can occur at the ISP level. While the user has no direct control over the functionality of the filter, the user indirectly, in nearly all countries, will have a choice of ISP. The user can therefore inquire as to which filters a particular ISP has installed and consequently which kind of data will be blocked out. On this basis the user can therefore decide which ISP to choose. It must be noted, however, that if all of the home country ISPs employ filtering software, a user who wishes to access unauthorised sites can simply subscribe to a foreign ISP that does not use such software.

If the host server is located in the country in question, then the government will have a number of existing remedies against individuals who contravene local laws. In theory, the government could require by law that the ISP install filtering software on the server that would prevent unacceptable content from being transferred to users. However, the same general filtering problems, as discussed above, would still apply.

If the host server is located outside the country, the ISP would generally be outside the country's jurisdiction and the government would not have the authority to impose any requirements on the ISP. To implement server-side restrictions, it would be necessary to interpose proxy servers<sup>23</sup> or firewalls<sup>24</sup>, through which all data entering

---

<sup>23</sup> A proxy server is a server on which incoming Internet content is cached (stored) before being forwarded to the client.

<sup>24</sup> A firewall is a server that enforces network access or security policy.

the country would have to pass and be inspected before reaching the user. For most countries, the only intermediate network node through which the data absolutely must pass on its way to the user is the router at the user's ISP site. If the user accesses the Internet directly through a foreign ISP, there are no immediate network nodes within the country through which the data absolutely must pass on its way to the user.

Most countries have very few ISP regulations. In addition there are low commercial and legal barriers to entry and competition and expansion in the ISP sector is vigorous. The introduction of ISP-level firewall or proxy server requirements may simply mean that ISPs would re-locate in a country where they would not face such regulations.

With current technology the introduction of a firewall impacts the 'throughput' of the network by decreasing the number of bits per second passing through the router and increasing delays in the network. Surveys suggest that in order to minimise damage to performance created by the introduction of a firewall, it is necessary to limit the number of clients accessing the network through any single firewall device.<sup>25</sup> Major difficulties exist with reconciling the speed at which technology is developing with any requirement to increase monitoring of data with firewalls. Countries which attempted to go down this route could be disadvantaged in the race to keep up with Internet developments.

Supporters of filtering at the ISP-level often point to Singapore, which has a requirement for ISP-level filtering based on a list of prohibited sites. Singapore currently has only one backbone connection to the outside world and three ISPs. However such a situation is unusual with many countries in the region having numerous international connections and hundreds of ISPs. The cost of implementing content controls at the ISP level in such countries would be large and the degradation of network service would be significant (with consequent economic costs).

---

<sup>25</sup> KeyLabs, an independent US lab specializing in software and hardware testing in a networked environment, have tested extensively and found that performance suffers with the introduction of firewalls. The full report can be found at <http://www.keylabs.com/results/firebench/index.html>

### **2.3 Filtering at the backbone node or border-crossing level**

An alternative to filtering at the ISP level would be to install giant filtering facilities at all the points where the Internet backbone enters a country. Simply, this would be a larger scale operation to the ISP level model described above. Having to handle huge volumes of data would, however, present additional problems. Since the costs of caching and filtering increase exponentially as the volume of data increase, the costs of these facilities may be prohibitive. In addition, the introduction of even simple firewall filtering criteria at the backbone node or border-crossing level would have negative effects on network performance.

In addition, filtering at the either the local ISP level, the backbone router level, or the border-crossing level would still not stop people accessing unacceptable content where they could connect directly to an ISP outside the country. If restrictions in one country grew, it could be anticipated that there would be a corresponding growth in the number of users obtaining Internet access outside the country. If the government wished to restrict this type of behaviour, it would be faced with significant technological and logistical enforcement problems.

It could also be anticipated that if governments implemented such filtering measures there would be a proliferation of sites which would accept encrypted URLs and return encrypted web pages. This would mean that it would be virtually impossible to detect anything other than the server's name on the request side and it would also be equally impossible to examine the content delivered. The technology used by secure servers (such as those used for on-line banking and e-commerce) to prevent the theft of information as it is transferred from the client to the server or vice versa is a good template. The user would be able to simply type in the URL of the desired site and the encryption and transmission process would occur without the need for any further action on the part of the user. Alternatively, the user could use a search engine that would encrypt web page requests (made by the user clicking on a link on the search page) and return the requested page in the encrypted form. No special expertise on the part of the user would be required.

To prevent users from requesting encrypted content, the government could attempt to block all encrypted web browsing. Yet again, if enough sites offered this service (especially portal sites), then much useful content would be blocked. In addition, blocking encrypted transmissions would make e-commerce impossible, with serious negative impacts on the nation's economy.

## **2.4 Content labelling**

Labelling or rating schemes for Internet content have been proposed and developed by groups such as the Recreational Software Advisory Council on the Internet (RSACi), SafeSurf, ImageCensor, Cybersitter and Net Nanny. A simple age-based rating system, similar to that used in movies, can be used. Alternatively there is also a more sophisticated labelling system that rates on a number of criteria. The W3 Organisation has developed the 'Platform for Internet Content Selection' (PICS) labelling system. PICS supports labelling schemes of either type. Web browsers are now PICS compliant. This allows users to screen content in web sites based on the PICS criteria.

Several of the current filtering software use criteria that can be recognised by the PICS system. Examples of the PICS-compliant rating criteria established by RASCI and SafeSurf are attached as Appendix A. The development of specific country versions would be necessary, as rating criteria are not currently established on a country-by-country basis.

In theory, a labelling system such as PICS may provide more useful results than blocking or content-filtering software. These systems rely on either voluntary compliance (self-rating) by content creators, or rating and labelling by third parties. Labelling or rating by a large number of diverse groups and individuals would obviously result in inconsistency. Standards-based (or subjective) rating systems would result in the same item receiving different ratings from different groups or individuals.

On the other hand, rules-based (or objective) rating systems tend to obscure the kind of information that is often important in deciding whether access to a site should be

prohibited. For example, the RASCI defines “objective” rating categories providing 5 rating levels (from 0 – 4) in each of the four categories: nudity, sex, language and violence. Many classical works of art would qualify for Level 4 in the “nudity” category which is described as “frontal nudity”. While it may be possible to achieve a greater consistency across multiple reviewers using a rules-based rating system, such a system is unlikely to provide the kind of value-based information that would be most useful in making a decision to block certain content. For this reason, many content developers are opposed to a requirement for self-rating.

Questions have been raised as to the validity of those who develop the filtering, blocking and rating criteria. Why do they presume that they have the necessary skills and mandate to perform such a task? There are groups, such as the American Civil Liberties Union, who have serious misgivings as regards the effect upon freedom of information of filtering, blocking and rating. They argue that the rise in such schemes represents an attempt at censorship by subjecting controversial material to a multi-layered bureaucratic process. This will have a more detrimental effect upon individual publishers in comparison to large well-resourced corporations.<sup>26</sup>

## **2.5 Other than the World Wide Web**

A common misconception is that the Internet is another word for the World Wide Web. The Web is a virtual space of information, using text, pictures, sounds and video as a means of communication. Web pages are only one of the methods by which information is exchanged on the Internet. Other methods of exchange, such as Internet Relay Chat (IRC), email, Usenet messaging system and so forth, are simply not amenable to labelling. How is a constantly changing subject matter to be categorised? Would it be possible to rate a telephone conversation as it occurred? Rating email would require the interception and monitoring of millions of emails a day. Again, this is not a practical proposition. The rating of discussion groups could only be feasibly done on the basis of the group’s stated subject matter. However,

---

<sup>26</sup> Fahrenheit 451.2: Is Cyberspace Burning? How rating and Blocking Proposals May Torch Free Speech on the Internet’, American Civil Liberties Union, August 1997, <http://www.aclu.org/org/issues/cyber/burning.html>

the actual contributions may have no relation to the stated subject matter. It would not be possible to predict this in advance for the purpose of labelling.

Blocking using lists of prohibited text strings is possible. Certain filtering products will, for example, block a discussion group, terminate a chat session, or delete an email message if it contains prohibited text strings. The same general problems with text string blocking exist.

## **2.6 Hardware-based restrictions**

The V-CHIP is a computer chip that filters television content, and operates on principles very similar to those of ratings-based software filters. As there is currently no simple way of programming a television, this capability is hardwired into the television set. The V-CHIP allows the user to block reception of television programs on the basis of rating criteria embedded in the television broadcast. Televisions can be programmed by parents to ensure that their children do not watch inappropriate programs. As computer screens increase in size, so US authorities think the more likely it will be that people will watch television on their computers. US authorities are therefore now considering requiring computer manufactures to install V-CHIPS into computers, a move that is being vigorously opposed by computer manufactures and civil liberty groups. In theory, such a chip could be made to detect labels on web pages, as well as the ratings encoded in TV broadcasts. In being hardwired filtering software, the chip could filter for unacceptable content. This is if a comprehensive and consistent labelling system for Internet content existed in the first place. However, the installation of a hardwired filtering program would do nothing to overcome all the obstacles to the implementation of a coherent and effective labelling system discussed above. The only distinct advantage of a computer V-CHIP above and beyond filtering software is that it might be more difficult to uninstall. The same techniques to circumvent filtering software could apply to the chip.

## **3. Non-legal measures taken to prevent child pornography on the Internet**

### **3.1 Codes of practice**

In recent years drawing up codes of practice for ISPs has been a popular non-legal approach to prevent the proliferation of child pornography on the Internet. Depending on how ISPs are organised, a code of practice can effect them in the following ways:

- code of practice that covers all ISPs in a state;
- code of practice that covers some of the ISPs in a state;
- code of practice that covers an ISP that operates in several states.

Codes of Practice have a distinct advantage in comparison to regular legislation in that they are more likely to be easily changed to meet new technologies and environments. Codes of Practice are generally also more acceptable to the ISPs. Because ISPs have been more heavily involved in the formulation of codes of practice than regular legislation, there is a greater chance that implementation of codes of practice will be more effective than regular legislation.

### **3.2 Hotlines and NGOs**

It is extremely important that cooperation takes place between the law enforcing authorities and NGOs if child pornography on the Internet is to be limited. All countries police forces have limited time and resources to search for child pornography on the Internet. State authorities or NGOs can ease the resource burden of searching the Internet for child pornography by establishing hotlines. Those who come across such material can leave details with the hotline. These details can then be passed to the relevant authorities.

Some countries have chosen to have official hotlines administered directly by the police. Other countries have other governmental organisations in charge of the hotlines. Finally, some countries have chosen to cooperate with watch-organisations, such as Red Barnet in the Scandinavian countries, which tip off the police if they find or are informed of illegal content on the Internet.

Groups such as Cyber Angels<sup>27</sup> and Internet Rapid Response Team (IRRT) are examples of groups of users who have organised themselves across boundaries in netizen groups. An objective of these groups is to police the Internet for unacceptable content. Groups of hackers have also joined the fight to track down unacceptable sites. Rather than necessarily reporting sites to hotlines or the appropriate authorities, hackers are more likely to technically disrupt the operation of the site.

An example of a self-regulatory body that has been successful is The Internet Watch Foundation (IWF) in the United Kingdom. The success of the IWF in the UK has meant that it has become the quasi-public face of Internet regulation. One of its functions is to overview the use of the Internet and brings to the attention of ISPs any illegal materials that are reported to its hotline. Critics of the IWF are concerned, however, that the organisation retains the status of being a private organisation with a very public function and as such lacks the structures of accountability that are normally associated with organisations that have a public function.<sup>28</sup>

The 'Combating Child Pornography on the Internet' conference<sup>29</sup>, held in Hofburg, Vienna, from 29 September to 1 October 1999, made the following conclusion relating to hotlines.

The critical role of hotlines or tiplines. We stress the importance of hotlines or tiplines, be they established by governments, the industry or by NGOs. They play an important role in allowing users to have an easy point of contact with a trusted third party to whom they can report illegal content, knowing that action will be taken as a result. The work of hotlines has led to much useful information, and lead to the removal of many images from the Internet. Their legal status should be clarified and improved, in order to ensure that they are protected against civil

---

<sup>27</sup> CyberAngels are divided into Internet Safety Patrols and operate in four main areas of the Internet: Internet Relay Chat, Usenet, World Wide Web and America Online. Their function is to actively promote, preserve and protect netiquette which "is the collection of common rules of polite conduct that govern our use of the Internet". David S. Wall, Policing and the Regulation of the Internet, Criminal Law Review, Special Edition 1998, p.84.

<sup>28</sup> David S. Wall, Policing and the Regulation of the Internet, Criminal Law Review, Special Edition 1998, p.85f.

liability in connection with information they provide to law enforcement agencies.

We encourage the establishment of new hotlines in countries where they do not yet exist, building upon experiences and best practices of existing hotlines. We welcome the steps undertaken to improve the networks among them, in particular the announcement made at the conference of the establishment the new Internet Hotline Providers in Europe (INHOPE) Association which is open to other hotline initiatives.

### **3.3 Conferences & Action Plans etc.**

The UN, government and non-government organisations have in many different ways dealt with the issue of Child Pornography on the Internet at conferences, expert meetings and seminars. Many of these conferences and meetings have lead to Declarations and Action Plans which the governments of the participating countries have been encouraged to follow.

Apart from the international action plans concluded from conferences, several countries have set up their own national agendas for action. This form of action usually leads to a far more robust action plan. This is due to the participating countries not having minimal need to compromise content details, as compared with negotiating with more sceptical countries. These plans are often more detailed, resulting in more efficient and effective implementation.

A meeting titled “Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An International Challenge” was organised by UNESCO and held in Paris, 18-19 January 1999. The participants at the expert meeting put forward a declaration and an action plan, which proposes certain measures for UNESCO and for Governments, international agencies, NGOs, industry, educators, parents, law enforcement agencies and the media.

---

<sup>29</sup> For more information refer to <http://www.stop-childpornog.at/conc.asp>

Following the meeting, UNESCO set up an organisation and program called 'World Citizen's Movement to Protect Innocence in Danger' which also includes IT companies in its list of involved members.<sup>30</sup> This is an international education and safety program designed to gather information and create networks among all relevant industries and community action groups to avoid duplication of efforts regarding Internet education for children and for adults.<sup>31</sup>

Initially the Asia Pacific region was not included in this movement, as no one had offered to set up an action group, but in March 2000 kIDs.ap was formed. The executives of the group are professionals working full time in the area of victims/offender counselling, child protection advocacy and law enforcement. The Mission is to combat the sexual exploitation of children, in the Asia Pacific region via on line services. This is to be achieved by providing an all encompassing website that highlights the problem of sexual exploitation of children through the provision of timely information and technical reference of general and academic value, that reflects an homogenous commitment from NGOs, government bodies and all sections of the community.<sup>32</sup>

Several action plans highlight the basic need to ensure the provision of sex education in schools. This can be seen as a primary measure to prevent child pornography on the Internet, in that children are taught what is acceptable behaviour when interacting with adults. This thinking is reinforced by the United Nations Special Rapporteur on the sale of children, child prostitution and child pornography, Ms. Ofelia Calcetas-Santos. She recommended that "Sex education in schools should teach children not only to understand their bodies and their sexual development, but also that they have ownership over their bodies and that not even close family members can touch them in certain ways....."<sup>33</sup>

Further examples of government organisations and NGOs who have dealt with the issue of child pornography on the Internet are attached as Appendix E.

---

<sup>30</sup> UNESCO, World Citizens' Movement to Protect Innocence in Danger, paper by Homayra Sellier, President, 18 September 1999.

<sup>31</sup> UNESCO, kIDs.ap, Innocence in Danger – Asia/Pacific Newsletter, number 1.

<sup>32</sup> UNESCO, kIDs.ap, Innocence in Danger – Asia/Pacific Newsletter, number 1.

Examples of conferences on the subject are attached as Appendix F.

---

<sup>33</sup> UNESCO, E/CN.4/2000/73, 14 January 2000, Commission on Human Rights Fifty-sixth session, p.6 section 141 (b).

## Chapter Two

---

### 1. International and national regulation of child pornography on the internet

#### 1.1 International legislation

The international regulation of child pornography is currently seriously impeded by divergent and inconsistent approaches at the national level.<sup>34</sup> It is vital that child pornography on the Internet is regulated internationally and criminalised worldwide in order to avoid publishers of such material travelling to countries with no or poor laws against such crimes.

Several international treaties deal with the issue of child pornography either directly or indirectly. Some of the relevant international regulations are discussed in the following sections of this paper. A list of relevant international treaties, declarations, resolutions, action plans are attached as Appendix B.

The 'Combating Child Pornography on the Internet' conference<sup>35</sup>, held in Hofburg, Vienna, from 29 September to 1 October 1999, made the following conclusion relating to worldwide criminalisation.

**Worldwide criminalisation of child pornography.** The conference calls for worldwide criminalisation of the production, distribution, exportation, transmission, importation, intentional possession and advertising of child pornography. In addition to national legislation, efforts for an international instrument, such as the ongoing negotiations within the Council of Europe on a Convention against Cybercrime, are welcomed and encouraged. States, which have not yet done so, are called upon to enact appropriate legislation. There must be no safe haven. Progress in this area must be monitored. States, regional and

---

<sup>34</sup> Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, *Macarthur Law Review*, (3) 1999 p. 143.

international institutions are encouraged to work towards harmonisation of legislation. While recognising some remaining difficulties concerning its definition, the conference identified international minimum standards concerning the prohibition of child pornography, in particular in its application on the Internet.

## **1.2 The UN Convention on the Rights of the Child**

The Convention on the Rights of the Child (CROC) has been ratified by all in the world states (including all Asia Pacific Forum member states) except the United States and Somalia. It has become the centrepiece for international action to protect and promote the rights of the child.<sup>36</sup>

The articles most important to the issue of child pornography on the Internet are listed below, but it is a fundamental premise of the Convention that no single article or group of articles can be interpreted independently and that the entire Convention must be seen as indivisible. The Convention also suggests an integrated and comprehensive approach to action, which can guide and unify priorities, policies and programs.<sup>37</sup>

### Article 3

1. In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.
- (...)

This article outlines the fundamental principle of the Convention that all actions concerning the child shall take full account of his or her best interests.

---

<sup>35</sup> For more information refer to <http://www.stop-childpornog.at/conc.asp>

<sup>36</sup> The Director of the Office of the High Commissioner of Human Rights, United Nations Press Release, GA/SHC/3537, 27 October 1999, Third Committee discusses ways to protect children.

<sup>37</sup> Background Document, World Congress Against Commercial Sexual Exploitation of Children, Stockholm August 1996, p.2.

## Article 6

(....)

2. States Parties shall ensure to the maximum extent possible the survival and development of the child.

Among other things this article underlines the obligation of States to ensure that the child develops both physically and mentally. This is important to keep in mind when prevention of child pornography is discussed.

## Article 17

States Parties recognise the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health. To this end, States Parties shall:

(....)

- (e) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18.

This article imputes a responsibility on nation States and the international community to protect children from exposure to pornographic materials, and it is arguable that by inference, this requires the production and distribution of child pornography to be criminalised worldwide.<sup>38</sup>

## Article 19

1. States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms

of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.

2. Such protective measures should, as appropriate, include effective procedures for the establishment of social programs to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement.

This article is central to the discussion of child pornography on the Internet as it makes it an obligation for the State to protect the child from all forms of maltreatment including sexual abuse.

#### Article 32

1. States Parties recognise the right of the child to be protected from economic exploitation and from performing work that is likely to be hazardous or to interfere with the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral or social development.

(....)

#### Article 34

States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:

---

<sup>38</sup> Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, *Macarthur Law Review*, (3) 1999 p. 157.

- (a) The inducement or coercion of a child to engage in any unlawful sexual activity;
- (b) The exploitative use of children in prostitution or other unlawful sexual practices;
- (c) The exploitative use of children in pornographic performances and materials.

### **1.3 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2000:**

This new Optional Protocol has taken many years to formulate, requiring a great deal of compromise to reach a final wording acceptable to all countries. The Optional Protocol was open for signature at a special session in New York from 5 to 9 June 2000 and will be open again for signature 6 to 8 September 2000. The following provisions of the Optional Protocol are particularly relevant:

The States Parties to the present Protocol, (...) Concerned about the growing availability of child pornography on the Internet and other evolving technologies and recalling the International Conference on Combating Child Pornography on the Internet (Vienna, 1999) and, in particular, its conclusion calling for the worldwide criminalisation of the production, distribution, exportation, transmission, importance of closer cooperation and partnership between Governments and the Internet industry (...).”

#### Article 3

1. Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether these offences are committed domestically or transnationally or on an individual or organised basis:

(...)

(c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes, child pornography as defined in article 2 (c).

#### Article 8

1. States Parties shall adopt appropriate measures to protect the rights and interests of child victims of the practices prohibited under the present protocol at all stages of the criminal justice process, (....)

#### Article 9

1. States Parties shall adopt or strengthen, implement and disseminate laws, administrative measures, social policies and programs, to prevent the offences referred to in the present Protocol. (....)

#### Article 10

1. States Parties shall take all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements for the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving (...) child pornography (...).

### **1.4 Convention on Cyber Crime<sup>39</sup>**

The Council of Europe Committee of Ministers have established a Committee of Experts in Crime in Cyber Space (PC-CY). PC-CY has been working on a draft Convention on cyber crime since April 1997. The treaty is expected to determine a list of behaviour which future contracting parties will be required to criminalise. The

---

<sup>39</sup> For more information on the Draft Convention on cyber-crime please refer to Peter Csonka, Administrator and Secretary to Committee PC-CY, Council of Europe, Contribution to the Conference on combating child pornography on the Internet and Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, Macarthur Law Review, (3) 1999 p. 172 ff.

treaty will also address the question of jurisdiction in relation to information technology and attempt to provide answers to this problem. The work will take into account previous soft-law instruments, such as the relevant Council of Europe Recommendations and will also deal with child pornography on the Internet. It will include a *sui generis* provision whose main purpose will be to protect the physical and moral well being of children by preventing their development from being harmed by pornography. In this context child pornography should be understood as meaning any visual depiction of a minor in a sexually explicit conduct by means of a computer system.

The negotiations involve European, North American, Japanese and South African government representatives as well as scientific experts. The Council of Europe released a draft version of a Convention of crime in cyberspace for public discussion on 27 April 2000.<sup>40</sup> The text should be finalised by a group of experts by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as Autumn 2001.

## **1.5 International Covenant on Civil and Political Rights (ICCPR)**

The preamble to the ICCPR highlights states responsibility to observe human rights and freedoms. The production and distribution of child pornography on the Internet can be seen to be in contravention of a state's responsibilities. Listed below are the relevant sections of the ICCPR.

Considering that, (...) recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,

Recognising that these rights derive from the inherent dignity of the human person,

(...)

---

<sup>40</sup> The text of the draft Convention can be found on the following website:  
<http://conventions.coe.int/en/projects/cybercrime.htm>

Considering the obligation States under the Charter of the United Nations to promote universal respect for, and observance of, human rights and freedoms,

Realising that the individual, having duties to other individuals and to the community to which he belongs, is under a responsibility to strive for the promotion and observance of the rights recognised in the present Covenant,

(....)

#### Article 5

1. Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognised herein or at the limitation to a greater extent than is provided for in the present Covenant.

2. There shall be no restriction upon or derogation from any of the fundamental human rights recognised or existing in any State Party to the present Covenant pursuant to law, conventions, regulations or custom on the pretext that the present Covenant does not recognise such rights or that it recognises them to a lesser extent.

#### Article 7

No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. (....)

There is strong evidence to suggest most children are coerced (physically and emotionally) as a means to produce child pornography for distribution on the Internet. These conditions are in contravention of this article.

## **1.6 Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11 (European Convention on Human Rights)**

Listed below are the relevant sections of the European Convention on Human Rights.

### Article 3

No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

There is strong evidence to suggest most children are coerced (physically and emotionally) as a means to produce child pornography for distribution on the Internet. These conditions are in contravention of this article.

### Article 4

(....)

2. No one shall be required to perform forced or compulsory labour.

(....)

As above, there is strong evidence to suggest most children are coerced (physically and emotionally) as a means to produce child pornography for distribution on the Internet. These conditions are in contravention of this article.

### Article 17

Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.

## Article 18

The restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.

### **2. National legislation**

For examples of different national approaches to regulating the Internet, please see Appendix C.

The differences between the national legal systems and approaches of the national legislators to child pornography on the Internet have led to many different national legislative models. Some countries still rely on obscenity and prostitution laws, others have laws specifically on pornography and child pornography, but few countries actually have adopted laws specifically on child pornography on the Internet.

It is possible to identify six different approaches to national regulations as regards ISPs. These approaches sometimes overlap or are used in combination. They are as follows:<sup>41</sup>

- traditional criminal law provisions on responsibility;<sup>42</sup>
- press law regulations;
- specific responsibility regulations for computer networks;<sup>43</sup>

---

<sup>41</sup> For more details of the 6 different approaches please refer to: Prof. Dr. Ulrich Sieber, Internet law, Responsibility of Internet Providers – A comparative legal study with recommendations for future legal policy, Computer law & Security Report Vol. 15 no.5 1999, p.292ff.

<sup>42</sup> In the absence of specific legal provisions, the responsibility of the ISPs for third party offences is determined according to general criminal law principles on the distinction between positive act and omission, the guarantor's obligations under criminal law and the rules on perpetration and complicity. Examples are Germany, Denmark, Austria, Switzerland, Spain and Japan. Prof. cf+ Dr. Ulrich Sieber, Internet law, Responsibility of Internet Providers – A comparative legal study with recommendations for future legal policy, Computer law & Security Report Vol. 15 no.5 1999, p.292f.

<sup>43</sup> The relevant reform legislation incorporates different types of provisions: 1. One can differentiate between general cross-section regulations applying to all areas of the law (above all in continental Europe); 2. Regulations applying to specific legal areas (particularly in Anglo-American legal systems); 3. The third category applies to most, but not all, areas of the law (especially in Australia and Asia), cf Prof. Dr. Ulrich

- special support duties of ISPs;<sup>44</sup>
- specific authorisations for interdiction orders;
- self-regulation.

There are a range of different approaches as to how to criminalise child pornography on the Internet from country to country. Also, there are huge cultural and historical differences in the sentencing/punishment of the offender once convicted. Another basic difference which should also be mentioned in this context is whether a citizen of a country can be prosecuted for criminal actions in another country. This has proved to be relevant in areas such as sex-tourism and also relates to the application of the law in cases of child pornography on the Internet. This allows for the prosecution of those involved in the production and/or distribution of child pornography via the Internet who operate in countries with less strict legislation.

Clarity is required in the drafting of national and international legislation as to what constitutes child pornography on the Internet. Also flexibility must be built-in to allow for inevitable advances in technology. As technology evolves it may be necessary for revisions to be made to the legislation to close loopholes.

When discussing the criminalisation of offenders involved in child pornography on the Internet it is imperative that the legislation does not penalise the child victims. This is obvious for the following reasons:

- almost all of the children are forced to participate (either physically or threatened);
- they are too young to be sentenced;
- criminalisation of the child victims inevitably will make it harder to investigate and solve crime related to child pornography on the Internet.

---

Sieber, Internet law, Responsibility of Internet Providers – A comparative legal study with recommendations for future legal policy, Computer law & Security Report Vol. 15 no.5 1999, p. 294f.

<sup>44</sup> Firstly the obligation to provide filtering software to the customers but sometimes additionally the obligation to install filtering software, to give notice of criminal activity and to exclude certain persons from using the Internet, cf Prof. Dr. Ulrich Sieber, Internet law, Responsibility of Internet Providers – A comparative legal study with recommendations for future legal policy, Computer law & Security Report Vol. 15 no.5 1999, p. 301f.

At the World Congress against Commercial Sexual Exploitation of Children, held in Stockholm, August 1996, a declaration was made that the World Congress was committed to

... Criminalise .... other forms of sexual exploitation of children, and condemn and penalise all those offenders involved, whether local or foreign, while ensuring that the child victims of this practice are not penalised...

## **2.1 US Communication Decency Act**

On 8 February 1996 President Clinton signed into law the Communications Decency Act (CDA), which made it a crime to transmit 'patently offensive material' or to allow it to be transmitted over public computer networks where children might see it. It authorised the US government to restrict online speech and conduct with fines of \$250,000 and gaol sentences of up to two years for anyone who made such material available to children online.

The American Civil Liberties Union (ACLU) responded by bringing an action against the US Attorney General seeking to have the Act declared unconstitutional. In particular it claimed that the legislation offended constitutional amendments prohibiting vagueness in laws and restrictions on free speech. Part of the ACLU's case was that existing US federal legislation already provided adequate sanctions in respect of obscene material and child pornography. The term 'patently offensive material' was condemned as unhelpfully vague. One example given (and accepted by the court) was that the phrase would interfere with the dissemination of information concerning HIV/AIDS which was specifically targeted at the young (13 – 20 year olds account for 25 per cent of new HIV cases in the US). Another example related to the Pulitzer and Tony award-winning play *Angels in America*, which deals graphically with homosexuality and AIDS and which would undoubtedly, in the court's view, be caught by the CDA's net.

The US government responded by suggesting that it would be open to the American courts to interpret the legislation restrictively so that it was applied only to 'real'

pornography. The government also emphasised the statute's defences which exonerate ISPs who introduced systems of credit card verification or adult verification by password. These defences were subject to particularly stinging criticism from the court, which dismissed them as unworkable, costly, inefficient and most importantly, unsupported by any currently commercially available software.

The three judges hearing the matter in Philadelphia delivered their unanimous judgment in June 1996 and granted a temporary injunction preventing the implementation of the Act. "The Internet", commented District Judge Stewart Dalzell, "may fairly be characterised as a never-ending worldwide conversation. The government may not through the CDA, interrupt that conversation." The decision will be the matter of further appeal to and review by the US Supreme Court, but the history of American case law relating to restrictions on broadcast and telecommunications media suggests that it is unlikely that the CDA will survive.<sup>45</sup>

## **2.2 UK Regulation Investigatory Powers Bill**

The British Regulation of Investigatory Powers (RIP) Bill has completed its passage through the House of Lords. It is due to appear on the Statute Book on 5 October 2000. In the UK the bill has sparked a great deal of debate as regards its potential effect upon civil liberties. The bill provides for the installation of the equivalent of a remote controlled black box in all ISP's premises. These boxes are equipped with a direct line that is capable of relaying all data passing through the ISP to a special monitoring unit in MI5. The bill has four main parts:

- to deal with the interception of communications;
- surveillance and covert human intelligence sources;
- encryption;

---

<sup>45</sup> The Net Out of Control – A New Moral Panic: Censorship, Angus Hamilton, paper appeared in *Liberating Cyberspace*, Liberty Press

- scrutiny of investigatory powers and the functions of the intelligence services.

This will allow the Home Secretary to issue a warrant requiring ISPs to intercept communications of one or more subscribers. Concerns have been raised that the technique used to monitor traffic will allow others to monitor which website a person has visited, the pages downloaded, the addresses of those with whom you have exchanged email and the discussion groups and the chat rooms you have visited.

The Home Secretary also has the powers to compel the surrender of encryption keys. If you do not you are liable for a prison sentence of up to two years. If a person claims to have lost or forgotten the key then it is their responsibility to prove that to a court. The onus is therefore placed on the individual. The bill also makes it a criminal offence, punishable by five years in prison, to tell anyone (including a client, an employer or your family) that you have been served with an order to surrender encryption keys, or that you have been forced to hand over encrypted material in plaintext form.

The UK Government Communications Headquarters (GCHQ) is the intelligence gathering agency that is charged with helping safeguard the nation's security, economic well-being and to protect it against serious crime. It has increased powers under the bill to monitor external communications to and from the UK so as to cover internal data traffic.

The RIP Bill has been criticised as an invasion upon UK citizen's civil liberties. It is claimed by many civil liberty advocacy groups that from October 2000, nobody in the UK can feel confident that their Internet use is not being intercepted by security services. It leaves the UK as the only Western industrialised country with a law enabling the government to demand encryption keys from individuals and corporations.

### **3. Jurisdictional issues**

Under international criminal law the state competent to try the case is the state on whose territory the offence was committed. The difficulty with the Internet of course, is that it is a worldwide network so it is extremely difficult to pinpoint where the offence actually took place.<sup>46</sup>

In addition to these legal jurisdictional problems, there are also practical investigative difficulties. Two police forces working in different countries leads to reduced effectiveness and efficiency. Add another country to the equation and investigations become much more difficult, as language problems, different laws and practices will be encountered. In the first instance it may well be fairly easy to arrange informal communication for the early stages of an inquiry, when it is only necessary to pass information. However, when arrests are planned and evidence is required from different countries, the whole process slows down considerably.<sup>47</sup>

#### **4. Internet Service Providers**

In some countries the law enforcement authorities concentrate their efforts on those partly responsible for the Internet infrastructure, the ISPs. Some of the reasoning is that often the people actually placing the illegal content on the Internet are hard to identify, they publish on the Internet from abroad and do not have adequate funds to cover liability in civil law actions. Placing legal obligations on ISPs is achieved through the construction of “assistance” or “complicity” which is derived from the provision of the network infrastructure or in the omission to take appropriate control measures.<sup>48</sup>

You can divide the providers responsible for the network infrastructure into the following three categories:

- the network providers;
- the access providers (providing access to the network);

---

<sup>46</sup> Agnes Fournier de Saint Maur, Head of the Trafficking in Human Beings Branch, Interpol, The sexual abuse of children via the Internet: a new challenge for Interpol, p. 2, Paper presented at the conference Combating child pornography on the Internet, Vienna, 29 September – 1 October 1999.

<sup>47</sup> David J. Davis, Criminal Law and the Internet: The Investigator’s Perspective, Criminal Law Review, Special Edition, August 1999, p. 51.

<sup>48</sup> Prof. Dr. Ulrich Sieber, Internet law, Computer law & Security Report Vol. 15 no.5 1999 p. 291.

- the host service providers (providing the computer systems –servers– through which the data is not only transmitted but also stored).

It would not be technically feasible to undertake comprehensive monitoring of the flow of data by the first two types of providers, so regulation and coordination should, and can only lie with the host service providers.

Due to the large amount of data, it cannot be expected that the Internet/host Service Provider can have knowledge of all of the data they store, but if and when they do have knowledge (for instance by being tipped off) of illegal content they should remove such content. This is currently the practice and law in many countries throughout the world. In this context hotlines are a good tool in combating child pornography on the Internet.

The 'Combating Child Pornography on the Internet' conference<sup>49</sup>, held in Hofburg, Vienna, from 29 September to 1 October 1999, made the following conclusions relating to the Internet industry and ISPs.

- **The need for a global partnership among all actors and stakeholders.** We commit ourselves to the strengthening of partnerships at national and international levels among governments, the Internet industry, hotlines and NGOs. We need an alliance of legal regulation, law enforcement and industry self-regulation. Legal regulation by governments must be complemented by self-regulation of the ISPs. Law enforcement can only be successful with the strong support of ISPs and from hotlines. Governments, the industry and NGOs must join forces in capacity building and training, as well as in awareness raising and empowerment of Internet users;
- **Closer cooperation and partnership between governments and the Internet industry.** The Internet industry is an indispensable partner of law enforcement agencies in the investigation and

---

<sup>49</sup> For more information refer to <http://www.stop-childpornog.at/conc.asp>

prosecution of child pornography but also in exchange of experience and capacity building. Open questions concerning the relationship between law enforcement and the industry must be clarified, eg the reporting obligations of ISPs and the preservation of data for evidence. Clarification and harmonisation of the responsibilities and liabilities of the Internet industry is necessary. In particular:

- voluntary self-regulation and codes of conduct of the Internet industry should be strengthened and expanded. Such self-regulatory mechanisms must be compatible with and complementary to governmental legislation;
- the Internet industry and law enforcement shall work together to examine mechanisms for preventing data necessary to prosecute child pornography violations, so that the data exists when law enforcement obtains appropriate legal process;
- the Internet industry and law enforcement should consider together how technology might be used to identify child pornography;
- the Internet industry has a responsibility to empower Internet users, including children and young people, to protect themselves and, where applicable, their children against illegal content on the Internet (filtering, rating systems).

## **5. Regulation of the Internet vs. freedom of expression, privacy and freedom of information**

The legal regulation of child pornography on the Internet gives rise to a degree of dissension between the rights of the child on the one hand and the rights to freedom of expression, information and privacy on the other.<sup>50</sup>

In some quarters of the media the Internet has been portrayed as a playground for pornographers, terrorists and political extremists. The use of the Internet by these

---

<sup>50</sup> In ECPAT, Child Pornography on the Internet a Position paper for ECPAT International at <http://www.crin.org/iasc/sedoc11.html>

protagonists as a tool to ply their respective trades has been well documented. Politicians have also been increasingly alarmed at certain Internet activities. Illegal activity, (such as child pornography) criminal activity, (such as credit card fraud) and the ability with which people can communicate anonymously using encryption technology have all worried governments. Governments have decided that the Internet should be regulated. The legislative debate has now begun on how to go about such regulation.

Civil liberties groups such as Cyber-Rights & Cyber-Liberties (UK) and the American Civil Liberties Union (ACLU) argue that any attempts by governments to police the Internet are unworkable and are a threat to civil liberties. Such groups highlight the fact that the Internet should be a bastion of free speech and democracy.

Some hold the opinion that by attempting to restrict expression, it only makes expression a scapegoat for deeper social problems. It is argued that speech does not cause sexism, or racism, or homophobia, and nor in any real sense perpetuates them. The argument continues by stating that the causes of racism, for example, lie in a multitude of historical, sociological and physiological factors including exclusion, class, poverty, identification and so on. Criminalising racist speech does not address those factors.<sup>51</sup>

According to Nadine Strossen, President of the ACLU and one of the main lobbyists against the CDA:

The evidence suggests that censorship of any material increases an audience's desire to obtain the material and disposes the audience to be more receptive to it. Critical viewing skills, and the ability to regard media images sceptically and analytically, atrophy under a censorial regime. A public that learns to question everything it sees or hears is better equipped to reject culturally propagated values than is one that assumes the media have been purged of all 'incorrect' perspectives.<sup>52</sup>

---

<sup>51</sup> *Freedom of Expression: Censorship in Private Hands*, Adam Newey, appeared in *Liberating Cyberspace*, Liberty Press.

<sup>52</sup> *Defending Pornography: Free Speech, sex and the fight for Women's Rights*, Nadine Strossen, Scribner, 1995.

The juridical relationship between freedom of expression and viewpoint diversity is well established in the US, where the Supreme Court's interpretation of the First Amendment has historically been based on a marketplace of ideas model. This is because freedom of expression operates best in an unregulated marketplace, where opposing viewpoints can be aired, and the truth (or something approximating to it) can be discovered. Many see that of all the media, the Internet constitutes the broadest 'marketplace of ideas' model to date.

The question of whether to tolerate the intolerant is a classic dilemma. Karl Popper called this the 'paradox of toleration': in order to extend toleration as far as possible in society, we must in the last resort reserve the right to extinguish intolerant viewpoints.<sup>53</sup> The Internet gives an unprecedented platform and reach to intolerant viewpoints.

There is no doubt that children used in the production of child pornography are harmed by the experience. Details are given in the introduction regarding not only the physical harm but also the multitude of symptoms they suffer including emotional problems, withdrawal, anti-social behaviour, mood swings, depression, fear and anxiety. The argument above defending freedom of expression, along the lines that it does not cause actual harm, cannot be applicable as regards child pornography because of obvious harm it does actually cause. Child pornography on the Internet is seen to perpetuate the sexual exploitation of children.

Welcoming the UK IT industry's proposals to tackle child pornography on the Internet, developed with the Home Office and the Police, Science and Technology Minister Ian Taylor said:

This is not a question of censoring legal material or free speech. The Internet has never been a legal vacuum. Responsible service providers want to see the law upheld 'on-line' as well as 'off'. The core of this initiative is about dealing with material which breaks our existing

---

<sup>53</sup> *The open Society and its Enemies*, Vol 1, Karl Popper, Routledge 1966

laws, particularly where child pornography is involved. It is also about consumers as parents and teachers being able to control 'net access of the young and vulnerable in their charge, according to their own individual standards.

More information relating to freedom of speech is attached as Appendix G.

## **6. The right to freedom of expression and information**

### **6.1 Cultural differences**

When discussing the possible clash between the rights of the child, and the rights to freedom of expression and information, it must be kept in mind that what is considered harmful, indecent and/or illegal in one country may be merely provocative, controversial but legal in another. A simple example is the difference in what is considered 'a child' in relation to pornography (some countries have the age of 15 as the limit and others the age of 18). Another example is the difference in the legality of creating/possessing pseudo-photographs/images of children. This particular area is discussed in chapter 1.

Each country has its' own standards, values and cultural differences which will influence the question of how to regulate the Internet. For example, in Denmark a conscious decision has been made not to use filtering software on schools' computers as limiting access to information is seen as "contradictory to the Danish culture". Another reason given is that it is futile to use filters as the children can access the illegal information from other computers (e.g. Internet cafes) if they wish to. It is perceived that educating students only to search for legal and relevant information is a more appropriate practice than installing filtering software.

There is no doubt that the right to freedom of expression extends beyond socially and culturally acceptable statements and ideas. The European Court of Human Rights has stated:<sup>54</sup>

---

<sup>54</sup> Castells v. Spain, Application No. 11798/85, Series A, Vol. 236 (1992) 14 E.H.R.R. 445, § 42.

.... freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress. Subject to paragraph 2 of Article 10 [of the European Convention on Human Rights], it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance or broadmindedness without which there is no democratic society.

As regards fundamental freedoms, another point of criticism which has been put forward by civil liberties organisations is that the filters and rating systems (which to a certain extent can prevent the spreading of child pornography on the Internet) may result in a privatisation of censorship. By applying filters or using rating systems private companies can end up regulating the behaviour of people and Internet users' access to information. This is especially the case for the filters which are installed by the ISPs at entry level. These filters have been criticised as they take the choice out of the hands of the citizens.<sup>55</sup>

Several international treaties outline the right to freedom of expression. Some of the most important articles are quoted below:

## **6.2 The Universal Declaration of Human Rights**

### Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek,

---

<sup>55</sup> Economic and Social Committee of the European Commission, Opinion on the Proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet (OJEC, 98/C 214/08, Brussels-Luxembourg, July 10, 1998), pp.29-32 para. 3.4.

receive and import information and ideas through any media and regardless of frontiers.

### **6.3 The International Convention on Civil and Political Rights (ICCPR)**

#### Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputation of others;

(b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

### **6.4 The European Convention for the protection of Human Rights and Fundamental Freedoms**

#### Article 10

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

(....)

### **7. The right to privacy**

Another problem closely linked to the freedom of expression is the basic human right to privacy.

Sexual behaviour is traditionally considered in most countries' national legislation and in international treaties to come under the right to privacy. Accordingly, it is considered as sensitive information and can therefore not be registered by the police unless it is justified due to links to criminal activity.

The right to privacy is contained in several international human rights treaties. Some of the most relevant articles are listed below.

## **7.1 The International Convention on Civil and Political Rights**

### Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

## **7.2 The Universal Declaration of Human Rights**

### Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

## **7.2 The European Convention for the Protection of Human Rights and Fundamental Freedoms**

## Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The people agitating for no or less regulation of the Internet often mention these articles. National case law has so far not drawn the exact line between the competing rights of the best interest of the child and freedom of expression and information and the right to privacy. International law is increasingly being called upon to balance such competing rights. In the face of compelling evidence of the harmful effects of child pornography, international law has more recently tended to favour the rights of the child. In 1996, the Child Pornography Panel Report of the World Congress concluded that child pornography should be outside the protection of freedom of speech laws.<sup>56</sup>

It should also be kept in mind that the individual rights are not always absolute, i.e. they can be limited when conflicting with other basic human rights. This is not just the case in relation to child pornography but also in relation to for example hate speech.

An example of this kind of limitation is Article 10 (2) of the European Convention on Human Rights:

(...)

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions,

---

<sup>56</sup> In ECPAT, Child Pornography on the Internet a Position paper for ECPAT International at <http://www.crin.org/iasc/sedoc11.html>

restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

The European Court of Human Rights has developed the principle of proportionality, which states that restrictive measures that impinge on the basic principles embodied in the convention must meet “a real social need and be effective without being discriminatory or disproportionate in the restrictions they impose”. The protection of children from the harmful effects of child pornography must constitute a legitimate social need.<sup>57</sup>

---

<sup>57</sup> Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, *Macarthur Law Review*, (3) 1999 p. 163.

## Conclusions

---

Children used in the production of child pornography are subjected to a wide range of physical and emotional harm. The advances in various electronic technologies in recent years have made the production and distribution of child pornography cheaper, easier, faster, more efficient, more secure and more widespread.

When addressing the 'regulation of the Internet vs. freedom of expression, privacy and freedom of information' argument, in the light of the evidence of the harm it causes, it is difficult to find in favour of those advocating freedom of expression and speech.

Using the Internet to distribute child pornography has made the concept of geographic boundaries and state borders meaningless. National and International law must become more dynamic in responding to the new challenges that child pornography on the Internet poses. If child pornography on the Internet is to be effectively regulated it must be criminalised worldwide. Currently the perpetrators escape prosecution merely by moving their operations to countries with the minimum, in many cases non-existent, national child pornography legislation. It will always be a difficult process. The difficult task ahead is highlighted in that there is still no international definition for a 'child' or for 'child pornography'. Cultural differences must be addressed if vital general international definitions are to be made. A review of all international and national legislation relating to child pornography on the Internet would be a constructive start to the process.

If regulation is to be successful it seems that the development of national and international laws in tandem will be required. Currently, there are several international treaties declarations, resolutions and action plans which deal with the issue of child pornography either directly or indirectly. Equally, there are also several international treaties, declarations, resolutions and action plans which deal with the issue of freedom expression and freedom of speech. These must be taken into consideration when deciding on how to regulate.

Perhaps the most effective way of ensuring that development occurs at an international level is to establish a global network under the auspices of the UN comprising representatives of national governments, the judiciary, police, Internet industry and other stakeholders. A separate network in the Asia Pacific region could also be established. This network could then 'plug-into' the global network. This ensures the effectiveness and efficiency of any efforts made to tackle child pornography on the Internet.

It must be kept in mind that the Internet technology is advancing at a blistering pace. This means that measures to combat child pornography on the Internet must constantly be adapting to also keep pace. It appears to be easier to conclude that regulation is necessary than as to the nature of the regulation.

The Internet was designed in such a way as to avoid control. Consequently, it does not lend itself to any form of regulation. There are many different technological measures to prevent access to child pornography on the Internet. These methods are designed to prevent access rather than to tackle the proliferation of child pornography on the Internet. They may be useful tools to be used in the family home, in schools or in any other institutions which have responsibilities for children accessing the Internet, though it must be noted that they all have specific failings. The one thing that they have in common is that if the user wants to circumvent the particular system in use, they can do so. Again, the way in which the Internet has been designed is the reason why such circumvention is possible.

It appears that one of the most effective ways of regulating the Internet is to work closely with the Internet industry, and especially the ISPs. There are many examples of successful codes of practices and hotlines in existence around the world. Arguments have been given as to why it is difficult to justify that ISPs should be responsible for all the data that they host. Rather than attempting to regulate the ISPs themselves, it appears to be far more effective for the authorities to work collaboratively with them. This results in the ISPs making a more worthwhile contribution to formulating what sort of regulations should be adopted. Also, once such regulations have been established, then the ISPs are to be seen to be far more enthusiastic regarding their participation due to a sense of perceived empowerment.

There are many other methods of exchange via the Internet, such as IRC, email, Usenet messaging system and so forth, which are simply not amenable to labelling. Encryption is another feature of the Internet which must be taken into consideration. This is currently the battleground where regulators and the advocates of civil liberties on the Internet are waging a bloody battle. The UK RPI Bill being one way in which the authorities are attempting to gain the upper hand. Civil liberty groups claim this is at the price of citizens' civil liberties. Encryption technology poses a threat to regulation of the Internet. Those who are distributing child pornography on the Internet are less likely to be detected when communicating using encrypted data, and are hardly likely to be willing to relinquish their encryption keys if questioned. Encryption is just but one example of the difficulties faced by the authorities in attempting to regulate against child pornography on the Internet. As ways are found to overcome technology, technology itself has produced new ways of evading authorities

## Appendices

---

### A Examples of Rating Systems Criteria

#### RSACi Ratings

##### **Nudity**

- Level 0 – no nudity
- Level 1 – revealing attire
- Level 2 – partial nudity
- Level 3 – frontal nudity
- Level 4 – provocative frontal nudity

##### **Sex**

- Level 0 – innocent kissing or romance
- Level 1 – passionate kissing
- Level 2 – clothed sexual touching
- Level 3 – non-explicit sexual acts
- Level 4 – explicit sexual acts; sex crimes

##### **Language**

- Level 0 – no offensive language
- Level 1 – mild expletives
- Level 2 – profanity
- Level 3 – strong language; hate speech
- Level 4 – extreme hate speech; crude, vulgar language

##### **Violence**

- Level 0 – none or sports violence
- Level 1 – injury to human beings
- Level 2 – destruction of objects with implied social presence
- Level 3 – death to human beings; blood and gore
- Level 4 – wanton, gratuitous violence; rape

#### SafeSurf Ratings

##### **Age Range**

0. All ages
1. Older children
2. Teens
3. Older teens
4. Adult supervision recommended
5. Adults
6. Limited to adults
7. Adults only
8. Explicitly for adults

## **Profanity**

1. Subtle innuendo. Description – subtly implied through the use of slang.
2. Explicit innuendo. Description – explicitly implied through the use of slang.
3. Technical reference. Description – dictionary, encyclopaedic, news, technical references.
4. Non-graphic-artistic. Description – limited non-sexual expletives used in a [sic] artistic fashion.
5. Graphic-artistic. Description - non-sexual expletives used in a [sic] artistic fashion.
6. Graphic. Description – limited use of expletives and obscene gestures.
7. Detailed graphic. Description – casual use of expletives and obscene gestures.
8. Explicit vulgarity. Description – heavy use of vulgar language and obscene gestures. Unsupervised Chat Rooms.
9. Explicit and crude. Description – saturated with crude sexual references and gestures. Unsupervised Chat Rooms.

## **Heterosexual (also a separate Homosexual theme with the same criteria and descriptions) Themes**

1. Subtle innuendo. Description – subtly implied through the use of metaphor.
2. Explicit innuendo. Description – explicitly implied (not described) through the use of metaphor.
3. Technical reference. Description – dictionary, encyclopaedic, news, technical references.
4. Non-graphic-artistic. Description – limited metaphoric expletives used in a [sic] artistic fashion.
5. Graphic-artistic. Description – metaphoric descriptions used in a [sic] artistic fashion.
6. Graphic. Description – descriptions of intimate sexual acts.
7. Detailed graphic. Description – descriptions of intimate details of sexual acts.
8. Explicit graphic or inviting participation. Description – explicit descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised sexual Chat Rooms or Newsgroups.
9. Explicit and crude or explicitly inviting participation. Description – profane graphic descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised sexual Chat Rooms or Newsgroups.

## **Nudity**

1. Subtle innuendo. Description – subtly implied through the use of composition, lighting, shaping, revealing clothing etc.
2. Explicit innuendo. Description – explicitly implied (not shown) through the use of composition, lighting, shaping, revealing clothing etc.
3. Technical reference. Description – dictionary, encyclopaedic, news, technical references.
4. Non-graphic-artistic. Description – classic works of art presented in public museums for family viewing.
5. Graphic-artistic. Description – artistically presented without full frontal nudity.
6. Graphic. Description – artistically presented with full frontal nudity.
7. Detailed graphic. Description – erotic frontal nudity.

8. Explicit vulgarity. Description – pornographic presentation.
9. Explicit and crude. Description – explicit pornographic presentation.

## **B List of Relevant International Treaties, Declarations, Resolutions, Action Plans etc**

- Universal Declaration of Human Rights, 1948
- International Covenant on Civil and Political Rights, 1966
- International Covenant on Economic, Social and Cultural Rights, 1966
- UN Convention on the Rights of the Child, 1989
  - The Optional Protocol to the Convention on the Rights of the Child, on the sale of children, child prostitution and child pornography, submitted by UNESCO and adopted by the General Assembly on 25 May 2000. The Optional Protocol was opened for signature at the special session in New York from 5-9 June and 6-8 September.<sup>58</sup>
  - Program of Action of the United Nations Commission on Human Rights for the Prevention of the Sale of Children, Child Prostitution and Child Pornography, 1992
- UNESCO
  - United Nations High Commissioner on Human Rights, Commission on Human Rights Resolution 1999/40, 26 April 1999
- World Declaration on the Survival, Protection and Development of Children and its Plan of Action, 1990
- Vienna Declaration and Programme of Action of the World Conference on Human Rights, 1993
- The Stockholm Declaration and Agenda for Action adopted by the Stockholm Congress on Commercial Sexual Exploitation of Children, 1996
- ILO, Worst forms of Child Labour Convention, 1999
- EU legislation etc.

---

<sup>58</sup> United Nations Press Release, Resumed Fifty-fourth General Assembly Plenary, 25 May 2000, 97<sup>th</sup> Meeting (AM).

- Joint Action to Combat trafficking in Human Beings & Sexual Exploitation of Children of 24.02.97
- Council of Europe:
  - The European Convention for the Protection of Human Rights and Fundamental Freedoms
  - Recommendation No. R (89) 9 on Computer-related crime
  - Recommendation No. R (95) 13 concerning Problems of Criminal Procedural law connected with information technology
  - Recommendation No. R (91) 11 concerning Sexual Exploitation, Pornography and Prostitution of, and Trafficking in, Children and Young Adults.
  - Draft Convention on Cyber-crime (expected finalised in 2000)

## **C Information on different approaches etc. in different states around the world**

### **Australia**<sup>59</sup>

Australia was one of the first nations in the world to censor the Internet. The regulation consists of:

- the Broadcasting Services Amendment (Online Services) Act;
- the Internet Industry Association's Code of Practice;
- a schedule of Content Control Options under this Code and State and Territory content enforcement provisions.

The explanation for this relatively complex system of laws and codes relates to the structure of the Australian Constitution that limits the jurisdiction of the Federal Government as a national censor and to the political manoeuvring behind the legislation itself.<sup>60</sup>

The Australian Broadcasting Authority (ABA) launched an Australian-wide hotline on 1 January 2000. The ABA will investigate complaints of child pornography on the Internet under the Broadcasting Services Amendment (Online Services) Bill of 1999. Under this Act, the ABA has implemented a co-regulatory scheme for Internet content regulation. The scheme is based on the development of codes of practice by industry and the investigation of complaints by the ABA. The Act also contains provisions for the protection of ISPs from civil proceedings for action taken in relation to the blocking of prohibited content hosted overseas.

In addition to its complaints handling role, the ABA will have a range of other functions including:

- monitoring compliance with codes of practice;
- advising and assisting parents and other carers of children in relation to the supervision and control of children's access to Internet content;
- conducting and coordinating community education programs about Internet services;
- conducting research into issues relating to Internet content and usage;
- liaising with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of online content;
- informing itself, and advising the Minister on technological developments and service trends in the Internet industry.

---

<sup>59</sup> For more substantial information and historical view on the Australian approach please refer to Gareth Grainger, Deputy Chairman, Australian Broadcasting Authority, Approaches to establishing New Hotlines – an Australian Perspective, paper presented at the Vienna Conference Combating Child Pornography on the Internet, 30 September 1999 and for a more critical view to Peter Chen, Forum: Regulating the Internet – Censorship? Australia's Internet Censorship Regime: History, Form and Future, Macarthur Law Review (3) 1999 p.121-142.

<sup>60</sup> Peter Chen, Forum: Regulating the Internet – Censorship? Australia's Internet Censorship Regime: History, Form and Future, Macarthur Law Review (3) 1999 p.133.

In this case, a child who is or looks like a person under 16 years defines Child pornography.

The Australian hotline is supported by legislation enacted by the Australian Federal Parliament, which provides national and uniform legislative coverage for the hotline. When the ABA identifies a child as being at risk, the appropriate government service authority is notified. If the ABA becomes aware of child pornography hosted overseas the ABA notifies overseas regulatory or other bodies (such as other hotline services) directly (subject to appropriate arrangements with Australian Police).

Even under the new law, and with the new initiatives established by the ABA, it is recognised that it will be extremely difficult to block overseas child pornography in Australia. Research shows that less than 2% of the Internet pornography viewed by Australians is produced or hosted in Australia.

### **Canada**

In Canada the Criminal Code, RSC, ch. C-46, @ 163.1(1)(a)(i) (1998) bans visual representations that show a person who is, or is depicted as, being under the age of eighteen years and is engaged in, or is depicted as engaging in, explicit sexual activity.

The British Columbia Court of Appeal has in 1999 ruled the child pornography law as it is written now, contravenes the Charter of Rights and Freedoms (Freedom of expression and the protection of privacy). Furthermore the court ruled that the law is flawed because it has the potential to penalise people for possessing and creating material that may merely be the products of the imagination and not intended for distribution.<sup>61</sup> The case is now on its way to the Supreme Court of Canada.

### **China, Korea and Vietnam**

China, Korea and Vietnam have actively sought to control their citizen's use of the Internet, either by forcing users to register with governmental monitoring organisations or by directly controlling Internet traffic coming into their countries through government-controlled Internet Service Providers.<sup>62</sup>

### **European Union**

Each member state has at present its own laws regulating the Internet in general and child pornography on the Internet in particular. These individual regulations raise concerns though as to the openness of the Internal Market, in that it may create risks of distortions of competition and the hampering of the free circulation of services. The European Union (EU) has issued a Communication Paper in which it concurred

---

<sup>61</sup> The decision of the Court of Appeal for British Columbia in R v Sharpe (BCCA 1999 416), judgment of 30 June, 1999 is at <http://www.courts.gov.bc.ca/jdb-txt/ca/99/04/c99-0416.html>

<sup>62</sup> David S. Wall, Policing and the Regulation of the Internet, Criminal Law Review, Special Edition 1998, p.87.

that “each country may reach its own conclusion in defining the borderline between what is permissible and not permissible”<sup>63</sup>

The Council of the European Union approved December 1998 a Joint Action to Fight Child Pornography on the Internet and also defined a comprehensive strategy. The Joint Action contains the following provisions:

In order to intensify measures to prevent and combat the production, processing, distribution and possession of child pornography and to promote the effective investigation and prosecution of offences in this area, the Member States will take the necessary measures to encourage Internet users to inform law enforcement authorities, either directly or indirectly, on suspected distribution of child pornography material on the Internet, if they come across such material (...).

Furthermore, the Member States shall also ensure that Europol, “within the limits of its mandate” is informed of suspected cases of child pornography, and “While engaging in a constructive dialogue with industry, Member States shall examine appropriate measures, of a voluntary or legally binding nature, to eliminate child pornography on the Internet”.

The Member States, “in contact with industry, shall cooperate by sharing their experiences and encouraging, if possible, the production of filters and other technical means to prevent and detect the distribution of child pornography material”.

In complement to previous joint actions, the Justice and Home Affairs Council (Joint Action 1997) reached a political agreement at one of its most recent sessions on a joint action to fight child pornography on the Internet. The action contains the following provisions:<sup>64</sup>

- In order to intensify measures to prevent and combat the production, processing, distribution and possession of child pornography and to promote the effective investigation and prosecution of offences in this area, the Member States will take the necessary measures to encourage Internet users to inform law enforcement authorities, either directly or indirectly, on suspected distribution of child pornography material on the Internet, if they come across such material (...).
- Internet users must therefore "be made aware of ways to make contact with law enforcement authorities or entities which have privileged links with law enforcement authorities, to enable such authorities to fulfil their task of preventing and combating child pornography on the Internet. Where necessary ... measures for the promotion of effective investigation and prosecution of offences in this area could be the setting up of specialised units within law enforcement with the

---

<sup>63</sup> European Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Illegal and Harmful Content on the Internet (COM (96) 487, Brussels-Luxembourg, October 16, 1996.

<sup>64</sup> W. Bruggeman, Child Pornography – Police and justice cooperation, p.4f., paper presented at the International Conference on Combating Child Pornography on the Internet, Vienna, 29 September to 1 October 1999.

necessary expertise and resources to be able to deal swiftly with information on suspected production, processing, distribution and possession of child pornography."

- The Member States "undertake to ensure the widest possible co-operation to facilitate an effective investigation and prosecution of offences concerning child pornography on the Internet". They shall use existing channels for communication such as Interpol. Where points of contact consisting of knowledgeable personnel have already been set up on a 24-hour basis to ensure timely, effective response to these offences, they shall be used for exchange of information and further contacts between Member States with a view to taking efficient action against offences involving child pornography. Member States shall notify the General Secretariat of the Council of the organisational unit acting as contact points; the General Secretariat shall then notify the Member States.
- The Member States shall also ensure that Europol, "within the limits of its mandate", is informed of suspected cases of child pornography.
- In "appropriate co-operation" with Europol the Member States shall examine the possibility of organising regular meetings of competent authorities specialising in the fight against child pornography on the Internet "with a view to promoting general information exchanges, analysis of the situation and tactical co-ordination".
- "While engaging in a constructive dialogue with industry, Member States shall examine appropriate measures, of a voluntary or legally binding nature, to eliminate child pornography on the Internet". In particular, they are to exchange experiences concerning the effectiveness of measures they have taken.

Finally, a EU funded project, COPINE (Combating Paedophile Information Networks in Europe), is working on tackling the problem of child pornography, paying special attention to the use of the Internet to disseminate paedophile material. COPINE is one of the first projects to be funded under the EU's STOP program to combat the sexual exploitation of children and trafficking in women.

## **Fiji**

See United Nations Press Release, GA/SHC/3537, 27 October 1999, Third Committee discusses ways to protect children p.5,

Also, Report of the Special rapporteur on the sale of children, child prostitution and child pornography in Fiji, oct. 1999, UNESCO, E/CN.4/2000/73/Add.3, Commission on Human Rights, Fifty-sixth session, Rights of the Child.

## **Ireland**

The Child Trafficking and Pornography Act 1998 makes it illegal for anyone to knowingly produce, distribute, print, publish, import, export, sell, show or possess

any child pornography. Children are defined for the purposes of the Act as anyone under the age of 17.

A [www.hotline](http://www.hotline) has been set up in Ireland on behalf of the Internet Service Provider Association of Ireland. If the hotline receives reports of child pornography on the Internet hosted in Ireland, it will request the relevant ISP to remove it.

## **Singapore**

Singapore, which has a reputation for censorship, has actively sought to control their citizen's use of the Internet. To do so, Singapore had to amend its laws to include the Internet.

Singapore has adopted a multifaceted approach to Internet censorship. First, the Singapore Broadcasting Authority (SBA), which regulates Internet content, has said that regulations are targeted only at the Internet function that could be described to be of a 'broadcast nature'. Second, it has adopted the peculiar, perhaps even unique, idea of class license: certain classes of content are deemed to be automatically licensed provided a code of practice is abided by. In effect, censorship is after, not before publication. Matters of race, religion and politics are given special attention on the Internet. When the code is breached, the license is revoked.<sup>65</sup>

Although the regulations carry the name 'broadcasting', the mechanisms employed resemble those that apply to the print media. Singapore's regulations are, in the main, an attempt to rationalise regulation of the Internet with regulation of the print media.

In keeping with the reliance on technology, Singapore ISPs have to use proxy servers that have a refused-access list to block access to blacklisted sites, currently about 100, which are mostly pornographic sites.<sup>66</sup>

## **United Kingdom**

Any person displaying child pornography on the Internet is guilty of the common law offence of shameless indecency. Furthermore, the statutory law, the Protection of Children Act 1978 and its Scottish equivalent, the Civic Government (Scotland) Act 1982.S.1 of the 1978 Act and s.52 of the 1982 Act, made it an offence to take, or permit someone to take an indecent photograph, possess the indecent photograph with a view to distributing it or showing it, or publish any advertisement implying that the indecent photograph will be distributed or shown. With the introduction of the Criminal Justice and Public Order Act 1994 the issue of computer pornography was specifically included. It is not however an offence to simply view child pornography on the web – only to possess with a view to its being distributed or shown by himself or others. "Pseudo-photographs" are included in the broad definition of the Act.<sup>67</sup>

The Obscene Publications Act 1959 and 1964 constitutes the major legislation to combat pornographic material of any kind in the UK. Furthermore there is Section

---

<sup>65</sup> Singapore Broadcasting Authority. <http://www.gov.sg/sba/netreg/regrel.htm>.

<sup>66</sup> Tong, Ming Chien (20 July 1996). Device to block out blacklisted web sites. Strait Times

<sup>67</sup> David Flint, The Internet and Children's rights, Computer Law & Security Report Vol. 16 no. 2 2000 p. 89.

43 of the Telecommunications Act 1984, which makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character' and is an imprisonable offence with a maximum term of six months.<sup>68</sup>

## USA

In the US the Communications Decency Act of 1996 made it a crime to make indecent or patently offensive words or pictures available on-line where children can find them. The Act was later ruled as unconstitutional as it outlawed materials that either "appear to be" or "convey the impression" they are sexually explicit pictures of children. Also the Child Online Protection Act 1998 which aimed to insulate children from online pornography by regulating commercial websites has been struck down. Child pornography is now prohibited by 18 USC 2252 which makes it a federal offence to knowingly receive child pornography and 18 USC 2251 which makes it illegal to advertise child pornography. The Child Pornography Protection Act 1996 has included "pseudo-photographs" (computer generated) to be illegal as well. In addition, State legislation also prohibits sexual abuse and exploitation of minors on the Internet.<sup>69</sup>

On 24 July 2000, the US House Judiciary Committee convened a hearing on the latest type of surveillance system. The Federal Bureau of Investigation (FBI) has developed an advanced packet sniffer which can be installed on an ISP's backbone to scan and record selected communications. This program has been given the rather sinister name of 'Carnivore' and the Committee hoped to gather information to assess the capabilities of the program. Until now the program's capabilities had been shrouded in mystery.

Concerns have been raised amongst members of Congress and civil liberties groups regarding Carnivore's ability to monitor large amounts of communications, as well as its still unknown configuration potential. Carnivore's critics gave testimony. Barry Steinhardt of the ACLU said the use of Carnivore is like "a wiretap capable of accessing the contents of all of the phone company's customers." This, he stated, was a direct violation of the Fourth Amendment's requirement of narrow and targeted searches, designed to protect both the privacy of individuals and the ability of the government to conduct searches.

---

<sup>68</sup> For further information on the UK legislation please refer to Y Akdeniz, The Regulation of Pornography and Child Pornography on the Internet, 1997 (1) The Journal of Information, Law and Technology.

<sup>69</sup> David Flint, The Internet and Children's rights, Computer Law & Security Report Vol. 16 no. 2 2000 p. 90

**D List of relevant documentation on the subject, (Copies are available through the Secretariat of the Asia Pacific Forum)**

1. Background Paper from the Asia Pacific Forum Secretariat to the Asia Pacific Forum, Issues mandated by the third annual meeting, Child Pornography and the Internet, Fourth Annual Meeting of the Asia-Pacific Forum of National Human Rights Institutions, 6-8 September 1999 in Manila.
2. World Congress Against Commercial Sexual Exploitation of Children, Stockholm, August 1996, Declaration and Agenda for Action.
3. World Congress Against Commercial Sexual Exploitation of Children, Stockholm, 27-31 August 1996 Background Document.
4. Background Document prepared for the Experts Meeting on Child Pornography on the Internet, Lyon, 28 May-29 May 1998.
5. Rita Shackel, Regulation of Child Pornography in the Electronic Age: The Role of International Law, Macarthur Law Review, (3) 1999.
6. Prof. Dr. Ulrich Sieber, Internet law, Responsibility of Internet Providers – A comparative legal study with recommendations for future legal policy, Computer law & Security Report Vol. 15 no.5 1999.
7. Clive Walker and Yaman Akdeniz, The Governance of the Internet in Europe with Special Reference to Illegal and Harmful Content, Criminal Law Review Special Edition 1998.
8. Yaman Akdeniz, The Regulation of Pornography and Child Pornography on the Internet, 1997 (1) The Journal of Information, Law and Technology (JILT).
9. ECPAT, Child Pornography on the Internet a Position paper for ECPAT International at <http://www.crin.org/iasc/sedoc11.html>
10. Economic and Social Committee of the European Commission, Opinion on the Proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet (OJEC, 98/C 214/08, Brussels-Luxembourg, July 10, 1998).
11. David Flint, The Internet and Children's rights, Computer Law & Security Report Vol. 16 no. 2 2000.

12. European Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Illegal and Harmful Content on the Internet (COM (96) 487, Brussels-Luxembourg, October 16, 1996.
13. Gary Leong, Computer Child Pornography – The Liability of Distributors, Criminal Law Review, Special Edition 1998, p. 19-28.
14. David S. Wall, Policing and the Regulation of the Internet, Criminal Law Review, Special Edition 1998, p.79-91.
15. David J. Davis, Criminal Law and the Internet: The Investigator's Perspective, Criminal Law Review, Special Edition, August 1999, p. 48-60.
16. Peter Chen, Forum: Regulating the Internet – Censorship? Australia's Internet Censorship Regime: History, Form and Future, Macarthur Law Review (3) 1999 p.121-142.
17. UNESCO, E/CN.4/RES/1999/40, 26 April 1999, Traffic in women and girls, Commission on Human Rights resolution 1999/40.
18. UNESCO, World Citizens' Movement to Protect Innocence in Danger, paper by Homayra Sellier, President, 18 September 1999.
19. UNESCO, E/CN.4/2000/73/Add.3, Commission on Human Rights, Fifty-sixth session, Rights of the Child, Report of the Special rapporteur on the sale of children, child prostitution and child pornography, Ms Ofelia Calcetas-Santos, Addendum, Report on the mission of the Special Rapporteur to the Republic of Fiji on the issue of commercial sexual exploitation of children, 11-16 Oct. 1999.
20. United Nations Press Release, GA/SHC/3537, 27 October 1999, Third Committee discusses ways to protect children.
21. United Nations Press Release, Resumed Fifty-fourth General Assembly Plenary, 25 May 2000, 97<sup>th</sup> Meeting (AM).
22. UNESCO, E/CN.4/2000/73, 14 January 2000, Commission on Human Rights, Fifty-Sixth session, Agenda item13, Rights of the Child.

23. UNESCO, E/CN.4/2000/75, 28 March 2000, Commission on Human Rights, Fifty-Sixth session, Agenda item 13, Rights of the Child.
24. UNESCO, E/CN.4/2000/L.48, 14 April 2000, Commission on Human Rights, Fifty-sixth session, Agenda item 11, Civil and Political Rights.
25. UNESCO, E/CN.4/2000/L.62, 17 April 2000, Commission on Human Rights Fifty-Sixth session, Agenda item 13, Rights of the Child.
26. Expert Meeting Papers, Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An International Challenge, UNESCO, Paris, 18-19 January 1999:
- Declaration and Action Plan, 19 January 1999.
  - Alex Hermoso, Director, PREDA Social Development Foundation and Father Shay Cullen, MSSC, The Philippines.
  - Mr Aidan White, Secretary General, International Federation of Journalists, Brussels, Freedom of Information in The Face of Worldwide Concern About Sexual Abuse of Children, Paedophilia and Pornography on the Internet.
  - Mark Hecht, Human Rights Internet, Canada, Between Promotion and Protection: Encouraging Freedom of Information in the Context of Worldwide Concerns on the Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet.
  - Atty Parry Aftab, Cyberangels, Civil Liberties, Privacy and Internet Abusers: Making the Net Safe for Young Children – Content Providers, Spam Filters, Search Engines, Rating Websites, Monitoring and Networking. An Overview.
  - Jean Christophe Le Toquin, AFA - Fournisseurs d'Internet France, Internet Service Providers and The Issue of Illegal Content.
  - The Initiative of the Movement against Paedophilia on the Internet; Beatrice van Bastelaar, MAPI, Belgium.
  - Prof. Ulla Carlsson, Coordinator of the International Clearing House on Children and Violence on the Screen, University of Gothenburg, Sweden, Child Pornography on the Internet Research and Information: Sensitisation of the Public.
  - Bruce Harris, Executive Director, Casa Alianza, Nicaragua, Latin American Programmes of Casa Alianza/Covenant House, Latin America.
  - Carol Aloysius, Associate Editor, The Observer, Sri Lanka, A Journalist's perspective of the problem in Asia.

27. Conference Papers from the Vienna conference on combating child pornography on the Internet, 29 September – 1 October 1999:

- General Background paper to the Conference.
- Vienna Commitment against Child Pornography on the Internet, Conclusions and recommendations of the international conference Combating Child Pornography on the Internet”.
- Introductory papers to the Working Groups:  
Working Group 1: Law Enforcement and Judiciary  
Working Group 2: Guidelines for Codes of Conduct  
Working Group 3: Hotlines
- Maxwell Taylor, Professor, University College Cork, Ireland, *The nature and dimensions of child pornography on the Internet.*
- Gustaaf Borchartd, Director, Directorate General "Justice and Home Affairs", European Commission, *Taking stock: activities of the European Commission in the fight against child pornography.*
- Message from Kofi Annan, Secretary-General of the United Nations delivered by Pino Arlacchi, Director-General, United Nations office at Vienna, *Presentation.*
- Guy de Vel, Director of Legal Affairs, Council of Europe, *Taking. stock of the activities of the Council of Europe.*
- Agnès Fournier de Saint Maur, Head of the Trafficking in Human Beings Branch, INTERPOL, *The sexual abuse of children via the Internet: a new challenge for Interpol.*
- John D. Ryan, Assistant General Counsel, America OnLine, Inc., *Presentation.*
- Nigel Williams, Director, Childnet International, Coordinator of the INHOPE Forum *The Contribution of Hotlines to Combating Child Pornography on the Internet.*
- Trond Waage, Ombudsman for Children, Norway, *Hopes and Fears on Internet - Children's rights in the electronic universe.*

- Ulrich Sieber, Professor, University of Würzburg, Germany, *Fighting Illegal and Harmful Contents on the Internet.*
- Yoshihisa Togo, Executive Director of the Japan Committee for UNICEF, *Presentation.*
- Holger Kind, Kriminalhauptkommissar, Bundeskriminalamt, Germany, *Combating child pornography on the Internet.*
- Willy Bruggeman, Deputy Director, Europol, *Child pornography - Police and justice co-operation.*
- Eamonn M. Barnes, President, and Thomas N. Burrows, International Association of Prosecutors, United States of America, *Combating use of the Internet to exploit children.*
- Peter Csonka, Administrator and Secretary to Committee PC-CY, Council of Europe, *Contribution to the Conference on combating child pornography on the Internet.*
- Richard Gerding, National Expert, General Secretariat of the European Council, *Combating Child Pornography on the Internet - The role of the European Judicial Network.*
- Jens Waltermann, Deputy Head, Media Division, Bertelsmann Foundation, *Self-regulation of Internet Content.*
- Jean-Christophe Le Toquin, Spokesman, AFA - French Internet Service Providers Association, *Guidelines for codes of conduct.*
- Peng Hwa Ang, Professor, Nanyang Technological University, Singapore, *ISP Self-Regulation: Why and Why Not?*
- Michael Schneider, AboveNet Germany GmbH, *Measures taken by German ISPs to combat child pornography - the NewsWatch approach.*
- David Kerr, Chief Executive, Internet Watch Foundation, Great Britain, *Presentation of Self-Regulatory Measures.*

- Edwin Mac Gillavry, Researcher, University of Groningen, Netherlands *Internet Service Providers and criminal investigation. A case study regarding the voluntary co-operation of Dutch ISPs with the investigating authorities.*
- Herbert Burkert, Professor, University of St. Gallen, Switzerland, *Hotlines.*
- Guy Verbeeren, Belgian National Crime Squad, *The Central Judicial Contact Point on the Internet in Belgium.*
- Ruth Dixon, Hotline Executive, Internet Watch Foundation, Great Britain, *Relationship of hotlines with law enforcement.*
- Jean-Christophe Le Toquin, Spokesman, AFA - French Internet Service Providers Association, *Relationships of Hotlines with Law Enforcement.*
- Gareth Grainger, Deputy Chairman, Australian Broadcasting Authority, *Approaches to establishing New Hotlines-an Australian Perspective.*
- Karl Hitschmann, Board Member, Internet Service Providers Austria (ISPA), *Purpose of Internet Hotlines within the self regulation environment.*

## **E Government Organisations and NGOs dealing with the issue directly or indirectly**

- UN
  - UN Committee on the Rights of the Child
  - UN Commission on Human Rights and its Special Rapporteur on the Sale of Children
  - UNICEF
  - UNESCO
    - World Movement of Citizens to Protect Innocence in Danger, (In the Asia Pacific: kIDs.ap)
  - UN Crime Prevention and Criminal Justice Division
- OECD
  - OECD Forum (25.03.98), Internet Content Self-regulation
- Council of Europe, The Committee of Experts on Crime in Cyberspace
- ILO (International Labour Office)
- Interpol (International Criminal Police Organisation)
- WHO (World Health Organisation)
- MAPI (Movement Against Paedophilia on the Internet)
- ECPAT (End Child Prostitution, Child Pornography and Trafficking)<sup>70</sup>
- The International Bureau of Children's Rights
- European Child Forum

---

<sup>70</sup> There are currently over 250 groups in the coalitions, which form the ECPAT network, in over 25 countries worldwide. ECPAT's mission statement reads as follows from their web site: "ECPAT is a global network of organisations and individuals working together for the elimination of child prostitution, child pornography and the trafficking of children for sexual purposes. It seeks to encourage the world community to ensure that children everywhere enjoy their fundamental rights free and secure from all forms of commercial sexual exploitation."

- Focal Point against Sexual Exploitation of Children  
[www.childhub.ch/dcifp/dci\\_home\\_uk.html](http://www.childhub.ch/dcifp/dci_home_uk.html)
- Australia: Federal Department of Health & Family Services.

**F Recent conferences, meetings, congresses etc. which have dealt with the issue of Child Pornography on the Internet:**

- **27-31 August 1996**, Stockholm, World Congress against Commercial Sexual Exploitation of Children, initiated by ECPAT, hosted by the Government of Sweden.
- **9 September 1996**, Debate on the problem of child pornography on the Internet, hosted by the Internet Developers Association, UK
- **July 1997**, OECD Ad hoc Meeting on approaches to content and conduct on the Internet
- **July 1997**, Bonn, Global Information Networks, Ministerial Conference
- **December 1997**, The Internet On-line Summit: Focus on Children, Washington DC
- **25 March 1998**, OECD Forum, Internet Self-regulation
- **April 1998**, Strasbourg, Council of Europe, The Use of the Internet within the Context of Sexual Exploitation of Children
- **May 28-29, 1998**, Lyon, Child Pornography on the Internet – Two international meetings of experts at the Interpol General Secretariat, convened by ECPAT and Interpol.
- **September/October 1998**, Monte Carlo, UNESCO Experts Meeting on Cyberspace Law.
- **27 October 1998**, Rome, Paedophilia and the Internet: Old Obsessions and New Crusades. The Objective of the conference was among other things to analyse and denounce the dangerous consequences on individual freedoms, on the right to privacy and on the development of new Internet technology, and of the new legislative and judiciary initiative undertaken in Italy.

- **18-19 January 1999**, Paris, UNESCO Expert Meeting on Sexual abuse of Children, Child Pornography and Paedophilia on the Internet: An International Challenge.<sup>71</sup>
- **28 February – 6 March 1999**, International Seminar on Sexual Abuse and Exploitation of Children: a health and criminal justice perspective, Durham, United Kingdom.
- **March 1999**, Asia-Pacific Internet Conference, Bali, Indonesia
- **18-19 May 1999**, Expert Conference on a European System for Content Rating, Brussels
- **29 September –1 October 1999**, Vienna, International Conference on Combating Child Pornography on the Internet – organised by the Government of Austria<sup>72</sup>

---

<sup>71</sup> UNESCO, E/CN.4/2000/73, 14 January 2000, Commission on Human Rights Fifty-sixth session, p.6 section 10 and 11. The meeting, convening national and international non-governmental organizations, inter-governmental organizations, representatives of UN Specialised agencies, national institutions and specialists – among them judges and legal experts – brought together some 400 participants. The Meeting dealt initially with the traditional problem of sexual abuse of children and paedophilia, and then considered this in the context of the Internet under three themes: The promotion of the free flow of information in a manner which would not place children at greater risk of sexual exploitation; How to make the Internet safe for children to use; and the need for research, information-monitoring and sensitisation of the public.

The meeting enabled the participants from all over the world to draw together existing information from groups and organizations engaged in the fight against paedophilia and child pornography on the Internet. The participants at the conference put forward a declaration and an action plan, which proposes certain measures for UNESCO and for Governments, international agencies, NGOs, industry, educators, parents, law enforcement agencies and the media.

<sup>72</sup> The Conference was co-sponsored by the US and Austria. The objectives were:

- re-inforcing cooperation among law-enforcement officials and the judiciary,
- establishing voluntary self-regulation mechanisms (codes of conduct) among Internet service providers,
- encouraging the establishment of further hotlines (hotlines enable citizens to report leads on child pornography found on the Internet) and of networking among existing hotlines.

## **G Further resources on freedom of speech and related concerns**

### **Useful general books on freedom of speech and related concerns include:**

- Eric Barendt, *Freedom of Speech* (Oxford: Clarendon Press, 1987)
- Joel Feinberg, *The Moral Limits of the Criminal Law*, 4 vols. (Oxford: Oxford University Press, 1984-)
- Stanley E. Fish, *There's No Such Thing as Free Speech, and It's a Good Thing, Too* (New York: Oxford University Press, 1994)
- Kent Greenawalt, *Speech, Crime, and the Uses of Language* (New York: Oxford University Press, 1989)
- Frederick Schauer, *Free Speech: A Philosophical Inquiry* (Cambridge: Cambridge University Press, 1982)
- Rochelle Gurstein, *The Repeal of Reticence: A History of America's Cultural and Legal Struggles over Free Speech, Obscenity, Sexual Liberation, and Modern Art* (New York: Hill and Wang, 1996)
- Richard L. Abel, *Speaking Respect, Respecting Speech* (Chicago: University of Chicago Press, 1998)

### **Useful journal symposia include:**

- *American Bar Foundation Research Journal* (Fall 1987): The Attorney-General's Commission on Pornography
- *Annual Survey of American Law* (November 1993): Hate Crimes – Propriety, Practicality and Constitutionality
- *California Law Review*, 82, 4 (July 1994): Critical Race Theory
- *Capital University Law Review*, 24 (1995): Liberalism Divided: the Supreme Court and the Problem of Hate Speech
- *Case Western Law Review*, 38 (1987/1988): Thomas I. Emerson and the First Amendment
- *Continuum: The Australian Journal of Media and Culture*, 12, 1 (July 1998): Censorship and Pornography
- *Duke Law Journal* (June 1990): Frontiers of Legal Thought II: The New First Amendment
- *Golden Gate University Law Review*, 23 (Spring 1993): First Amendment Law

- *Harvard Civil Rights-Civil Liberties Law Review*, 27 (Summer 1992): The State of Civil Liberties: Where Do We Go From Here?
- *Harvard Journal of Law and Public Policy*, 10 (Winter 1987): The First Amendment
- *Law & Sexuality: A Review of Lesbian and Gay Legal Issues*, 2 (1992): Legal Restrictions on Homophobic and Racist Speech: Collateral Consequences on the Lesbian and Gay Community
- *Law and Contemporary Problems*, 55, 1 (Winter 1992): Comparative United States/Canadian Constitutional Law
- *New England Law Review*, 20, 4 (1984-1985): Pornography
- *New York Law School Law Review*, 38, 1-4 (1993): Women, Censorship, and "Pornography"
- *Northern Kentucky Law Review*, 23 (1996): Political Correctness in the 1990's and Beyond
- *Notre Dame Law Review*, 72 (July 1997): Propter Honoris Respectum: Frederick Schauer
- *Ohio Northern University Law Review*, 21, 3 (1995): Demise of the First Amendment? Focus on Rico and Hate Crime Litigation: Shield from Terrorism? Or National Gag Order?
- *Stanford Law Review* (May 1995): Race and Remedy in a Multicultural Society
- *Sydney Law Review*, 17, 1 (March 1995): Freedom of Speech and the Constitution
- *Texas Law Review*, 66 (June 1988): Academic Freedom
- *UC Davis Law Review*, 29 (Spring 1996): Developments in Free Speech Doctrine: Charting the Nexus between Speech and Religion, Abortion, and Equality
- *University of Chicago Law Review*, 59 (Winter 1992): The Bill of Rights in the Welfare State: A Bicentennial Symposium
- *University of Chicago Legal Forum* (1993): A Free and Responsible Press
- *University of Colorado Law Review*, 64, 4 (1993): Ira C. Rothgerber, Jr. Conference on Constitutional Law: Freedom of Speech in a World of Private Power

- *University of Illinois Law Review* (1992): Race Consciousness and Legal Scholarship
- *University of Michigan Journal of Law Reform*, 21, 1/2 (Fall 1987/Winter 1988): Pornography
- *University of New Brunswick Law Journal*, 44 (1995): Freedom of Speech in the University Context
- *University of Pittsburgh Law Review*, 40, 4 (Summer 1979): Principles of Expression and Restriction: A First Amendment Symposium
- *Villanova Law Review*, 37, 4 (1992): Hate Speech and the First Amendment: On A Collision Course?
- *Washington and Lee Law Review*, 47, 1 (Winter 1990): Offensive and Libellous Speech Symposium
- *Wayne Law Review*, 37 (Spring 1991): Campus Hate Speech and the Constitution in the Aftermath of *Doe v. University of Michigan*
- *Wide Angle*, 19, 3 (July 1997): Pornography
- *William and Mary Law Review*, 32, 2 (Winter 1991): Free Speech and Religious, Racial, and Sexual Harassment
- *William and Mary Law Review*, 33, 3 (Spring 1992)
- *William Mitchell Law Review*, 18 (Fall 1992): Hate Speech after *R.A.V.*: More Conflict between Free Speech and Equality?
- *Yale Law Journal*, 104 (May 1995): Emerging Media Technology and the First Amendment

**Useful online sources include:**

- Australian Legal Information Institute (AustLII) <http://www.austlii.edu.au>. This site provides access to an extensive selection of primary and secondary Australian legal materials, and has links to many international legal databases and electronic journals.
- High Court of Australia Home Page <http://www.hcourt.gov.au>. The Court's home page offers decisions, recent speeches, biographies of the judges, etc.
- Australian Parliament <http://www.aph.gov.au>. This site provides access to Hansard, legislation, committees, parliamentary who's who etc.
- United Nations <http://www.un.org>. The site offers access to documents and decisions of the UN.

- European Court of Human Rights <http://www.echr.coe.int>
- United Kingdom Parliament <http://www.parliament.the-stationery-office.co.uk/>. This site offers access to both political and legal decisions, plus all the usual stuff on government, and is updated very quickly.
- Guide to the US Supreme Court <http://www.jurist.law.pitt.edu/supreme/>. This site provides a companion to the jurisprudence, structure, history and Justices of America's highest court, including its calendar, current and historical decisions, procedures, historical resources, and media coverage of the Court.
- Oyez Oyez Oyez, A Supreme Court WWW Resource <http://oyez.at.nwu.edu/oyez.html>. Operated by Northwestern University and using tapes from the National Archives, this site offers recordings of oral arguments from more than 50 historic US Supreme Court cases since 1961. You need RealAudio software to listen to these cases, but it can be downloaded from the site.
- Cornell Law School Server <http://www.law.cornell.edu>. Operated by Cornell's Legal Information Institute, this site offers the full text of all US Supreme Court decisions from May 1990 to the present, as well as more than 50 historic decisions since 1947.