Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 08-Jul-1999
Dist. : 12-Jul-1999

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

APPROACHES TO CONTENT ON THE INTERNET

DSTI/ICCP(97)14/FINAL
Unclassified

79911

Or. Eng.

CONTEXT FOR THE INVENTORY

Snap-shot view

This inventory report aims at reviewing the existing legislation and practices in Member countries concerning Internet content issues and gathering the views of the different actors involved. In many Member countries these approaches are still in the process of being developed, in light of evolving technologies, and in consideration of work under way in the public and private sectors. As a consequence, the report represents a "snap-shot" view of OECD Member country approaches to content on the Internet, as reported by Member countries as of mid-1998. Furthermore, the Inventory focuses on the Internet within the context of the broader network environment; however, it is recognised that the nature of the Internet as it is known today may change significantly with technological advances in the years ahead. The document has been prepared under the auspices of the Information, Computer and Communications Policy Committee based on Secretariat research and input supplied by Member countries.

Private sector role

The important role of the private sector in the development of technological and self-regulatory solutions to address issues related to Internet content is widely recognised. This inventory includes a chapter which highlights some of the private sector initiatives in this area. In addition, where countries have reported on the activities of private sector actors, this has been included as part of the national approach section. However, given the rapid pace of technological evolution and the various models for self-regulation which are currently emerging in Member countries, a comprehensive survey of private sector activities in this area is not intended.

TABLE OF CONTENTS

OVERVIEW

The development of open information and communications networks -- in particular the Internet -- has dramatically increased the opportunities to conduct a variety of electronic transactions which allow the access to and distribution of all kinds of information on a global scale. These changes offer an enormous potential for social and economic development. As policy makers begin to evaluate their approaches to the wide variety of issues which arise from the developing information society, in particular in the context of electronic commerce and the promotion of network technologies for social and economic purposes, one of the concerns which is raised is the need to examine issues and consequences related to the content of information on the Internet.

In addressing content issues, governments must take into consideration the desirability of economic growth based on emerging network technologies, the value of free expression and the free exchange of ideas for citizens, and the concerns for preventing or limiting the use of networks for purposes contrary to public order and safety. The complexity of these issues is exacerbated by the inherently international nature of the network environment, the importance of the developing information society, and the diversity of cultural norms in this area. OECD governments have recognised that internationally co-ordinated approaches may be needed to exchange information and establish a general understanding about how to address these issues. The OECD is an appropriate forum in which to review these issues because it has continuing experience in developing consensus about specific policy and regulatory questions relating to information and communications networks and technologies, and in addressing policy issues that have technological, economic and legal dimensions.

The objective of this report is to respond to an OECD Council request in February 1997 for the ICCP Committee to consider proposals by the Delegations of France and Belgium for international co-operation concerning the Internet. The ICCP Committee agreed to undertake a study aimed at reviewing the existing legislation and practices in Member countries concerning the Internet and gathering the views of the different actors involved. The Communiqué issued following the May 1997 meeting of the OECD Council at the Ministerial level stated that "[b]earing in mind the great potential of the Internet, Ministers looked forward to the results of the study being undertaken in the OECD to compare national legislation and policies concerning the Internet, recognising the important advisory role of the private sector, and to identify areas in which international co-operation may be needed".

Content issues are on the agenda for consideration in both the public and private sectors, and recently a number of high level government statements -- including the Clinton Administration's "Framework for Global Electronic Commerce"[1], the Ministerial Declaration that followed from the Bonn Ministerial Conference on Global Information Networks[2] and the statement by European Commissioner Bangemann on the "Policy Response to Globalisation and Convergence"[3] -- have called for specific attention to be given to these issues. A number of initiatives have already been undertaken to examine various aspects at both the national and international level in a variety of forums, including the European Commission, the Council of Europe, and the World Intellectual Property Organisation (WIPO).

This document has been prepared based on written input received from Member countries, the private sector, and international organisations, as well as discussions at two *ad hoc* meetings of the ICCP

Committee on "Approaches to Content on the Internet" held on 1-2 July 1997 and 22 October 1997, and a joint OECD-BIAC "Forum on Content Self-Regulation" held on 25 March 1998. It seeks to provide an inventory of current national approaches and related international initiatives underway, identify the issues involved in this area, and provide a context for consideration of possible future work of the OECD in this area. It is an information document intended to assist further discussion of these issues and identify technological solutions, but it does not make recommendations to governments about how to proceed. The issues under consideration are broad in nature and the views of Member countries reflect the wide diversity of public opinion on these matters.

This report focuses on "content", specifically in the context of the Internet. Section I describes a broad background of "content on the Internet", highlighting some of the unique issues involved in policy making for the new technologies. The section attempts to provide a foundation for a general understanding about the nature and development of the Internet and its operating protocols, the ways that people can access and use the Internet, the ability to control content at different points in the delivery or access process, and some of the technological solutions for addressing content issues.

The core of this document is Section II, which presents a snapshot of the current situation in OECD Member countries. This section consists of: an inventory of existing legislation, policies and practices, and approaches in OECD countries; important private sector initiatives currently under way in this area -- including technological solutions, self-regulatory measures, and contractual agreements; and the work of other international organisations.

The inventory shows that although some countries appear to be more advanced in their thinking and actions to address issues raised by to Internet content, all OECD governments have indicated their serious interest and have taken steps to give the issues full examination and attention. Many countries have actively engaged in a process to identify and implement solutions. Some countries are focusing on specific areas of concern, while others are studying the broader issues. The inventory reveals that, despite the various stages of policy development, there are some "common threads" which appear in most national approaches in one form or another. Without intending to be exhaustive, and without implying any kind of ranking in the order they are presented, the following list presents a number of common points which are frequently taken into consideration as OECD countries develop and implement approaches to Internet content issues:

- Defining the diverse services and technologies available and identifying main actors in terms of the functions they perform.

- Clarifying liability and responsibility for various parties.

- Reaffirming the application of existing law to the new medium.

- Achieving jurisdiction and enforcement in the global network environment, including technological capabilities and limitations to control or enforce, and the choice of law.

- Respecting fundamental rights, common values and community standards.

- Recognising cultural diversity.

- Protecting special groups (especially children).

- Protecting privacy and personal data.

- Focusing on technological solutions, and the importance of the role of industry.
- Focusing on education and empowering users.
- Determining whether international co-operation is necessary, what it could entail, and how it might be accomplished.

APPROACHES TO CONTENT ON THE INTERNET

I. Content on the Internet

Emerging network technologies make it possible for people, businesses and governments to transact electronically with one another in a wide variety of new ways, which offer enormous social and economic benefits of all types. The explosive world-wide growth of open networks -- in particular the Internet -- has made the transmission of all kinds of digitised data fast, cheap and simple, thereby constituting a basis for electronic commerce and new forms of communication. The public consumption of computer technologies, which are becoming more powerful, less expensive and easier to use, is increasing at the same time as graphic-based Internet applications are being developed. This evolution drives the further development of new kinds of information-based products and services, and the creation of innovative content and applications.

The Internet offers lower barriers to entry than other forms of mass media, and its unique mechanisms for distributing and accessing content -- which are in some ways all-to-all and at the same time one-to-one in nature, blurring the distinctions between producers, senders and receivers of information -- makes the Internet distinct from more traditional media in many ways. Furthermore, the dynamic interactive environment not only makes it possible to exchange information and ideas in new ways, but the enormous variety and quantity of information that can be exchanged create unprecedented opportunities for expression of linguistic and cultural diversity, community connections, and entertainment. A number of long-term benefits are expected from this technological transition, in particular in terms of economic growth, job creation, education, and health care. Any consideration of issues related to the Internet must be put in the context of these sweeping benefits, with an eye towards the importance of network technologies for individuals, businesses, and governments.

As the Internet expands and evolves it brings with it new issues related to information content that are peculiar to the emerging medium. Along with the opportunities offered by open networks and digital technologies come new kinds of disputes and different ways to engage in illegal or controversial activities. In that context, there has been public concern about the content of some of the information distributed and accessed on the Internet. Applying traditional methods for addressing illegal and controversial content in the electronic environment offers new challenges; however, the technology also brings with it a variety of new ways to resolve some of the issues raised.

What is illegal, harmful or controversial content?

The Internet makes a wide variety of information available, the vast majority of which is high-quality content that offers considerable social and economic value for Internet users. However, there is also some disagreeable and detrimental content in the mix, some of which is illegal under national laws and some of which may not be illegal but is considered harmful or controversial when viewed by certain sections of the population, such as children. A discussion of illegal, harmful or controversial content is complicated in the first instance simply in terms of defining the topic: it is not always clear what is meant by “illegal”, “harmful” or “controversial”. To some extent this is a linguistic issue, because a variety of

terms used in different contexts are meant to indicate basically the same concepts, including "objectionable", "offensive" and "illicit". Furthermore, this question can be exacerbated where the term "illegal" is only meant to refer to a *criminal* offence, and "harmful" is meant to indicate content which raises *civil* law issues because it "harms" another party. For purposes of this report, the term "illegal" means content that constitutes a criminal or civil offence under national law; "harmful" indicates content that is considered detrimental to some people, particularly children; and "controversial" describes the broader grey area where content might be considered illegal or harmful in one culture or community but not in another.

Illegal, harmful or controversial content, in the broadest terms, can include: sexually explicit material; material with implications for minors, such as child pornography, violence against children, or abusive marketing; incitement to hatred, violence, or racism; material with national security implications, such as sedition, terrorism, bomb production; communication of erroneous information, such as fraud, false or misleading advertising, or defamation; or content which violates individual rights, such as the right to privacy, or intellectual property rights. Some content is outright illegal (*e.g.* child pornography) and a punishable offence under criminal law. Some is not illegal for adults but is subject to restricted access for minors. Generally, what is illegal in the physical world is also illegal in the electronic environment; but while this works in the national context, at the international level different legal regimes mean standards for determining legal status vary. Where content is not illegal but is controversial, it is a subjective issue which could include political opinions, religious beliefs, or other opinions that may be objectionable to one but not another. Community and cultural standards generally determine what is harmful or controversial, but they are hard to uphold in the global environment. At least for purposes of developing policies to address content issues at the national level, it may be useful to make the distinction between illegal content and harmful content, as they may require different approaches.

The way in which the technology is used can also act as a boundary for determining "illegal" content where there are legal distinctions between different methods of communication. In some cases, different laws might apply to public communications (such as broadcasting) and private communications (such as a private correspondence). For example, where a negative statement about another individual made in a private email communication is just an opinion, if the same message becomes a public declaration by being widely distributed in an electronic mailing list, it could be defamation. The convergence of telecommunications, broadcasting, and print technologies together with the large variety of Internet applications that are available can make it difficult to clarify these distinctions.

The importance of understanding the technology

In order to fully comprehend the unique issues involved in policy making for new technologies, a clear understanding of how the technologies work is critical. A full examination of the technology should be the first step in policy making, if law and policy are to respond to technology development rather than lead it. The following section provides a general description of the nature and development of the Internet and its operating protocols, the ways that people can access and use the Internet, the ability to control content at different points in the delivery or access process, and the technological solutions for addressing content issues in order to provide policy makers with a foundation for discussing the various approaches to content on the Internet.

Transition to electronic transactions

Information is becoming more valuable, and the production, distribution and use of information is an increasingly important economic activity. Information is often exchanged as a commodity and may

be protected by intellectual property law. Information producers seek access to distribution channels while consumers demand access to a broad range of information sources. Furthermore, the free flow of information is a fundamental element of democracy.

Traditional telephone, broadcast and cable television, and radio systems have long used electronic means to distribute information in analogue form; however, the shift to digital technology is revolutionising the way that information is created and handled. Digital computer processing and network technologies are replacing traditional methods for producing, storing, transmitting and disseminating information. Combining different kinds of information representations -- such as text, audio, images and video -- is easy with digital technology, and the distinctions between different types of information production and distribution are becoming less clear. The Internet and related network technologies are changing the way people communicate and do business, and they have a widespread impact on the public and private sectors, necessitating changes in a variety of basic commercial, legal and other structures.

Basic architecture of the Internet

The Internet developed out of the United States' ARPANET project in the 1970s, originally sponsored by the US military. It requires no central administrative body to oversee its operations; it functions because system operators around the world adopt common data transfer protocols to enable computers and networks to communicate with one another. In recent years, these common protocols have emerged from several loosely organised, unofficial, but widely accepted, standards-making bodies -- most notably the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Assigned Number Authority (IANA), and the World Wide Web Consortium (W3C)[4] -- which bring together input from academic, industry, governmental and non-profit sectors to develop technological standards that form the basis upon which the Internet functions. The process for developing technical standards for the Internet is currently evolving, and the private sector plays an increasingly important role. Recently, the process has been somewhat formalised with the adoption of many standards by the International Organisation for Standards (ISO). It is important to note that these organisations merely work together co-operatively to develop protocols for the Internet -- they do not have any authority over its operations.

The Internet might be described as comprised of three distinct layers. The first layer is the infrastructure: actual physical connections that link Internet computers together. Next is the basic operational software that works behind the scenes as part of the core mechanisms which allow the network to function. Finally, more tailored user-interface software makes the network accessible and easy to use. Two or more computers connected together for purposes of sharing files or applications form a network.[5] A network is "closed" when its bounds are limited -- when it is either not connected to other computers or networks, or it is connected to a given number of other computers or networks which together comprise a closed system (such as a "local area network"). "Open" networks are created when many networks are connected to many other networks, which in turn are connected to other networks in such a way that it is impossible to know exactly what computers are connected. The Internet is such a "network of networks"; it has no central location or tangible presence, but is more a global phenomenon embodied in an enormous open network.[6] Separate computers and networks, which are interconnected and collectively form the Internet infrastructure, are owned by governments, public institutions, businesses, and individuals around the world. Each particular network is a separate, autonomous system that is independently managed. The Internet's distributed infrastructure relies upon special types of computers called "routers" to connect the different pieces of the network together. Interconnections of distinct, autonomous networks using common protocols is the basis of the Internet.

The Internet's basic hardware and software architecture was designed with the goal of creating a resilient network. This was accomplished through a system of decentralised, redundant, multiple connections between computers and networks that allow for automatic re-routing around connections that are damaged, overloaded, or otherwise unavailable. Because of this design, a particular transmission might travel any number of paths en route to its destination, and the path that it takes is determined dynamically by the system itself. The basic operating software for the Internet uses "protocols" that govern how data is sent from one site to another. The most important of these are the "TCP/IP"[7] protocols which tell the routers where to send data, and that allow "packet switching" communications where transmissions are broken down into smaller pieces, or "packets", that travel independently on the network and are re-assembled at their destination. The packets comprising a particular transmission may or may not be sent along the same route to their final destinations. The Internet protocols work together to make efficient use of the network infrastructure, so that even though there is not a dedicated link connecting two endpoints, for all practical purposes, it seems to the users that there is.

The "client-server" model is a common structure for Internet communications. In a client-server environment, the computational workload is divided between the local "client" computer operated by the user and the "server" computer that is connected to the Internet. In this model the client computer and the server computer each carry some of the operating and applications software in local storage. Applications software tailored to the various tasks which a user wants to achieve, and an easy way for users to know the addresses for computers connected to the Internet, make the network useful and simple.

Because numeric designations are difficult for people to remember, the user-friendly "domain name system" (DNS) was created to map names of network connections associated with particular Internet Protocol (IP) numbers. Every computer that is connected to the Internet has a numeric IP number which functions as an address record which tells the system where to send data. In its current implementation, the IP address is a unique number consisting of four parts separated by dots (such as "192.168.10.5") specifying the exact location of a connection to the network so that packets can be routed to a particular computer or device for delivery. The DNS assigns a "domain name" to a corresponding IP number. As the system is currently designed, a domain name has two or more parts separated by dots (such as "www.oecd.org") with one section indicating a specific computer or device, followed by a more general "top-level domain" (TLD) indicator, representing either a country code (for example .fr stands for France) or one of the generic top-level domains (such as .com, .org, or .net). It is possible for a single computer to host more than one domain name or to have more than one IP number, and a given domain name can represent more than one computer or a file system shared among computers. A computer or other device, while required to have an IP number to receive or send packets, need not have a domain name.[8]

Internet access and applications

Usually, access to the Internet is achieved either through a computer that is directly connected to a network which is directly linked to the Internet, or through a computer that uses a modem to connect via common carrier to another computer or network which is linked to the Internet. An example of the former is the kind of Internet access available to users on local area networks, such as those found at corporations, government agencies, universities, libraries, and other types of organisations, often with a dedicated connection to the Internet and a router. The latter type of access is often achieved via a commercial "Internet service provider" (ISP) which provides a "dial-up" connection to the Internet to consumer-users for monthly or hourly fees.

The non-hierarchical systems which comprise the Internet and the unique interactive nature of its distribution and access mechanisms mean that there is no centralised control of content on the Internet. Content on the Internet is dynamic in that it can be modified, adapted, transferred, re-used and re-sent

simply and quickly. It is mobile in that digitised data can easily move from one application to another. Furthermore, information can be exchanged between individual users, or it can be distributed from one-to-many, or from many-to-many. The ever-evolving state of information technologies make it difficult to describe definitively the applications available for accessing and distributing information on the Internet. However, there are generally seven different kinds of transmissions possible in today's Internet operating environment, as follows:

- One-to-one transmissions via electronic mail or "e-mail" (including one-to-several transmissions where e-mail distribution lists are used).[9]

- One-to-many transmissions via automatic electronic mailing lists, such as "Listserv".[10]

- One-to-many or many-to-many transmissions via distributed message databases, such as "Usenet newsgroups".[11]

- Real time communications, such as "Internet Relay Chat" (irc) or Internet telephony.[12]

- Real time remote computer operation, such as "Telnet".[13]

- Remote information retrieval, such as "File Transfer Protocol" (ftp) and "Gopher" .[14]

- Interactive graphical information retrieval and manipulation, as embodied by the "World Wide Web" (WWW or Web).[15]

The World Wide Web is the most recently developed and probably the most popular Internet application. The Web is unique because it is an open, distributed, decentralised and inexpensive system for organising and retrieving remote information, which is easy to use, both for presenting information to a wide audience, and for accessing information from disparate sources. The WWW uses "hypertext mark-up language" (HTML) to organise information in flexible ways for easy access and viewing. Client software programmes that "browse" the Web can view many types of information; they can also interpret hypertext "links"[16] to direct the browser to connect to another relevant Web page. This is possible no matter where the actual server that holds the information is located as long as it is connected to the Internet. The Web connects a vast collection of information from diverse sources by linking Web sites from one server to another. It is not only easy to use the WWW to locate information by following Web links, it is also easy to "publish" information on the Web by creating a Web page and making it available on a computer that is connected to the Internet. A Web site can be made accessible to all Internet users, or it can be limited to certain users through passwords or other access controls. A "search engine" is a specific kind of server that is accessible through the Web; it looks for key words or categories identified by the user can be used to locate particular information.

Unseen operations: duplicating data

Many of the Internet technologies, especially the WWW, often employ mechanisms for duplicating data which help them to operate as efficiently as possible in the global environment. Basically, duplication is used when some particular data is accessed repeatedly, such as a popular Web site that is visited frequently; the system works better if a copy of that data is offered as another source for accessing the content. Usually these are unseen operations that happen automatically and out of the sight of the user. Currently, there are two fundamental kinds of duplication mechanisms used for Internet operations: mirroring and caching.

Often "mirroring" is used to provide a local access point for data to reduce the distance for network connections and ease system and network congestion. A mirrored site, where a complete duplicate of the original site is hosted at another location, is usually created by a system operator because the content it holds is very popular and it is accessed very frequently by a large number of users. In such a case, the user accessing the data may or may not know whether he is accessing the original site or the mirrored site. The updating of the mirrored site may happen automatically every time the original site is updated, or it may be done manually by the system operator of the mirror.

Caching is another duplication mechanism used to address the high cost and frequent overload of communication lines. In this case, content is "cached" or temporarily stored in a local server, so that when information is requested, the local version is sent rather than the remote version. This provides an effective shortcut to increase the efficiency of network operations. The cache mechanism is totally automatic; data are duplicated dynamically by the system when certain content has been accessed frequently during a particular period of time or from a particular location, and they are generally discarded after a certain period of time, or when demand has declined. A cache mechanism is content independent, that is, it is merely an automatic response of the technology to help the network operate efficiently when the same data is being accessed very often. Cache files may be stored on a local area network or at the network backbone level (or anywhere in between). The user does not usually know the details of the caching mechanism in place.

Accessing content

Basically, when a user wants to access data on the Internet, the first step is to obtain a connection to the network, and to initiate the appropriate client software on his computer to run Internet applications. Where the user accesses content through newsgroups, the user must identify a newsgroup and subscribe to it. Where a user accesses content via the WWW, a search engine can be used to identify the location of particular information, and then the user points the browser software to the appropriate Web site to access the content. One important element of access to content on the Internet is that the potential audience is world-wide; when content is posted on the Internet, via a newsgroup or the WWW, it becomes available to anyone with Internet access.

There is an important basic difference between the way content is accessed on the Internet and through other types of media. The difference is often characterised in terms of "push" technologies and "pull" technologies. For instance, television or radio are "pushed" at the user who exerts only a minimal effort to seek out the content, while the Internet requires the user to "pull" the content onto his computer. An example of the most pervasive kind of truly pushed information in the physical world would be a message contained in a billboard or skywriting. There are few push technologies operating on the Internet today that compare with real-world billboards, but there are some pull applications which appear to be pushing because they require minimal effort by the user to initiate the transmission. "Pointcast", a form of "webcasting,"[17] offers an example of an application that looks like a push technology because the user subscribes and pre-selects the content he would like to see and then receives the specifically tailored content automatically. Unsolicited e-mail or "spam", usually used for commercial purposes in mass mailing, is one of the only push applications used on the Internet today. However, the possibilities for push technologies are not entirely clear; there might be potential for technology of the future to act like a billboard, for instance where a commercial backbone provider would require a certain information tag to be added to any data that crossed the backbone line. At present, content does not generally appear on a user's screen by accident; some initiation on the user's part is involved.

Identifying the main actors by function

There are a number of actors that play a role in the exchange of information on the Internet, including users, systems and software providers, content providers, various kinds of information carriers that provide the "pipes" and routing systems for data transmission, and service providers that can provide any number of different online services such as Internet access, Web site creation or hosting, or other kinds of intermediate services. In developing approaches to content on the Internet, it is important to determine which parties have the ability to control information on the Internet at different points in the delivery or access process. In the early days of the Internet, identifying the primary actors involved in Internet operations by broad category was sufficient because there was very little cross-over in their specific activities. However, today it is important to think about the actors in terms of their functions, the type of contact they have with information, and the technological and economic feasibility of any particular actor exerting control over the content of that information. The fluid nature of technology development means the functions change quickly. Today the various actors can perform a number of different functions, and those functions may change in the process of creating, accessing or delivering content.

Technological solutions and industry action to address harmful content

Technological solutions can empower users to make choices about the kinds of content they access and do not access, or they can empower Internet service providers to control who accesses the content they provide. These technologies do not provide absolute solutions -- the nature of the Internet makes it difficult to place absolute controls on content, and the economic and social costs of attempting to do so might be considerable -- but technological solutions are an important alternative to consider. Technological solutions are widely recommended as the best available approach to content issues today because they are readily available, easy to use and effective. Advocates argue that these technologies can accommodate a diversity of community values and educational needs, give positive guidance for children, and at the same time offer protection for free expression and the free flow of information. However, some commentators point out the possibility that these technologies could lead to censorship or at least further regulation of content, and that they are burdensome, unwieldy and costly. Also, there are concerns that certain kinds of valuable content cannot be accommodated by the technologies, and in particular that cultural differences are difficult to accommodate, raising the risk that technological solutions will homogenise the Internet. Nevertheless, there is wide support for finding solutions within the technologies themselves, driven by user demand and market principles.

Empowering users to choose

Filtering technologies and rating systems can be used together to enable users to block unwanted content. Basically, filtering technology provides mechanisms for creating "labels" that indicate specific characteristics of the content of certain data on the Internet, which can be read by filtering software to give information about the content of that data. When used in conjunction with a system for rating the content, the information indicated in the label gives clues about the content of the data based on certain rating criteria. Users can then choose which rating they would like to use and what kind of content they would like to block by using the filtering technologies. The ratings can be applied by content publishers themselves, or by third parties. What is critical in the choice of the rating system used within a filtering platform is who determines the rating criteria and on what basis. In that context, there is a tension between the need to reach a "critical mass" of rated sites in order for filtering technologies to be most useful, and the concern that a "lowest common denominator" rating will emerge that does not accommodate diversity in cultural and community values. A number of rating systems could emerge to work within a labelling framework.

Stand alone software is another method for limiting access to certain kinds of content on the World Wide Web. In this case, the software company provides either a "blacklist" of sites which are blocked by the software, or a "whitelist" of sites that are recommended for viewing based on certain criteria set forth by the software company. In some cases the software allows the user to select which kinds of content should be blocked. Often these companies employ people who follow links to search the Internet for Web sites that should appear on the list. They also use "web-crawler" technologies that search the Web looking for key word strings that identify sites likely to carry material which is deemed unsuitable by their standards. One of the primary issues raised with regard to these types of software solutions is whether the rules for exclusion from or inclusion on the lists are clear and public.

Another possible way to empower users to avoid unwanted content could be a top-level domain (TLD) mechanism that would indicate sites known to carry certain kinds of material. Such a TLD would make it possible for users to steer clear of or block all sites with that domain name. The creation of a special ".xxx" designation for adult-oriented Web sites to indicate a sort of "red-light district" on the Web has been proposed. This proposal would make it possible both to shut off access to those Web sites, and to locate them. One concern raised in connection with this type of system is that there is a risk that users who want to protect their children from harmful content might believe that all sexually explicit material is only found on ".xxx" sites, and they will not be aware of the possibility for harmful content to be found elsewhere on the Web.

Restrictions on access set by service providers

Blocking content could also take place at the level of the service provider rather than the user. The same types of blocking and filtering software would allow commercial providers to market blocking services for users who are willing to let someone else make the decision about what is blocked. For instance, Internet service providers could offer services to parents directed at protecting children from unwanted content.

Mechanisms for restricting access to certain content based on user criteria, such as age, is another way to restrict access to content. However this method is limited in today's Internet operating environment because there are few systems in place for verifying certain information about a user, such as age, credit card number or ID number, so it is difficult for restricted access systems to confirm information about the person they are dealing with reliably. Certification systems could be developed to verify electronically relevant information about an individual or entity without necessarily revealing a true name or other identification information. They could be used when it is not necessary to know the identity of the transacting party, but merely that the party has certain characteristics: age, address, registration to use a service, or membership in an organisation. For example, a consumer could be certified to be a certain age in order to purchase age-sensitive products in the electronic environment where the merchant need not know the identity of the consumer, but merely needs assurance that he is not selling to someone who is underage.

Self-regulation by industry

In addition to technological innovations to empower users and service providers to limit access to content on the Internet, there are a number of industry initiatives under way directed at developing self-regulation mechanisms, such as codes of good conduct. A number of national governments specifically endorse industry self-regulation as a front-line mechanism for addressing content issues. In many cases, codes of conduct to provide guidance on compliance with national law and expectations about business practices are emerging from industry associations representing the interests of their members. Generally,

the codes tend to focus on co-operation with law enforcement authorities, clarification of liability and responsibility issues, approaches to privacy and handling personal data, investigation of complaints, procedures for addressing illegal or harmful content, and promotion of technological tools to empower users. However, there have been questions raised with regard to the appropriateness of industry associations to act as representatives of service providers, in particular where service providers are international and industry organisations are based on memberships at national level.

Establishing hotlines and complaint handling procedures by industry actors is also an important element of self-regulation. Hotlines can provide a mechanism for users to report illegal or harmful content that they see on the Internet. In many cases, the hotlines are jointly sponsored by industry and government.[18] An established complaint-handling procedure must accompany the hotlines to ensure that reported information will be dealt with consistently. The process which follows the receipt of a complaint about allegedly illegal content is particularly important where hotline operators might be put in the position of making legal decisions that they might not be qualified to make. It is important to consider carefully the powers that hotline operators may be granted to act against particular content.

II. Current approaches

Government approaches: legislation, policies and practices

Many countries have developed national approaches to the issues raised by information content on the Internet. Policy makers are reflecting upon the issues at hand, and in many cases considerable efforts are focused on the development of technological solutions and industry driven initiatives to address public concerns about Internet content. The following inventory of national approaches presents a snapshot of the current situation in the OECD Member countries. Although some countries appear to be more advanced in their thinking and actions to address these issues, all OECD countries have indicated their serious interest in the issues and have taken steps to give those issues full examination and attention.

Australia

The Australian Federal (Commonwealth) Government announced principles[19] for a national approach to regulate the content of online services such as the Internet on 15 July 1997. In broad terms, the scheme focuses on the protection of minors from objectionable material and involves:

- A self-regulatory framework for online service providers supervised by the Australian Broadcasting Authority (ABA) with provision for investigation of unresolved complaints by the ABA.

- A sanctions regime that includes fines for serious breaches of the *Broadcasting Service Act 1992* by online service providers.

- A framework that will not hold online service providers responsible for the content accessed through their service where the online service provider is not responsible for the creation of that content or does not knowingly allow a person to use an online service to publish illegal material.

- A commitment that the Commonwealth will encourage the co-operative development of uniform State and Territory offence provisions regulating online content users.

The responsibilities of the various actors are recognised through the principle that online service providers will not be liable for content accessed by means of their service where the provider is not responsible for the creation of that content. Prime responsibility for content is intended to lie with the act of publishing or transmitting material by online users, and to be regulated by proposed State and Territory legislation. Service providers will not be subject to these State and Territory laws except to the extent that they are acting as content creators.

The Australian Constitution vests the power to regulate communications in the Federal government. This power is expressed principally through broadcasting and telecommunications legislation enacted by the Federal Parliament which in broad terms regulates "content*" (Broadcasting Services Act*) and "carriage" (*Telecommunications Act*), respectively. The censorship of non-broadcasting media *e.g.* cinema films, video and publications is a shared Federal/State responsibility with the States (and Territories) enforcing classification decisions at the point of sale.

The regulation of Internet content is not specifically provided for in Federal legislation at this time; however, some prosecutions in relation to child pornography have been launched under the *Federal Crimes Act*. Some State governments have amended their censorship legislation to include "online" offences but there is general agreement to consider a national approach with uniform State/Territory legislation complementing the Federal scheme (amendments to the *Broadcasting Services Act* expected to be introduced into Parliament in 1998) announced on 15 July 1997.

As a general principle, it is intended that material accessed through online services should not be subject to a more onerous regulatory framework than off-line material such as books, videos, films and computer games; that is, what is legal "off-line" should be legal online, subject to appropriate protection of minors. The framework is intended to: encourage online service providers to respect community standards in relation to material published by means of their service; encourage the provision of means for addressing complaints about content published by means of an online service; and ensure that online service providers place a high priority on the protection of minors from exposure to material which may be harmful to them.

As a general rule, where a service involves private or restricted communications (such as e-mail and intranets), it will not be subject to the regulatory framework, except to the extent that current provisions in the *Crimes Act* relating to the use of a telecommunications service in an offensive or harassing manner apply.

The co-regulatory approach -- industry self-regulation within a legislated framework -- is consistent with a number of studies and reports undertaken in recent years, specifically the Australian Broadcasting Authority (ABA) report "Investigation into the content of on-line services" (June 1996).[20] Recognising the global nature of online services and the inherent limitations of national systems of regulation, the Australian Government will actively pursue in international fora collaborative arrangements for multilateral codes of practice in relation to online content and the development of online content labelling techniques. The ABA, an independent statutory authority within the portfolio of the Minister for Communication and the Arts has actively forged links with other national regulatory bodies and has been commissioned by UNESCO to report on comparative online content regulation.

At the direction of the Minister for Communications, the Information Economy and the Arts, the ABA is currently investigating a number of issues such as matters that might be included in codes of practice and developments in the use of online content labelling. Their advice on these issues is intended to assist in the transition to the new regulatory arrangements.

Austria

Thus far, the Austrian approach is based on the principle that the rules that apply off-line to also apply in the online environment.[21] Generally, all relevant laws apply to the Internet; however, enforcement can be a problem. In addition, the roles of actors not known in the traditional off-line environment (such as access providers) will require further examination. The Nationalrat, one of the two chambers of the Austrian Parliament, has requested the Minister of the Interior to take measures to prevent access to data that encourage crime. A special law to combat illegal use of the Internet is planned, but no draft exists as yet. Planned measures will, in all likelihood, include a requirement for providers to assist in identifying people responsible for content.

A hotline has been set up where citizens can report criminal content (especially hate propaganda and child pornography).[22] While no general definition for "harmful content" exists, in Austria, harmful content is considered the sum of all types of content defined as harmful and illegal under specific laws, including the interpretation of these laws by the courts. Existing national laws already permit the police to order criminal content to be taken off the Internet and complaints concerning online content from foreign countries are passed to the competent authorities abroad via Interpol. It is important to note that Austrian law applies if the intended outcome or effect of a criminal offence takes place in or affects Austria even in part. Therefore Austrian law is considered to apply to criminal acts committed on the Internet if illegal content is received and/or downloaded in Austria.

Austria has also established working groups to study these issues. In principle, illegal actors who use the Internet as a medium for publication or a means for committing fraud would fall under the existing Austrian legislation on media or on criminal behaviour. However, Austria considers that the main problem appears not to lie in national law, but in enforcement across national borders. Since content on the Internet is readily accessible from anywhere in the world, it frequently makes national legislation a moot point. Austria is interested in examining the question of what laws apply, and how to address fundamental legal differences, particularly in cases where illegal content in one country falls under the right to free speech in another. Furthermore, Austria is addressing the question of whether new regulations are required to define the obligations of the different types of service providers. The new Austrian *Telecom Act* prohibits harassment and intimidation, and requires reasonable precautions against misuse.[23] The ISPs are only subject to criminal prosecution if they knowingly ignore illegal content.

Belgium

The Belgian approach to Internet content issues begins from the premise that the emergence and development of the information society and the explosive growth of the Internet which has accompanied it are very important and positive. These developments will have a great influence on society, notably with respect to employment, education, electronic trading, finance and the provision of services to citizens by public authorities. Unfortunately, it must also be noted that the development of the information society also has a certain number of negative aspects. As yet it is only a matter of marginal phenomena, but this is no reason to deny or underestimate the problems.

To fully understand the Belgian perspective, it is important to recall the tragic events that occurred in Belgium last year, and the country's strong reaction to the sexual exploitation of minors. When it emerged that information on paedophilia was circulating on world-wide computer networks like the Internet, it became clear from the Belgian perspective that government intervention was necessary. These efforts began with an investigation as to whether a reform of existing legislation on telecommunications could prevent the dissemination of this kind of information on the Internet. The main conclusion was that given the complexity of the problem and its international context, any hasty changes in

this legislation would likely be largely ineffective. The current national approach to the problem is, therefore, based on the principle that initiatives should be taken at European and international level, and that the strategy to follow should place considerable emphasis on self-regulation. Regulatory action by the authorities may subsequently be useful to provide legal backup for the self-regulation regime.

In the light of this evolution, Belgium currently concentrates its efforts on developing measures aimed at combating the sexual exploitation of minors via the Internet. Research has shown that the criminal law provisions concerning paedophilia have sufficiently general coverage to be directly applicable to new media such as the Internet. The concrete solutions introduced may serve as an example for combating other kinds of illegal information available on the Internet (*e.g.* illegal gaming, racism and terrorism).

Representatives of the public authorities (Telecommunications Ministry, Prime Minister's Office, Ministry of Scientific, Technical and Cultural Affairs, Belgian Institute of Postal Services and Telecommunications) and the private sector (Internet service providers) have been in consultation and are examining the following subjects in particular: the drafting of a code of conduct for Internet providers and the establishment of a contact point (or collaboration with an existing contact point) for the detection of information of a paedophilic nature. This co-operation should lead to practical solutions and concrete initiatives for the fight against the sexual exploitation of minors. The Internet Service Providers' Association of Belgium (ISPA) recently took the first steps to implement a code of conduct intended to apply to all access providers. The ISPA is also expected to support the use of contact points. Lastly, the National Commission against the Sexual Exploitation of Children will be holding a national forum at the end of May, at which this problem will be dealt with in depth. The Commission may formulate recommendations for the attention of politicians.

Belgium is also pursuing technological solutions, in particular blocking and filtering systems, such as the Platform for Internet Content Selection (PICS). Along with promoting self-monitoring by users and training programmes, Belgium will promote these developments for application at the European and international level. The Belgian Government recognises technology as an important part of a "package" of solutions that can be developed and used to address these problems. Other such measures include the drawing up of codes of conduct for Internet access providers or international collaboration among several contact points permitting the transfer of information on illegal contents, which clearly go beyond the purely technical aspects of the problem. Belgium also recognises the need to ensure good collaboration among both national and international legal services, and stresses the importance of international collaboration to adjust and amplify the different initiatives, in both public and private sectors.

Canada

Canada considers that although its laws have not been defined with respect to specific activities as they relate to the Internet, Canadian laws of general application also apply to Internet activities. Canadian laws are generally technology-neutral and apply to activities, rather than actors. The *Canada Constitution Act*, the *Charter of Rights and Freedoms*, the *Criminal Code*, the *Copyright Act*, the *Telecommunications Act* and the *Broadcasting Act*,[24] federal and provincial consumer protection legislation, as well as other civil statutes apply to Internet practices and services. To date, case law in matters related to Internet content is very limited and most prosecutions under the *Criminal Code* have been against end-users. There is still uncertainty surrounding the extent of liability faced by Internet access and service providers. Under Canadian law, each person is responsible for statements he or she makes whether it be by post, telegram, facsimile or other mode of telecommunication, in print or electronic media or on the Internet. There are in Canada two distinct regimes of private law: the civil law of the Province of

Quebec and the common law regime applicable in the rest of Canada. Various provincial and federal statutes have also created regimes of civil liability in the area of privacy.

Internet issues are not new to the Canadian government, as studies and work have been done by the Information Highway Advisory Council (IHAC). IHAC was created in April 1994 and is composed of representatives from the information and communications technology industry, as well as from cultural industries, unions, libraries, universities and consumer groups. It was established to advise the federal government on carriage and content issues, including those related to the Internet, copyright, information controls and privacy. As a response to IHAC recommendations, Canada began a study in the summer of 1996 to describe how present laws apply to Internet activities, and to assist in defining the main concepts and actors involved in Internet services. The study was published in March 1997 and is entitled "The Cyberspace is not a 'No Law Land'."[25] Also, in 1997, Canada completed a second phase of revisions to its copyright legislation. It was agreed among all parties and stakeholders that any required revisions dealing with the digital environment and the Internet would be part of a subsequent phase.

To date, the government and the federal broadcasting and telecommunications regulator, the Canadian Radio-television and Telecommunications Commission (CRTC), have not instituted any actions relating to content on the Internet. Telecommunications facilities used by the Internet come under the purview of the Telecommunications Act and the CRTC. Because facilities-based telecommunications carriers are obligated to provide non-discriminatory access to their networks, the CRTC has the authority, under the Telecommunications Act, to limit their financial liability in the provision of services. Canadian carriers, as defined in the Act, are the only ones eligible for this treatment. In August 1996, the government issued a Convergence Policy Statement in order to provide an appropriate policy framework for the convergence of the Canadian broadcasting and telecommunications industries for the provision of facilities and services in a new competitive environment. The Convergence Policy Statement put forward the government's policy objectives and clarified a policy framework to allow cable companies and telephone companies to compete in each other's core markets, subject to the relevant rules under the Broadcasting Act and the Telecommunications Act.

The Canadian Government has been in close communication with the private sector regarding many aspects of liability on the Internet. With a view to assisting industry, Statistics Canada recently conducted a survey of Internet service providers in Canada. Internet Service Providers (ISPs) were asked to indicate the significance of the "threat of litigation" as a barrier to growth and whether they had received customer complaints regarding offensive content.

In general, the federal government does not operate community education programmes on offensive content, but does support and promote them. The Media Awareness Network, linked to Industry Canada's SchoolNet site, is a national online organisation dedicated to media education and media issues affecting children and youth. It provides both a clearinghouse of information and an interactive network for the sharing of ideas and initiatives.

The following studies have been commissioned or supported by the Canadian Government:

- "Building the Information Society: Moving Canada into the 21st Century" (May 1996), Government of Canada.

- "Connection, Community, Content: The Challenge of the Information Highway, Final Report of the Information Highway Advisory Council" (September 1995), Information Highway Advisory Council.

- "Illegal and Offensive Content on the Information Highway" (June 1995), a background paper prepared by Gareth Sansom, Spectrum, Information Technologies and Telecommunications Sector (SITT), Industry Canada.

- "Preparing Canada for a Digital World, Information Highway Advisory Council, Phase II Conclusions and Recommendations" (April 1997), Information Highway Advisory Council.

- "The Cyberspace is not a "No Law Land" (February 1997), a study of the issues of liability for content circulating on the Internet prepared for Industry Canada by Michel Racicot, Mark S. Hayes, Alec R. Szibbo and Pierre Trudel.

- "Undue Exploitation of Violence" (March 1996), a consultation paper released by the Department of Justice, Canada.

Czech Republic

The Czech Republic has not developed specific policies or positions on issues related to Internet content. However, on 7 May 1997 information on the use of the Internet in the Czech Republic was presented in the Parliament in order to examine the possible impact on legislation. Legislative changes in connection with the Internet are expected to be introduced sometime in 1988 following parliamentary discussion specifically with respect to the Broadcasting and Telecommunication Laws.

There are currently 43 Internet service providers in the Czech Republic. In general, the position of the Czech Republic Government with respect to public services is that content on the Internet should be regulated by the author, and that the responsibility of observing the valid legislation lies with the author, as the provider can supervise it only in a limited way. In the case of non-public services, the Government views them as similar to a telephone conversation or postal item where the information is considered to be private and cannot be manipulated without permission of the author or court decision. The Government is also prepared to introduce strict rules for domain registration; at the present time domains with unethical names are not being registered in the Czech Republic.

Denmark

Regulation of content

In Denmark, the Internet is viewed as a new media through which one can perform acts already established in the "real world". From this perspective, content on the Internet falls into categories with different characteristics, such as private correspondence, marketing, news coverage, etc. These types of content correspond to types of communication or mediation already well known and regulated. From the Danish perspective, the overarching principle governing the Internet is that the same rules apply regardless through which media an act is expressed. Thus, no special rules should apply for content distributed through the Internet. A review of the existing regulation is under way in order to secure that the rules are applicable to the environment of the Internet.

In Denmark, pornography (with the exception of child pornography) is legal. Thus, pornographic material can be purchased by everybody in news stands, bookstalls, etc. Denmark believes that it is the task of the parents to protect their children against items deemed unsuitable. With respect to television, because when turning on the television set or changing the channel, the viewer does not know what he or

she is going to see, certain rules have been established to protect children. Denmark believes that this same condition does not apply to the Internet where pornography and other material that may be considered to be objectionable will only be available as a consequence of a number of deliberate choices.

In Denmark, the penal code is applicable to illegal material such as child pornography, fraud, discrimination, defamation and slander. According to the penal code, both the person committing the actual crime and the person instigating or in any way taking part in the crime are considered liable. Under the terms of the Danish regulation, the liability is laid upon the originator of an offence. This applies regardless of whether the illegal material is distributed as private correspondence in the form of e-mail or published on a bulletin board. Based on the assumption that only the author of an e-mail has knowledge of the content, in Denmark no other person can be legally responsible for the content.

In the case of the offence being performed through publication, the potential that someone other than the initial originator may be held liable increases. A number of provisions in the Danish penal code state that the person distributing the offensive material is also liable. However, as a condition for determining such liability, the person distributing the illegal material must be found to do so intentionally. With respect to the Internet, prohibition of child pornography means that the person uploading child pornography to a bulletin board ("BBS") will be legally responsible. If the person managing the BBS -- the SysOp -- specifically invites the uploading of child pornography, he can be punished for complicity. If the SysOp is aware of illegal material being made available on the BBS and does not remove it, he can also be held liable for the distribution. However, a SysOp or an Internet supplier can not be made liable for illegal content which he or she has not contributed to, participated in, or had no prior knowledge of.

The only possibility for placing strict liability for a penal act is in reference to the Danish Media Responsibility Act. According to the Act, an editor is liable for anonymous material being published. However, this Act will only apply to a very limited extent to distribution through the Internet as the Act covers only news distribution conforming to a number of substantial demands as to the nature of the distribution. In addition a notification must also have been given to the Press Council.

Where the originator of an offence must be held liable for an offence that has taken place –especially in relation to the Internet– tracking down an anonymous offender and being able to prosecute across national borders can be particularly problematic.

The basis for the Danish regulation of commercial marketing is a general clause of the Act on Marketing (§ 1). The clause does not differentiate among the various media being used by the commercial actor and thus can be applied to infringements taking place on the Internet.

Due to the strong impact of the media, advertising on television and radio in Denmark is subjected to restrictive rules beyond those included in the Act on Marketing. The Internet has a similar direct and strong ability to influence consumers as users may automatically receive advertisements without having requested them. Therefore, similar sharpening of the regulation for Internet-specific activities could be advocated. Furthermore, Denmark believes that with time, marketing via e-mail will grow to such an extent that it will be necessary to impose limitations in this field and that broad international agreement will be necessary to develop effective and appropriate regulation.

Non-regulatory initiatives

Danish legislation sets standards for content which are considered suitable, adequate and applicable to the Internet. However, due to its global nature, the Internet poses certain difficulties with respect to the investigation of crimes and the enforcement of laws and regulations. These circumstances

have raised the issue of the possibility of self-regulation. From the Danish perspective, the potential benefits of self-regulation must be carefully weighed against the possible implications for the freedom of information. The Danish Government has not undertaken any initiatives concerning the elaboration of a "code of conduct".

With respect to the ability of parents to protect their children from Internet content suited for adults only, Denmark believes that rating of content on the Internet may be a viable solution. Thus, tools for parental control could give parents, teachers and others the ability to set limits that meet their own moral standards and which they judge to be suitable for the children in question. However, it is fundamental that such rating and filtering tools do not unnecessarily exclude material and must reflect cultural diversity.

The use of rating and filtering tools must take place on a voluntary basis, and it should always be obvious to the user when filtering technologies are being used. From the Danish perspective, three fundamental principles must apply to all forms of self-regulation of the Internet: voluntary use, transparency and cultural diversity.

The Danish government is preparing a report on the responsibilities of the actors on the Internet, including:

- In which situations is the ISP responsible for illegal content?
- Does the ISP have the right to sort or to block access to content in all situations?

Furthermore the Danish government is preparing an initiative to bring together law-enforcement agencies and ISPs in order to discuss enforcement of criminal law on the Internet, including:

- Establishment of a hotline for illegal content.
- Identification of the respective roles for law enforcement and the ISPs in the enforcement of criminal law on the Internet.
- Possible development of a code of conduct for ISPs.

The Danish Centre for Human Rights has completed a study commissioned by the Danish Government which has resulted in a note on the Internet as a tool for dissemination and safeguarding human rights.

Finland

In Finland the Internet is viewed merely as a new means of accessing information which does not present any special need for new legislation. Internet content is subject to the same laws and regulations as the off-line world, and criminal law applies as it did before the information society emerged.

Although there are no definitions of the main concepts or actors involved in Internet services specified in the legislation in force, Finland clearly distinguishes the different roles, functions and responsibilities of content providers, on the one hand, and technical intermediaries, on the other. In addition, content providers could be classified as those who provide their own self-made content and those who provide content and/or links to content made by someone else. Technical intermediaries on the

Internet might be differentiated as network operators and Internet service providers providing simply access to the Internet or both access and hosting services.

The Finnish Government believes the development of the information society should not be hindered by heavy liability and economic burdens or by constant regulatory activities. This might include the compulsory use of filtering software -- which the Government views as counterproductive -- or compulsory use of labelling techniques -- which is considered to be too expensive and impossible to use effectively because of divergent cultures and values world-wide. Finland believes that the question of harmful content on the Internet (content which is not illegal but might not be suitable for a certain category of users) should primarily be dealt with through educational measures.

A report on freedom of speech in mass communications was issued in February 1997, which takes into account the convergence of new and existing technologies and media. It suggests creating a system of editorial responsibility similar to the one for traditional media for online services. It also emphasises the traceability of anonymously made electronic messages. The report has been largely debated in public because of the allegedly negative effects. The proposed system could be disproportionately expensive and place too heavy technical obligations on different actors in the online activities. Nevertheless, the report is expected to serve as a basis for a proposal for a new law in Finland.

The Finnish Ministry of Transport and Communications hosted a meeting for Finnish Internet service providers on the issues of Internet content and self-regulation. The basic idea of creating a self-regulatory body was welcomed, as was the concept of working with police authorities to establish a hotline where illegal content could be reported. The Ministry expressed its concerns on the subject but, for the time being, has decided to let the private sector determine the modalities and extent of the co-operation.

Two discussion papers dealing with online content and conduct issues have also been prepared by a working group in information networks. They are called ”Privacy and Freedom of Speech on Information Networks” and ”Public Communication On Information Networks”. These papers have not resulted in any regulatory measures.

France

In France, an important distinction is made between what belongs to the category of private correspondence and is therefore protected by secrecy of correspondence, and what belongs to the category of public communication where the fundamental principle of freedom of expression applies. France believes that these issues must be respected but must also be reconciled with the respect of certain imperatives of general interest like public order and national security. In addition, the characteristics of the services and messages should take precedence over their method of transmission ("carrier medium"). In the communications field, where technological progress is extremely rapid, France believes it is essential that the legal rules should be technologically neutral. In this respect, the distinction between Web-related services and electronic mail is taken in France as a fundamental line between broadcast communications and private correspondence. Nonetheless, the legal status of a number of services, notably forums, remains unclear.

It is hard to distinguish between actors who perform several different service functions. It is for this reason that France believes that defining service functions is worth pursuing in view of the implications in terms of applicable legislation and particularly in terms of liability. The definitions should relate to functions rather than to individual types of actor on the grounds that, in providing services, actors may combine several different functions. In this respect, observation of how services are provided allows

a distinction to be drawn between infrastructure operators, access providers, service providers, operators providing a range of services, host providers, and content publishers.

Aware of the opportunities offered by the development of the Internet but also the issues this development raises, the public authorities in France have, for several years, undertaken a number of studies and introduced measures with regard to information content on the Internet. In 1996, the Government gave a member of the Conseil d'État an interministerial remit to analyse the legal issues raised by Internet development and to identify areas where existing legislation might need to be amended. While the conclusions of the ensuing report stressed that the legal system in France was adequate to the task of punishing offences committed on the Internet, it also recommended that international co-operation should be developed, that self-regulation should be encouraged (although not to the exclusion of regulation by government) and that responsibilities should be clarified in order to deal with problems relating specifically to the Internet. On the other hand, the public authorities in France have encouraged the emergence of a concerted dialogue on the issue of self-regulation by Internet actors. A working party, set up in October 1996, has drawn up practical recommendations. The list of measures arising from this work is currently being validated. Following upon debate by the Parliament, administration, experts, and users, a new in-depth study has been assigned by the Prime Minister to the Conseil d'Etat with the goal of outlining the changes to the law that will be necessary. These modifications must permit an effective response to the negative aspects of the Internet, while at the same time ensuring the promotion of freedom of communication. Two other studies in progress relate more specifically to electronic commerce and the protection of freedom and private life.

In terms of the principles on which self-regulation should be based, France believes two specific requirements are important: the need to set up a direct link, such as a hotline, to allow a rapid response to problems encountered by users with regard to information content, and the need to co-ordinate the response of service providers to changes in Internet practices. The provision of non-governmental channels of information to ensure that action is taken on the incidents reported, and that, more generally, self-regulating bodies exchange information and co-ordinate their activities, might be avenues that could be explored in greater depth.

Moreover, with regard to new technologies, work is proceeding in France on the design and development of content filtering systems. The education sector is the main area in which this technology is currently being used on a trial basis. To be effective, France believes such tools must be designed to accommodate the labelling of a critical mass of content within a limited number of different analytical grids. Achieving this critical mass requires concerted international action that respects the diversity of different cultural viewpoints, whether in terms of the multiple labelling of content by an individual actor or a supply of services that has been adapted by a third party. It nonetheless remains true that this type of tool does not solve the problem of intentional use of the Internet for criminal purposes. France believes that this solution is therefore insufficient and cannot absolve governments of the need to identify common values and areas in which co-operation would be desirable.

While every encouragement must be given to national initiatives on self-regulation, France believes it is important to bear in mind that at present there is no way to determine whether the system is capable of regulating itself efficiently. There can be no question of these ethical rules taking the place of action by the legal authorities in the event of proven offences. The identification of common values at international level is considered to be necessary although not easily achievable. France believes that action must therefore be taken to ensure that any problems that might arise in defining such values does not act as a brake on the consideration that will, at all events, have to be given to the legal system and the penal regime in particular.

In addition, France considers it advisable to clarify the scope of responsibility of actors to ensure the requisite degree of security for the development of such services. From this standpoint, the French authorities had originally planned to make the existing legislation more explicit and, in particular, that access providers cannot be presumed to be responsible where they did not take part in the offence or were unaware that the offence took place. This amendment was ultimately not introduced.

Germany

The German approach to the issue of content is not to regulate the Internet as such, but to establish a broad legal framework for the provision and utilisation of information and communication services which can be offered on any network, including the Internet. The Federal Government's Information and Communication Services Bill ("IuKDG" or "Multimedia Law") was adopted and entered into force on 1 August 1997.[26] Additionally, the Media Services Interstate Agreement of the German *Länder* also entered into force on 1 August 1997. This Multimedia Law is the first general regulatory framework pertaining to the information society in Germany. It is the first law to include - in addition to amendments to existing laws - provisions governing the responsibility of service providers (for example, on the Internet), digital signatures and data protection for the new services. The law thereby provides legal and organisational security and creates a sound basis for electronic commerce.

The IuKDG takes into account the applications of modern information and communication technology, which today increasingly pervade all spheres of life. These include a range of applications such as: online shopping; the electronic handling of routine private banking transactions; the communication of confidential medical data between doctors, health-insurance companies and patients; and the transboundary communication of transaction data in global banking. The paramount principle of the IuKDG is: deregulation before regulation. The law confines itself to the statement of essential facts that the Government believes require immediate regulation in order to define the legal framework required for economic development and eliminate any existing legal uncertainty. In addition, areas of particular interest to the public will be safeguarded, such as the protection of minors and consumer-related issues. The law contains provisions on teleservices generally, data protection, digital signature, the penal code, administrative offences, the dissemination of publications morally harmful to youth, copyright, and price indications.

The responsibility of the actors involved, particularly that of the providers, is clearly defined in the German IuKDG. Under the law, all providers are responsible for their own content while mere access providers are not responsible for third-party content that they make available; however, the obligation to exercise due restraint irrespective of responsibility remains unaffected. Providers who make third-party content available are responsible for such content if they have knowledge of the content and are technically able and can reasonably be expected to block the use of such content.

The laws governing criminal and administrative offences in Germany have been amended in order to guarantee that general legal provisions (including penal law) can be applied not only off-line but online as well. In light of the increasing possibilities for using and disseminating illegal content, the term "writings" was redefined to include both data carriers and working memories. In this way, under German law, all criminal and administrative offences committed by means of or with writings are covered even if the latter are disseminated via electronic data networks.

General prohibitions pursuant to German penal law and administrative offences law have been extended to cover content made available through information and communication services. This was first accomplished by redefining the term "writings" which plays a central role in penal law. Under German law, writings now clearly include data storage in computer systems. However, this does not mean

government control of content in Germany. Content -- including content made available or transported by information and communication services -- is governed by the principle of freedom of opinion, which is protected as a basic right. Censorship is prohibited under German constitutional law. In addition to the above-mentioned limits stipulated by general legislation, and in particular by penal and administrative offences law, special regulatory provisions have been made for content which, though below the penalty threshold of penal law, is harmful to youth, the intention being to create a barrier to help protect minors. The Information and Communication Services Law provides that, by request, the Federal Board for the Review of Publications Harmful to Youth, if so requested, shall see to it that also content disseminated via data networks be examined by a plural body. If this body takes the view that the content in question is harmful to minors, it will include this specific content in a list and the content involved will be subject to restrictions on distribution regarding minors. This does not make the content illegal; it will continue to be accessible to adults as long as the restrictions on distribution are observed and technical arrangements have been made to guarantee that the content will only be offered or disseminated to persons of full legal age.

At the same time, major German enterprises and associations including content providers and service providers have joined forces to ensure voluntary self-regulation in online communications. They established the multimedia service providers self-regulation organisation, which started work on 1 August 1997.

Greece

In Greece, Internet-related issues are primarily examined by the Ministry of Transport and Communication and the National Committee for Telecommunications (NCT). In Greece, it is generally accepted that regulations relating specifically to content and access to the Internet are necessary. In this regard, Greece is applying existing law, including the recent EU Ministerial resolutions, and believes in broader international co-operation.

Within the framework of its regular meetings with representatives of the main Internet service providers in Greece, the NCT has examined the issue of illegal and harmful content on the Internet and has reached an initial agreement for the development and application of a self-regulatory system.

A working group will study the issue and will submit proposals for the implementation of a self-regulatory system, which will also include the operation of a hotline. The principal Internet service providers in Greece and a representative of the NCT are participating in this working group.

Hungary

Under the Hungarian legal system, information-related rights and freedoms are highly regulated. The Hungarian Constitution guarantees the freedom of information, the freedom of expression, the freedom of scientific research and teaching, and the right to protection of personal data. In addition to the combined Data Protection and Freedom of Information Act of 1992, there are a number of sector laws which apply, including:

- The Telecommunications Act of 1992.
- The Broadcasting (or Media) Act of 1996.
- The Telecommunications Policy (to be accepted in 1998).

In response to the needs of the Hungarian public and private sectors, a separate bill on the legal status of electronic documents and digital signatures is being prepared, and others, such as the information policy bill, are planned.

The Hungarian Constitutional Court and the Parliamentary Commissioner for Data Protection and Freedom of Information (since 1995, known as the Information Ombudsman) have a major role in shaping the legal environment. The Interdepartmental Committee for Information Technology and Telecommunications (1997) is responsible for developing information and telecommunications policy and providing the highest level of co-ordination. The tasks and functions for the strategy and execution of information and telecommunications policy are divided among several ministries and government offices, including the Ministry of Transport, Telecommunications and Water Management, Ministry of the Interior, the Prime Minister's Office, the Ministry of Culture and Education, and the National Committee for Technological Development. Several non-governmental bodies monitor activities in the information and telecommunications field, in order to provide balance and represent the interests of the various players, including the National Telecommunications and Information Technology Council (1996), the Telecommunications Conciliatory Forum (1995), and the Information Technology Conciliatory Forum (1997). Among other duties, these organisations are charged with operating a hotline service where illegal content can be reported, and appropriate follow-up measures are initiated.

In Hungary, the Internet is generally considered to be a new means of accessing information which does not present any special need for new legislation. Internet content is subject to the same laws and regulations as the off-line world, and the Hungarian Criminal Code applies in the same way it did before the information society emerged. That is, what is legal "off-line" should also be legal online.

Hungary does not currently have any national initiative to study harmful or illegal content on the Internet; however, last year a public debate on hate speech was initiated in both print and electronic media, and a study was commissioned by the Ministry of Culture and Education on the copyright and content restriction issues in relation to the recently launched "Sulinet" programme (which is intended to provide full Internet access for all secondary schools in the country).

While there are no definitions of the main concepts or actors involved in Internet services specified in the legislation in force, Hungary clearly distinguishes the different roles, functions and responsibilities of content providers and technical intermediaries. In addition, Hungary generally classifies content providers as those who provide their own self-made content, and those who provide content and/or links to content made by someone else. Technical intermediaries in the Internet environment might be differentiated as network (infrastructure) operators and Internet service providers simply providing access to the Internet or both access and host services. Technical intermediaries are officially regarded as telecommunications service providers in Hungary, and are therefore subject to the telecommunications law.

There are at least six national (Hungarnet, EUnet, Datanet, Matavnet, Sulinet, Elender) and more than hundred local and regional Internet service providers based in Hungary at this time. Many are members of the Association of the Hungarian Internet Service Providers (1997) which was originally created to develop and execute the domain name allocation policy, and handle other policy issues.

Hungary believes that the principal responsibility for content lies with its creators or publishers. As a general rule, each person should be responsible for the statements he or she makes, whether it be by post, telegram, facsimile or other modes of telecommunication, in print or electronic media, or on the Internet.

In Hungary, online service providers are not liable for the content accessed by means of their service where the provider is not responsible for the creation of the content. However, online service

providers may not knowingly allow a person to use their service to publish illegal, harmful or controversial content.

The Hungarian Government believes the development of the information society should not be hindered by heavy liability and economic burdens, nor by constant regulatory activities. This could include the compulsory use of filtering software, which is seen as counterproductive, or the compulsory use of labelling techniques that are, to their view, too expensive and could be impossible to use effectively because of world-wide ethical differences. Hungary believes that the question of harmful content on the Internet -- specifically content that is not illegal but may not be considered suitable for certain categories of users -- should primarily be dealt with educational measures. Nonetheless, the Hungarian Government acknowledges that international co-operation is necessary due to the transborder nature of these activities.

In order to take account of the convergence of new and existing technologies and media, in-depth studies and public debate are needed. Among others, the following topics are to be studied:

- Rating, labelling, filtering and screening techniques, such as PICS (Platform for Internet Content Selection).

- Editorial responsibility for online services (similar to those for traditional media).

- Traceability of anonymously made electronic messages.

The results of these and similar activities might be used as a basis for amending or modifying existing legislation. Legal issues related to content on the Internet are gaining importance with the progress of the “Sulinet” programme mentioned above.

It should be noted that thus far no crime or other serious offence committed over or via the Internet has been reported in Hungary. Nonetheless, several cases were reported to the Information Ombudsman, for example:

- An Internet service provider cut off a Web-site containing the Hungarian translation of Adolf Hitler's Mein Kampf.

- The police investigated the case of an attempted bomb attack where the “recipe” of the bomb could have been taken from the Internet, and the police wanted to learn about all Internet-subscribers in the region.

- Handicapped children were offered for adoption on the Internet, including photos and detailed descriptions.

Iceland

No formal study of Internet content issues has been conducted in Iceland to date. The distribution of material via the Internet is seen as just a new medium, and the existing legal framework is considered largely sufficient to deal with issues that may arise through its use. Two recent court cases have been decided based on the existing law on pornography. A proposal is under consideration in the Parliament of Iceland that is intended to amend the penal code to make it specifically applicable to computer fraud. In addition, a recently appointed editorial board for the Administration's Web site is preparing to publish a code of acceptable use, intended to guide editors of official Web sites.

In Iceland, the determination of legal responsibility appears to be clear as it relates to providers of information. The status of service providers, such as operators of Internet nodes, who provide only technical facilities and services necessary for operating the networks, has not been as clearly defined, as there is no legal precedent. The primary wholesale supplier of Internet connectivity in Iceland has an acceptable use policy that stipulates measures for authentication and traceability, and, in addition, disallows uses that might be considered malicious or unethical.

Ireland

The Department of Justice of Ireland has recently established a Working Group on Illegal and Harmful Use of the Internet which includes representatives from the public and private sector and has the following terms of reference:

- To identify the nature and extent of the issues surrounding the illegal and harmful use of the Internet.

- To prioritise such Internet issues with particular reference to the need to address the issue of child pornography in the short term.

- To examine and assess the current approaches both domestically and internationally to addressing Internet issues.

- In relation to those issues which can be domestically addressed, to identify the legal, technical and structural problems which arise and to make specific recommendations for their resolution in terms of short-, medium-, and long-term proposals as appropriate.

- In relation to those issues which require resolution in an international context, to make recommendations which will inform policy in this regard.

Ireland takes the perspective that technology has moved ahead of the legislation, and that national law, even when amended, will only partly address the very complex international legal issues to which the Internet gives rise. Ireland believes that technological developments will have a role in addressing the negative use of the Internet, but they are only one element in the effort to address these issues. The Working Group is examining policies to support industry self-regulation and the development of technological solutions which can help to empower users to protect themselves. However, Ireland believes that such self-regulatory efforts should be considered as part of an appropriate regulatory environment within which self-regulation would operate. Ireland has an eye towards international developments, and believes, in particular, that industry solutions would be most effective if internationally co-ordinated.

Italy

Italy pays special attention to the Internet phenomenon, particularly in its role in the global information and communications infrastructure. In order to ensure the proper development of the technology and guarantee the participation of all citizens in the new forms of communication, the Italian Government -- conscious of the significant social, cultural, economic and educational implications of this tool -- launched some time ago a number of initiatives and took major steps (including tax measures) to stimulate growth at all levels.

Given the nature of the medium and its rapid development, the Italian Government and Parliament are working to prepare concrete proposals related to rating content transported on the global networks. The priority areas of this action plan include: protection of minors (against violence, pornography and illegal forms of commercialisation); the protection of intellectual property; economic security (fraud and illegal use of electronic means of payment); and the protection of privacy (unauthorised transmission of personal data, other violations of privacy).

Therefore, Italy is fully in line with the guidance issued at EU level which encourages co-operation between States at the level of Ministers of Justice and the Interior, emphasises questions of liability of access and service providers and promotes self-regulation. In that context, at the stage of "domain name" registration, the Italian domain name registration authority has drawn up a ruling which provides for the allocation of responsibility for activities related to the use of the Internet, which the person requesting the domain name is bound to observe.

In Italy, the protection of the fundamental rights and liberties of individuals, in particular in respect of personal data -- already affirmed by certain European Community legislation[27] -- is reflected in the Italian regulatory environment by a specific law[28] which covers a range of subjects including databases, security, protection of privacy. As regards personal data, a particular class of information is envisaged (sensitive data) -- such as state of health, membership of a political party, religious convictions -- which is subject to very strong regulation aiming to guarantee full protection of secrecy and privacy.

In the framework of electronic security and of the integrity and authenticity of electronic documents, Italy has recently approved a law which gives legal status to digital documents -- drafted by the public administration or by individuals -- as well as to their storage and transmission by telecommunications. Under this law, digital documents will achieve the status of legal writing through the use of complex software based on asymmetric key cryptography supported by the electronic signature of the author.

In Italy, several criminal laws provide for prosecution for distribution of information with illegal content, or even harmful content, by means of information networks. The Italian Parliament approved a law[29] charging the Government with the responsibility of promulgating one or more decrees to implement Italian laws regarding the processing of personal data. The Government is also charged with determining how to apply the law regarding the protection of data by communication and information services using telecommunications, and defining, among other things, the tasks of the Internet service providers.

The Italian Parliament has recently approved a new law[30] which includes provisions against the sexual exploitation of minors and introduces new articles in the penal code.[31]

The Italian Minister of Communications has initiated an informal project with the goal of producing a code of conduct for service providers on telecommunication networks. The basic principles of the code for this Internet Code of Self-Regulation are as follows:

1. The provisions of the code are founded on the characteristics (global expansion, interactivity and flexibility) which distinguish the Internet from other tools of communication and are closely linked to the evolution of these characteristics over time.

2. The Code has two fundamental principles: freedom of expression and protection of the individual.

3. The Code's objectives are the creation of an environment for development and economic, social and cultural growth; and the prevention of all kinds of illegal or harmful communication and information.

4. The Internet Code of Self-Regulation complies with national EU norms, as well as with international treaties, and should be interpreted in accordance with these norms.

5. Liability on the Internet is personal in nature and is not closely linked to the institutional role of the subject but to what may be broadcast at any given moment on the network.

6. The Code of Self-Regulation was put in place by operators and users and is designed for them. Compliance is voluntary and involves observance of the principles, obligations and recommendations of these bodies by the compiler.

7. The Code deals with the creation and operation of the bodies necessary for its implementation and the settling of law suits on the application of the rules. The bodies are made up of experts in the technical and legal fields relating to the network.

On the question of the civil liability of the owners of public communication channels, case law exists in Italy concerning online magazines, which are considered to meet the criteria necessary for their inclusion on the press register and establishing them as media. Italian law also establishes the existence of online magazines noting them on the register which will be held by the new Authority for the Guarantee of Communications. This integration of information providers operating on the Internet and bodies of the traditional press leads to particular objective responsibilities with respect to broadcast content.

In the Italian Government's view, the efficient prevention of the improper use of the Internet -- especially for youngsters -- is possible through the adoption of literacy and training policies and by opening up the possibility for everyone to use the network. To achieve this goal, a Forum for the Information Society has been created under the auspices of the Presidency of the Council. It has a sub-group devoted to the Internet which has established a direct and constant relationship with the operators of the network and with associations of users and consumers.

The Minister of Communications has taken measures to reduce by approximately 50% the price of telephone communications for access to the Internet. Furthermore, a programme has been initiated directed particularly at schools to enable all students to have access to the use of new technologies not only passively but also in an interactive way.

Finally, the first conference of European Internet Access Providers Associations to tackle the general problems of the Internet and, in particular, the content and self-regulation of the network, took place in Naples in October 1997.

There is an effort by the Parliament to gradually upgrade Italian laws. A number of initiatives are under way to examine the need for laws specifically to address sexual exploitation of minors in the Internet context.[32]

Japan

The National Police Agency (NPA) of Japan formed a study group to examine issues related to indecent information which is harmful to youth on computer networks, including the Internet and proposed solutions as to how to deal with such information. The NPA maintains that provisions in current criminal laws in terms of public indecency apply to information on the network.

The Japanese Ministry of Justice formed the Study Group for the Legal System on Electronic Commerce in July 1996 to investigate a variety of issues in the context of electronic commerce. This Study Group examines the following items from the view point of civil law and commercial law: the necessity of legal arrangements on electronic commerce; an authentication system which is able to prove

identification of correspondents in transactions and applicants; and a system which authenticates the contents of electronic documents and their integrity. In connection with the development of an infrastructure to support electronic authentication techniques, the study group also considers: technology on cryptography underlying electronic authentication; the content held on the system; and the necessity of legal arrangements for the system.

To address issues related to the flow of illegal and harmful information on the Internet, the Japanese Ministry of Posts and Telecommunications[33] (MPT) formed the Study Group for the Advancement of the Condition for the Use of Telecommunications in September 1996 which published a report in December of the same year. The report was based on the premise that current criminal and civil laws and regulations apply to the flow of information on the Internet. It notes that from the viewpoint of protecting freedom of expression, any new legal restrictions would have to be considered very carefully. The report recommended that, for the time being, the only action to be taken should be: 1) the formation of guidelines by Internet service providers; and 2) the rating of illegal and harmful information, and promotion of the development of filtering systems which block information with certain ratings. In accordance with this report, an association of telecommunications carriers which provide Internet access services are currently working on the development of policy guidelines; and, in conjunction with educational institutions and local authorities in model areas, the MPT is conducting research and development in the technology for filtering and rating harmful information on the Internet from the receiver's standpoint. In practice, this research and development concentrates on: 1) technology to support content rating; and 2) technology for co-operative and effective utilisation of dispersed rating information.

Whereas MPT considers encryption and electronic certification to be integral to the issues at hand, the MPT set up the Survey Study Group Concerning Electronic Information and Network Usage (August 1995), and the Study Group Concerning Electronic Payment, and Electronic Money (April 1996), and is continuing to examine these issues. Since October 1996, these efforts have been supplemented by the Study Group on Electronic Certification over Networks, which is examining the appropriate form of certification authorities and certification work over networks, to provide effective means to prevent data falsification or impersonation in the context of electronic commercial transactions over open information and communications networks. In addition, the Telecommunications Council, an advisory body to the MPT, included in its interim report *Info-communications 21st Century Vision* (April 1997) the need to take action with regard to new social problems that can occur as the information and communications networks become more advanced, and proposed: 1) self-regulated guidelines by providers; 2) technological measures; and 3) the need for provisions for handling customer complaints and queries.

The Japanese Ministry of International Trade and Industry[34] (MITI) has focused much of its attention on supporting the activities of the Electronic Network Consortium (ENC).[35] The ENC comprises more than 90 organisations including major online service providers and promotes the provision and dissemination of blocking capabilities available to Internet users. In September 1997, the ENC developed a filtering system in accordance with the PICS platform as specified by W3C.[36] The software can be downloaded free of charge from the homepage of the New Media Development Association[37] (NMDA) which was formed by network and computer industries. On the basis of the internationally accepted rating system RSACi, more than 13 000 Japanese Web pages have been rated, covering many of the most harmful Web pages in Japan. The filtering software has been downloaded by several thousand organisations, including educational institutions and private companies. The ENC has also provided this software for the schools engaged in the "one-hundred-school networking project", which is a project implemented by MITI and the Ministry of Education (MOE) to provide a networking environment for 100 elementary, junior-high, and high schools throughout Japan. In February 1996, ENC published the first voluntary codes of conduct in Japan, *General Ethical Guideline for Running Online Services* and *Recommended Etiquette for Online Service Users*[38].

MITI has also worked to strengthen the Consumer Advice Office to equip that office to effectively address the complaints of consumers about Internet content issues. In that context, MITI and the Economic Planning Agency have co-organised the "liaison council on consumer issues in the use of information technology and electronic commerce", for exchanging information on problems and coping with complaints. Finally, MITI has worked to strengthen co-operation with other ministries and agencies, including the Management and Co-ordination Agency (youth policy), the Ministry of Education (providing filtering software to schools) and the National Police Agency (providing information).

Korea

The Korean Government believes that industry self-regulation is the best approach to address Internet-related issues. Korea generally applies the current laws of the criminal and civil codes to the Internet. Korea believes that technological solutions are also an effective method to address some of these issues, and the Government is promoting more advanced and user-friendly forms of software that help parents control illegal and harmful information and is currently studying an Internet content rating system.

The Korea Information Communications Ethics Committee (ICEC) was established in April 1995 to help prevent the distribution of illegal and harmful materials via electronic media and to promote a safe information environment. The ICEC consists of 13 civil representatives from various professions and fields, who are appointed by the Minister of Information and Communication. The ICEC has undertaken a broad range of activities, including: setting out a code of ethics for service providers (including ISPs); operating a hotline for handling suggestions and reports from the public; reviewing online information content that is distributed for the purpose of public use; requesting ISPs to block illegal and harmful materials; and promoting a desirable information culture.

Korea ISPs are currently operating hotlines and have formed the Consultation Committee for Information Ethics of ISPs as part of the ICEC to develop appropriate measures for regulating the distribution of illegal and harmful materials. They are also working with the ICEC to promote the safe use of the Internet.

Luxembourg

Luxembourg has no special laws specifically concerned with illegal/harmful content on the Internet. The issue is therefore addressed by the existing general laws. However, it is recognised that amendments to existing legislation may be required to adapt these laws to the electronic environment.

The Luxembourg Government acknowledges that international co-operation is necessary due to the transborder nature of these activities.

Mexico

The enhanced services sector in Mexico has been fully liberalised and there are currently 96 Internet service providers based in Mexico. The governmental entities in Mexico charged with overseeing the technical issues related to the provision of Internet services are the Ministry of Communications and Transport *(Secretaría de Comunicaciones y Transportes)* and the Federal Telecommunications Commission *(Comisión Federal de Telecomunicaciones)*. The Ministry of Trade and Industrial Promotion *(Secretaría de Comercio y Fomento Industrial)* is responsible for market access issues. In addition, the Ministry of Finance and Public Credit *(Secretaría de Hacienda y Crédito Público)* is responsible for the financial, customs and taxation issues involved.

The Mexican Government supports the free flow of information across its borders. However, the Government recognises that some national legislation may not be adapted to the Internet environment, and it is, therefore, assessing the need for any legislative changes that may be necessary to make such rules and regulations applicable online. The Mexican Government acknowledges that, due to the international nature of this problem, international co-operation in this area is necessary.

Netherlands

In the Netherlands the issues related to Internet content are considered within the context of the concept that freedom of expression is a constitutional right that should be respected. Nevertheless, in the Netherlands, the distribution of any materials containing sexual conduct involving minors (15 years of age or younger) is punishable by laws intended to protect minors from becoming involved in the production of (child) pornography. Offering harmful materials (including images of violence) to minors is a punishable offence as well. There are, however, no legal limitations for adults who publish their own private information (*i.e.* the government does not censor information for consumption by adults). This leads to the question of what actions have been taken, to date, in the Netherlands to combat illegal and harmful content on the Internet. The Netherlands recognises the major social and economic potential of global information networks and the Government believes that in order to fully benefit from this potential, an environment must be created to combat excesses, including the distribution of illegal and harmful content or other indecent behaviour.

The Government of the Netherlands generally favours self-regulation for Internet content issues and a number of steps have been taken both by industry alone and by industry working in close co-operation with the Government. In 1996, a hotline to help fight child pornography was established, followed by a similar hotline to combat racism. Internet providers found to be disseminating illegal or harmful content will receive first a warning to remove this material and, if they do not respond, legal action will be taken. The initial experiences of the child pornography hotline within the Netherlands have been positive; however, following up on incident reports involving providers outside the country has been difficult.

Problems related to Internet content are high on the political agenda in the Netherlands. Within the framework of the National Action Programme for the Electronic Highway, a project has been launched to look into the legislative aspects related to these issues. Technical and social developments in the areas of information and telecommunications lead to several relevant questions, which this project will address:

- Is governmental action possible and useful?
- In what cases is action desirable?
- What instruments to support this action should be implemented?

On 29 May 1997, the Dutch Parliament approved a policy paper, “Not for All Ages”, concerned with protecting minors from harmful and illegal audio-visual media, including film and video, as well as multimedia and television. The principal concept contained in the paper is that every medium product or programme is the responsibility of the industry which brings it to the market. Such content should be classified according to the specific industry criteria in order to avoid possible harm to youth. In the Netherlands, age classification and product marketing are to be based on harmonised norms and criteria. A national institute, founded by the media business and partly subsidised by the Government, but statutorily independent, will be responsible for developing, maintaining and safeguarding these norms. The

establishment of a hotline and ongoing evaluations are intended to help maintain the integrity of this approach.

Self-regulation in the Netherlands is based on industry-developed codes which include sanctions. In addition, certain Dutch laws will be revised in order to implement the European Directive Television without Borders; for example, the Media Law will be tightened and Article 20a of the Criminal Code will be expanded, strengthened and aimed at businesses that are not, or have no intention to be, a part of the self-regulating system.

New Zealand

The New Zealand approach to controlling content on the Internet is consistent with its objective of not reducing the usefulness of the Internet to the majority of New Zealanders. New Zealand Internet service providers (ISPs) were therefore encouraged to develop an industry code of practice[39] which has been implemented by all leading ISPs in the country. All ISPs party to the code of practice must inform their subscribers of their obligations under the code.

In New Zealand, content distributed on the Internet is not regulated specifically, but is subject to existing New Zealand legislation. In particular, publishing objectionable content on the Internet is against the law in New Zealand under the Films Videos and Publications Classification Act 1993. There have already been several successful prosecutions of New Zealanders for using the Internet to distribute objectionable material. The law does not distinguish between the Internet and other media when it comes to the publication of objectionable material.

Norway

The Norwegian approach to Internet content issues is based on the premise that dissemination of information on data and telecommunications networks should, as far as possible, be subject to the same standards as traditional information, and that rules that apply off-line should also apply in the online environment. However, monitoring the Internet and law enforcement may pose problems. Norway believes that the general provisions in the national legislation are applicable to content on that is under Norwegian jurisdiction. It is however recognised that certain regulations are not adapted to the swift technical developments of the Internet environment. Distribution of illegal content over data and telecommunication networks from Norway databases is covered by the provisions of the Norwegian Penal Code. For example, according to the Norwegian Penal Code, it is illegal to distribute pornography from Norwegian sites.

The Norwegian Government's campaign to combat violence in the visual media, which has been active for more than two years, includes information activities on publicly available networks. The campaign focuses on co-operation between government authorities, business, industry, organisations and the public at large. As part of this campaign, the National Criminal Investigation Agency (Kripos) receives information from an international hotline run by Save the Children Norway that monitors the Internet in order to reveal illegal content, and exchanges information with law enforcement agencies in other countries.

It is illegal not only to distribute, but also to download child pornography from foreign sites. The Norwegian Penal Code prohibits the possession of such material. The distribution of materials depicting gross violence are also prohibited under the Penal Code (amended May 1998).

It is the opinion of the Norwegian Government that suitable and updated national legislation must be the basis for controlling controversial content and conduct on the global networks. Norway also believes that due to the international nature of the online environment and Internet content issues in particular, international co-operation in this area is necessary and should be developed gradually.

Industry self-regulatory initiatives

The Internet service providers in Norway have established a group called "Internettforum", for promoting the Internet, suggesting codes of conduct, giving advice on legal issues in the Internet field, and discussing liability and responsibility questions. The forum is a subsidiary of the Norwegian Office Machine and Equipment Dealers' Association *(Kontor- og datateknisk landsforening)*.

Recently an Internet ethics council *(Internett etisk rld)* was established by the IT-providers association. Representatives from industry, Internet service providers, access and content providers and legal experts are members of the council. It will be an advisory council working in a way similar to the ethical council of the Norwegian press and media *(Pressens faglige utvalg)*.

The Ombudsman for Children in Norway initiative

The Ombudsman for Children in Norway *(Barneombudet)* has initiated a project called "Child Porn on Internet" in co-operation with Save the Children Norway *(Reed Barna Norge)* to set up an international hotline. The project was initiated in May 1996, and the first reports from the project were presented to a workshop at the UN Ministerial Conference in Stockholm entitled "Commercial sexual exploitation of the child" in August 1996. An international campaign to combat paedophilia on the Internet and the distribution of child pornography on the Internet is part of this project.[40]

Save the Children Norway runs the international hotline on the Internet (children@risk.sn.no) and co-operates with national hotlines, *e.g.* Internet Watch Foundation in the United Kingdom. Substantiated information will be passed on to the Norwegian police, who gather and forward information on illegal content in other countries to relevant authorities.

The work of Save the Children Norway is focused solely on the protection of children. The organisation regards the Internet in a positive manner, recognises the importance of preserving the free flow of information, and is not concerned with material intended for adults. According to Save the Children Norway the amount of child pornography available on the Internet is considerable. The organisation's experiences using the Internet to build an international network to help combat child pornography on line has been positive and it has received positive feedback from the majority of Internet users. During 1997 about 2 100 tips were received on content traders, Web pages and news groups distributing illegal content.

In November 1997 a Nordic meeting of police authorities and Internet access providers was held to discuss further co-operation in this area. The Norwegian Ombudsman for Children suggested that the Internet service providers establish a Scandinavian "Net-nanny", a special branded access for children, containing white-listed Web sites. This kind of service should be set up by the industry. The proposal will be followed up by the Nordic Ministerial Council.

The Ombudsman for Children has proposed to establish a national hotline in Norway as part of the Norwegian Government's campaign to combat violence in the visual media. In addition, during January and February of 1999 Norway will host an international workshop on Children and Media in co-operation with UNICEF, UNESCO and WHO.

Poland

Poland does not currently have a national initiative to study harmful or illegal content on the Internet. It is, however, recognised that some legislative changes will be necessary in the process of accession to the EU in order to conform Polish law with the law of the EU.

Portugal

In the context of the legal framework applicable to Internet communications, the Portuguese national legislator has concentrated its efforts on technological and economic issues. The most effective contribution to better protection of privacy, intellectual property rights, of human dignity and economic security (for example, from fraud and credit card piracy) is seen as the delineation of the responsibilities and of the terms and conditions of access to the network. In this regard, relevant Portuguese laws include the Constitution of Portugal (which guarantees a right of access to computer networks of public use), Law No. 28/94 of 29 August on personal data protection and Law No. 109/91 of 17 August relating to computer crimes.

Portugal has closely examined the documents produced within the European Union framework relevant to the control of Internet content. The Government of Portugal considers that the position taken by EU institutions, based on industry self-regulation, the introduction of filtering devices, content rating, greater user awareness of the advantages and disadvantages of the Internet, and the different judicial treatment of illegal and harmful content, will be of assistance in the further development of Portuguese legislation.

Spain

Article 20 of the Spanish Constitution establishes the right to freely express and disseminate personal opinions, irrespective of the medium used.

The limitations to that right, in particular crimes relating to illegal/harmful content on the Internet, are currently addressed by existing legislation. For example:

- The recent Penal Code (Organic Law 10/1995) covers all kinds of crime, including some specifically related to electronic media (*e.g.* electronic mail (Article 197) and intellectual property rights (Article 250)).

- The Privacy Law in force since 1992.

- Intellectual property rights are also covered in the electronic media (Intellectual Property Law, 12 April 1996).

- Some of the administrative procedures which are applied to media operating in the physical world also apply, or gave been amended to apply, to electronic media; for example, registration procedures for electronic publications.

Although there is no clear evidence that major new specific laws are required in this area, in the future, minor legislative changes and the updating of regulations in very specific domains and self-regulatory instruments will probably be needed. There is a broad perception in Spain that close international legal and jurisdictional co-operation is needed due to the transborder nature of these activities.

Sweden

On 19 June 1997, the Swedish Government decided to ask for the Law Council's opinion on a draft legislation on electronic mediation services. According to the proposal, the supplier of a service has an obligation to prevent distribution of a message if it is obvious that the content of the message is such as is described in certain enumerated provisions of the Swedish Penal Code, for example, the provision on incitement to criminal acts, persecution of a population group, child pornography and unlawful representation of violence). A supplier can be held liable if it is obvious that a user, by posting the message, has made himself guilty of an infringement of the copyright legislation.

In order to fulfil his obligations, the supplier must supervise his service. However, the supplier is in general not expected to exercise prior control of the content of all messages sent to the service before the messages are put into circulation, but simply to inspect the content of his services regularly. If the number of messages make such an inspection difficult, other supervisory methods, such as the possibility for users to inform the supplier of illegal messages via hotlines is sufficient. The proposed legislation also contains an obligation for the supplier to inform the users of the service of his identity and to what extent incoming messages become available to others. There are some important exceptions to the scope of the proposed law. The law does not apply to network operators, the mediation of messages within a Government agency or between agencies or within an enterprise or a legal group of enterprises or services that are protected by the Freedom of the Press Act or the Fundamental Law on Freedom of Expression. Furthermore, the law is not applicable to e-mail.

According to the proposal, the supplier is responsible for a violation of the obligation to prevent distribution of a message if the violation is committed intentionally as well as for acts of gross negligence. A bill may be presented to Parliament in early autumn and the law is proposed to come into force in April 1998. In the proposal, the Swedish Government underlines the importance of self-regulatory mechanisms, such as codes of conduct, hotlines and the availability of systems for rating and filtering content. The Swedish branch of the international Internet organisation ISOC has begun work in this field.

The Government Committee on Media has presented a proposal intended to guarantee freedom of expression in new media. The Committee's view is that the Internet in itself is not a medium, but a system that makes different forms of computer communications possible. The Committee underlines the importance of protecting the freedom of expression when it is exercised on the Internet as well as on other networks or media. Some of the applications of the Internet are currently covered by the far-reaching rules of protection in the Swedish Constitution; however, the Committee proposed that this area should be widened.

Switzerland

The Swiss approach to Internet content issues is based on a broad overview study on penal, data protection and copyright aspects of the Internet completed in May 1996 by an interdepartmental working party of the Federal Office of Justice.[41] The report aims to help prevent illegal abuses of data networks and makes a number of recommendations aimed at Internet access providers in support of their efforts to draft a code of ethics. The basic principles set forth in the report are outlined below.

If the provider has first-hand knowledge of or is given concrete information by third parties that gives grounds for suspicion that certain network content could be unlawful, the provider should immediately conduct or commission investigations with a view to suspending this content, as necessary. If the provider has certain knowledge of unlawful network content, and in particular of content which is punishable by law, the provider should immediately take the technical measures that are feasible and

reasonable to suspend access to this content. This should also be done when the provider is aware that particular network content constitutes an infringement of copyright or industrial property rights. The provider should draw attention in the service contract to the customer's obligation to respect copyright and industrial property rights and should reserve the right to temporarily suspend a site suspected of infringement and unilaterally terminate the contract in the event of infringement.

It is recommended that access providers set up a "focal point" to collect and analyse information from providers, their customers and third parties about unlawful network content. This focal point should function as a service and information "hub", offering affiliated providers up-to-date information about network content which is to be suspended as well as professional and technical support.

It is recommended that the provider should, in principle, conclude service agreements only with private individuals who have sound judgement and are of age. Furthermore, customers should be granted access to the network solely through user identification and a password (pin code). In the service contract, the provider should reserve the right to suspend a "suspicious" site temporarily and to terminate the contract unilaterally if the customer disseminates unlawful content from a site or if such content can be called up from that site. The service contract should explicitly invite the customer to report any unlawful network content and any other unlawful Internet applications of which he or she becomes aware directly to the provider and/or to the focal point.

Providers should be aware that displays of violence punishable under the terms of the Swiss Penal Code are not confined to film or photographic presentations but may also be contained in other articles or presentations (for example in computer games) and that promoting or placing on offer displays of violence is also a punishable offence. The same applies to presentations of hard-core pornography.

The provider should brief his customers adequately on the potential data protection hazards involved in using the Internet and taking advantage of its services. He should also draw their attention to measures and products for ensuring the confidentiality, accuracy and availability of personal data (*e.g.* coding and encryption techniques). The provider should process only the personal customer data required for providing his services. Technical and organisational measures should be taken to ensure that the data processed are made available only to staff requiring them to do their work. The data should not be used for any purpose other than that cited on obtaining the data, that which is obvious from the circumstances or is prescribed by Swiss law. Data may only be made available to third parties with the customer's consent or if the provider has a qualified obligation to make the data known. The provider should not draw up personal profiles of customers and should not make their names, addresses and telephone numbers accessible via the Internet, unless the person involved has given his consent, unless there is a legal justification for doing so or an overriding public or private interest is involved.

Turkey

The Turkish Ministry of Transport established the country's Internet infrastructure on a revenue-share basis. Today, there are about 100 Internet service providers (ISPs) which, in Turkey are also responsible for content. Internet content is subject to the same regulations and laws as the off-line world. It is also the ISP's responsibility to take precautions against the infringements of copyright or industrial property and patent rights.

In January 1998, the Ministry of Transport formed the Internet Higher Council, comprised of representatives from the public sector, private sector (ISPs), users, experts, and non-governmental organisations (NGOs). The Internet Higher Council will advise the Ministry on technical and content issues.

In 1997, a law proposal on Protection of Personal Data was prepared and is currently before Parliament.

United Kingdom

In the United Kingdom, existing law applies to the electronic online environment in the same way as it does off-line. This has in some cases required some updating of existing law: for example, the Obscene Publications Act 1956 was amended in 1994 so that "publication" now explicitly includes the transmission of electronically stored information. In addition, the Protection of Children Act 1978, which contains provisions against child pornography, was similarly amended to apply to computer-generated "pseudo-photographs". Most law in the United Kingdom, however, is technology neutral. Existing national law is thus applicable to content and activities across all media, which is fundamental for ensuring that technological developments do not outstrip the law's capacity to regulate them. The Internet does, however, present new issues of enforcement and responsibility, not least because of its inherently global nature.

The UK Government, police and Internet industry began discussions in September 1996, with a view to developing a framework for dealing with these issues. The result is the industry-led and funded Internet Watch Foundation (IWF) framework. The framework was put forward by the two leading trade associations in the United Kingdom, the Internet Service Providers Association (ISPA) and the London Internet Exchange (LINX), with the support of the UK Government and the police, and facilitated by the Department of Trade and Industry (DTI).

Under existing UK law, Internet service providers have a clear liability for illegal material hosted on their servers, once they are informed of its existence. In effect, once alerted to illegal material or activity on their servers, ISPs will be liable as accessories if they fail to take reasonable steps to deal with it. What is reasonable is defined as industry practice as exemplified by the IWF model. Internet Watch therefore offers ISPs a service, facilitating their compliance with existing law and any ISP declining to take action once informed of the existence of illegal material on his servers would risk prosecution.

Under the IWF framework, ISPs take responsibility for the removal from their servers of material which is notified to them as being illegal in the United Kingdom. A reporting hotline (via e-mail, fax and telephone) has been set up through which Internet users may report instances of material which they believe may be illegal. Action varies according to the source of the material. In the case of newsgroup articles, which make up the vast majority of the material reported, IWF distributes details simultaneously to all subscribing ISPs, who then remove the material from their individual news feeds; this is done regardless of the origin of the offending message. In the case of material contained in a UK-hosted Web site, IWF will inform the ISP hosting that Web site, who will take steps to have the material removed. Of the small proportion of articles originating in the United Kingdom, details have been passed to the police for enforcement action against the originator. Thus the originator remains responsible for content; the police remain responsible for enforcement. In the case of illegal material hosted on a non-UK server, IWF currently simply passes details to the National Criminal Intelligence Service (NCIS - the body responsible for liaison between UK police forces and their international counterparts). NCIS then passes the information to the appropriate foreign authority. It is envisaged however that IWF will develop its own direct links to other national self-regulatory bodies, which will facilitate the exchange of information.

A key aspect of IWF is that it ensures that users retain responsibility for material which they post on the Internet. To this end, a further part of IWF's remit is to address the possible abuse of anonymity. Provision of an Internet pseudonym is not in and of itself a danger, and anonymity can serve a useful purpose in a number of contexts. The difficulty only comes if this service is abused, if the pseudonym is

actually untraceable and this anonymity is used to commit crimes. Under the IWF framework, UK ISPs are therefore working on proposals to maintain "audit trails", so that the real identity of the user can be traced, in the event that the police can show that they need this information in the investigation of a crime.

The second part of IWF's remit relates to material which, while it is not illegal, may be harmful to minors, or found offensive. The United Kingdom believes that rating systems and filtering/screening software must play a key role here. Such tools allow users to tailor their, or their childrens', experience of the Internet to their own personal standards, without denying access to legal material to those who wish it, and therefore without harm to the Internet's traditions of free speech. The IWF was therefore charged with developing a rating system for legal content suitable for application in the United Kingdom. An advisory board was convened in early 1997 comprising representatives of children's charities, educators, and consumers' and civil liberties groups, with the aim of recommending a suitable system. The IWF is also working on ways of ensuring the take-up and use of ratings, for example by pre-installing the necessary software on PCs, and by creating off-the-shelf profiles to make filtering more user friendly for those with little computer knowledge, for example based on the approximate standard of a PG film (parental guidance - for general viewing but some scenes may be unsuitable for small children), or the pre-9pm watershed on UK television.

IWF had originally intended to concentrate first on UK action. Their experience so far has shown, however, that the vast majority of the illegal material reported to them appears to have originated outside the United Kingdom, and they have therefore begun to look at international co-operation as a priority. IWF has developed a proposal for international co-operation between self-regulatory bodies, which includes measures to improve international co-ordination in dealing with illegal material, develop sampling software to facilitate the tracking down of illegal material, and develop a set of standard factual ratings which could be drawn on by any group wishing to use filtering technology.

Non-governmental initiatives in the United Kingdom

Within the United Kingdom, R3 Safety-Net is an industry proposal for addressing the question of illegal material on the Internet with particular reference to child pornography. It presents a package of measures developed by key players from the ISPA, LINX and the IWF. The proposal was developed in discussions facilitated by DTI between service providers, the Metropolitan Police and the Home Office. The immediate and particular focus of these proposals is to help eliminate child pornography on the Internet, though the approach may also be applicable in the future to other types of illegal material available on the Internet.

The Safety-Net proposal is based upon a number of simple principles. In general, the law applies to activities on the Internet as it does to activities not on the Internet. The issue addressed has nothing to do with censorship of legal material or free speech; the core issue is crime and how to deal with material or activity which society, through democratic process, has deemed to be unacceptable in law. Legal, but possibly offensive, material raises a quite separate issue. Service providers must take a responsible approach to the provision of services by implementing reasonable, practicable and proportionate measures to hinder the use of the Internet for illegal purposes, and to provide a response mechanism in cases where illegal material or activity is identified. Service providers should not be asked to take responsibility for enforcement of the law. End users should retain responsibility for the content they place on the Internet, whether legal, or illegal and the Police should retain responsibility for law enforcement. By taking appropriate measures, across the industry, service providers can offer protection to the end user and to themselves. The law that determines what material or activity is illegal is the law of the country in which the consumer is affected by it.

The approach establishes an independent foundation to support the adoption, by Internet service providers and users, of responsible policies based on rating and reporting of illegal material. It gives priority in the first instance to child pornography, but may also be applicable to other forms of illegal material in the future. The approach also supports the rating of legal material so that users can tailor the nature of their experience on the Internet, according to their own standards.

The IWF has been established to implement the Safety-Net Agreement, and offers itself to fulfil an independent role in receiving and processing complaints about child pornography (and other illegal material) on the Internet and to support the development of rating systems. The Foundation will also sponsor research and development into ways of improving the detection, traceability and removal of illegal material on the Internet. The IWF takes responsibility for establishing a rating and reporting service for illegal material. This has to be complemented by responsibility on the part of users for the material they place on the Internet and by responsible service provider policies in order to have the desired effect. In particular, policies on the rating of material by users, on removal of child pornography and on tracing the originators of illegal material are required. These issues are of greatest urgency in relation to Web pages and Usenet news groups. Other policies may need to be developed and extended over time.

United States

The United States considers the Internet an increasingly critical medium of information sharing, commerce, education, entertainment and communication, with both unique and emerging capabilities, and strongly supports the global expansion of Internet-based services. The private sector has played the leading role in the expansion of Internet-based services and the Clinton Administration believes that market forces should continue to drive Internet developments. Governments should refrain from imposing unnecessary, inappropriate or burdensome restrictions on the provision and use of Internet-based services, as such regulations distort the further expansion of such services. Where government involvement is deemed necessary and appropriate, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for the provision of Internet based services. Moreover, existing laws and regulations should be reviewed and amended or eliminated where they may hinder the further expansion of Internet-based services. In applying any existing laws or regulations, it is necessary to analyse whether the policies underlying the relevant law will be furthered by applying the law to the Internet.[42]

The starting point for understanding US regulation of content on the Internet (or elsewhere) is the First Amendment to the US Constitution. That amendment explicitly protects freedom of expression, and establishes a general presumption that neither the US government nor the governments of its states may criminalise or burden speech on the basis of content. Over the years, US courts have crafted a large, complex body of law interpreting the free speech protections of the First Amendment, including the establishment of exceptions that allow limited regulation of speech.

US courts apply three levels of tests to determine whether speech can be regulated. The "strict scrutiny" test, applicable to restrictions that are clearly based on the content of speech, allows speech to be regulated if necessary to serve a "compelling state interest", if the regulation is "narrowly drawn to achieve that end." Government must generally employ the "least restrictive means" of regulating. Under the "intermediate" test, applicable to content-neutral regulations affecting speech, a regulation must be "narrowly tailored to serve a significant governmental interest and not burden substantially more speech than necessary to remedy the condition the government identified as needing correction". A third test, the "rational basis" test, applies to regulation that does not directly implicate speech, such as economic regulation that affects a broad group.

In the United States, direct content regulation traditionally falls into five classes: advocacy of unlawful conduct, obscenity, threatening and offensive language, invasions of reputation and privacy, and commercial speech. Otherwise, US courts allow some content-neutral restrictions on the "time, place, and manner" of the speech, and some regulation of "public fora". Speech restrictions must also meet various legal requirements; *e.g.* they may not be excessively vague or overbroad. Major categories of content found online that receive no or limited First Amendment protection include: obscenity, "harmful to minors" material, threats of harm and harassing communications, child pornography, enticement of minors to engage in prostitution or other illegal sexual activity, and fraudulent statements for the purpose of obtaining money or property from another. Commercial speech (*e.g.* advertising) receives First Amendment protection, but may be subject to various regulatory requirements. For example, advertising relating to pharmaceutical products, securities, or professional legal services is regulated by agencies at the state or federal level.[43] Untruthful commercial speech, however, is not protected by the First Amendment. The Federal Trade Commission Act prohibits deceptive or unfair commercial conduct, including false or unfair advertising. Advertising is also regulated at the state level by the individual state's attorneys general and consumer protection agencies, as well as through public and private enforcement of consumer protection, unfair competition, and deceptive trade practices statutes. The essential purpose of the regulation of advertising is to ensure fair competition and to protect consumers from false claims and representations. Note that pure "hate speech" -- expression that disparages a person or group on the basis of race, religion, ethnicity, etc. -- receives full First Amendment protection and may not by itself be made the object of criminal sanctions, according to the US Supreme Court.

In addition, US courts apply different levels of scrutiny to different communications media. Because of the unique characteristics of each medium, the same standards are not applied to the print media, broadcasting, cable television, direct broadcast satellites, common carriers, information service providers, and Internet service providers. For example, because of the scarcity of radio spectrum, broadcasters are considered public trustees, and US laws require them to air programming that serves the public interest. In contrast, the government cannot compel newspapers and magazines to provide such content. Restrictions on "indecent" speech -- a category of sexual-related speech considered less objectionable than "obscene" speech -- are illustrative. While obscene speech can be restricted in any medium, indecent speech is allowed in some media but not others.

Although information privacy is not an unlimited or absolute right, concerns about the misuse of personal information have been reflected in a diverse set of laws and regulations to protect privacy. While there is no single statute or regulation that governs the collection, communication, and use of all types of information about individuals, the United States has a sectoral approach to privacy protection that relies on a mixture of legislation, regulation, and private sector self-regulation (such as codes of conduct and corporate policies). Federal law regulates the government's collection, use, and distribution of a significant amount of personal information. In addition, it is generally against the law to intercept the content of any communication without consent or specific authority. The 1996 Telecommunications Act extends comprehensive protection to transactional data held by common carriers. Many online service providers and Internet access providers contract with subscribers to provide privacy protection.

As the widespread public use of the Internet is a relatively recent phenomenon, case law applicable to First Amendment rights on the Internet is limited. In a recent decision striking down key provisions of the Communications Decency Act of 1996, a US law that regulated online obscenity and indecency, the US Supreme Court allowed obscenity restrictions to remain in place, but declared the Act's restrictions on indecent communications unconstitutional. The Court's decision does not convert the Internet into a no-law zone, however. On the contrary, many types of expression that may be regulated in the physical world -- such as threats, obscenity, and the other classes of speech discussed above -- may also be regulated on the Internet.

On 16 July 1997, President Clinton convened a meeting of industry, parent and teacher organisations, and government representatives to work together to create a family-friendly Internet without abridging the constitutional guarantees of free speech and free expression. The Administration's plan calls for: (1) the provision of easy-to-use blocking, filtering and labelling technology for parents and teachers by the Internet industry; (2) the enforcement of existing laws that protect children online by the Administration; and (3) greater involvement by parents and educators in the use of the Internet by children.

Non-governmental initiatives in the United States

The not-for-profit sector in the United States has been active in promoting the benefits of technology in schools and homes. The following information is representative of the resources currently available for parents and teachers in the United States.

- American Association of School Administrators <http://www.aasa.org>
- American Library Association <http://www.ala.org>
- Centre for Children and Technology <http://www.edc.org/CCT/ccthome>
- The Centre for Democracy and Technology <http://websites.cdt.org>
- Centre for Media Education <http://www.cme.org/cme>
- Centre for Media Literacy <http://www.medialit.org>
- The Children's Partnership <kidspartner@earthlink.net>
- Community Technology Centres' Network <http://www.edc.org>
- The Electronic Frontier Foundation <http://www.eff.org>
- KIDSNET < kidsnet@aol.com>
- National Association of Elementary School Principals <http://www.naesp.org>
- National Association of Secondary School Principals <http://www.nassp.org>
- National Centre for Missing and Exploited Children <http://www.missingkids.org>
- National PTA <http://www.pta.org>
- National School Boards Association <http://www.nsba.org/itte>
- National Urban League <http://www.nul.org>
- The Online Public Education Network (Project OPEN) <http://www.isa.net/project-open>

B. Private sector approaches

Some of the most important initiatives currently under way in this area are coming from the private sector. The business community is working both on its own and in conjunction with the public sector to develop solutions to address these issues, including technological solutions, self-regulatory measures, and contractual agreements. Additionally, a number of non-governmental organisations are studying the issues and helping to facilitate education, training and promotion of ethical behaviour among individual and business Internet users. The following inventory of private-sector initiatives currently under way at the national and international level outlines the major private-sector efforts in this area.

Labelling Systems

Platform for Internet content selection[44]

The Platform for Internet Content Selection (PICS) represents an industry-wide response to attempts to regulate content on the Internet. PICS was developed by the World Wide Web Consortium (W3C).[45] PICS is a set of open technical standards for creating filtering software and rating systems for Internet content. It specifies how to create rating labels for Internet content. These labels can indicate specific aspects of content, such as indications of offensive language, sexual content and the level of violence. Rating services determine the substance of the labels by setting the criteria. PICS provides for both self-labelling (by the author or publisher) and third party labelling. PICS is "values neutral" in the sense that it does not specify the content of labels, simply their format and how they can be transmitted. PICS flexibility allows a single Web site to have multiple labels applied by different rating systems. Users are free to choose which rating services to install on their computer. They can also choose whether to block access to content that has no label at all, or to override the block after viewing the material.

As the use of the Internet and the awareness of filtering technology grows, it is likely that consumers will demand more content rating, and incentives to develop PICS-based solutions will increase. Users will have a growing variety of rating services from which to choose, and will be able to select those that most closely reflect their own values. PICS is neutral in that it provides the technical framework for the implementation of ratings systems. PICS is not censorship and does not judge content in any way. PICS is flexible in that it is multi-dimensional, allowing an unlimited number of rating systems, adaptable to any cultural or social values, to be created on the basis of PICS. PICS is family-centred in that it empowers parents to perform their parental role in the Internet environment to decide what material is appropriate for youth.

A number of companies offer products that implement the PICS standard. Rating services have been developed by RSAC[46] and SafeSurf to work within the PICS platform. Microsoft has integrated the filtering software in its Web browser Internet Explorer 3.0.[47]

Rating systems

A number of independent rating systems have been developed which can operate using the PICS platform for content filtering. The various systems operate on subjective determination about what is suitable and what the criteria for selection of content should be. It is important to for all kinds of rating systems to encourage Internet content providers to rate their pages. There are a number of compelling reasons why a provider or Web master might rate, not least of which is the signal it sends to governments around the world, that the World Wide Web is willing to self-regulate, rather than leaving it to government legislation to decide what is or is not acceptable.[48]

Recreational Software Advisory Council on the Internet

The Recreational Software Advisory Council is an independent, non-profit organisation based in Washington, DC, that offers one of the most popular content rating systems in the United States. The RSAC on the Internet (RSACi) system provides consumers with information about the level of sex, nudity, violence, offensive language (vulgar or hate-motivated) in software games and Web sites. To date, RSACi has been integrated into Microsoft's browser, Internet Explorer, and MicroSystem's Cyber Patrol Software. CompuServe (United States and Europe) has also committed to rate all its content with the RSACi system.[49]

Stand-alone software

A number of stand-alone software programmes have been developed which enable control over content by "blacklisting" -- where access to listed sites is blocked --- and "whitelisting" -- where access is only possible to listed sites. These lists are compiled either through employees who follow links to identify sites for inclusion on the lists, or through the use of Web crawlers that search for key word strings to locate likely pages for inclusion. A variety of stand-alone, inexpensive and easy-to-install software is available to block access to material judged inappropriate for children. Most packages give parents the option to choose the kinds of material to block such as sexually explicit material, violence, advertising, or extremist views and each of the filtering software programs offer different choices as to the content categories to be filtered. The leading stand-alone software packages currently available are:[50] Cyber Patrol, CYBERsitter,[51] The Internet Filter, Net Nanny, Parental Guidance, Netscape Proxy Server, WebTrack, and SurfWatch.[52]

Codes of conduct, hotlines, complaint handling procedures and other initiatives

More generally, a number of online industry associations around the world have undertaken a variety of industry self-regulatory initiatives, including drafting codes of conduct and implementing hotlines and complaint-handling procedures. Industry associations which have developed draft codes, to date, include the following:[53]

- Internet Industry Association of Australia (INTIAA).
- Committee of Australian University Directors of Information Technology (CAUDIT).
- Western Australia Internet Association (WAIA).
- South Australian Internet Association (SAIA).
- Eros Foundation of Australia.
- The Canadian Association of Internet Providers (CAIP) http://www.caip.ca.
- Canadian Standards Association (CSA) (Standard Model Code for the Protection of Personal Information).
- Finland advertising and professional content providers association.
- ISP Association of the Republic of Korea.

- Internet Watch Foundation of the United Kingdom.

- Electronic Network Consortium of Japan http://www.nmda.or.jp/enc/guideline.htm.

- The Association of the Internet services providers associations of the countries of the European Union (Euro-ISPA) http://www.euroispa.org/index.html.

- The Internet Service Providers Association of the UK (ISPA - UK) http://www.ispa.org.uk/.

The following countries have Internet-based hotlines which provide mechanisms for users to report illegal or harmful content that they see on the Internet: Austria, Belgium, Denmark, Greece, Hungary, Korea, the Netherlands, Norway, Sweden, United Kingdom, United States.[54]

There are a variety of other private sector initiatives under way, including:

- Childnet International http://www.childnet-int.org.

- Global Internet Liberty Campaign (GILC) http://www.gilc.org/.

- 2B1 Foundation < http://www.2b1.org>.

- ECPAT (End Child Prostitution in Asian Tourism) http://www.rb.se/ecpat/porno.htm.

- Redd Barna (Norwegian Save the Children) http://childhouse.uio.no/redd_barna/.

- National Centre for Missing and Exploited Children *(*NCMEC) http://www.missing.kids.com.

- EURIM (The European Informatics Market) <http:// www.eurim.org>.

C. International activities

European Commission

Based on the Commission's work within the Working Party on Illegal and Harmful Content on the Internet and on the "Green Paper on the Protection of Minors", the work already achieved within the EU has led to broad agreement on the following concepts which bring together the diversity of member states' approaches :

- Illegal content must be distinguished from harmful content. The two categories require different measures to deal with them.

- The protection of human dignity, a subset of illegal content, must be distinguished from the protection of minors, a subset of harmful content.

- The protection of human dignity refers to a type of restriction to prohibit certain kinds of material considered as intolerable both for the individual and the community at large and as going to the roots of society. Prohibitions on general categories of material detrimental to human dignity such as "obscene", "contrary to morals" or "indecent" exist in most member states (child pornography, violent pornography, incitement to racial hatred or violence).

- The protection of minors is to ensure that minors do not normally have access to material which could damage their physical or mental development, while at the same time allowing adults access to such material (violence, sexually explicit content, etc.).

- Illegal content must be dealt with at source by law-enforcement agencies. The industry can help reduce circulation of illegal content through properly functioning systems of self-regulation (such as codes of conduct, establishment of hotlines) in compliance with and supported by the legal system.

- In tackling harmful content, the priority actions should be to enable users to deal with harmful content through the development of actions to increase parental awareness and technological solutions (filtering) and content rating systems, and developing self-regulation which can provide an adequate framework, in particular for the protection of minors.

The Commission has identified areas in which to establish a clear and predictable framework within which industry as well as users can realise the potential of the networks and will promote them. Concrete measures where industry could take initiatives with support and encouragement from governments could include:

- An international network of hotlines (especially dealing with content affecting human dignity, such as child pornography).

- Development of compatible rating systems, which take account of cultural and linguistic diversity.

- Exchange of experience between all those involved, in particular industry, self-regulation bodies and users.

The Communication on illegal and harmful content on the Internet[55] was adopted on 16 October 1996. It has been debated by the European Parliament and the Committee of the Regions, who have adopted reports. It sets out proposals from the Commission for immediate action to deal with harmful and illegal content.

The Council requested the Working Party on illegal and harmful content on the Internet to present concrete proposals for possible measures to combat the illegal use of Internet or similar networks. The first report[56] was submitted to the Council on 28 November 1996. The report follows the proposals made in the Communication and elaborates on a number of issues such as self-regulation and liability. A second report,[57] submitted to the Council held on 27 June 1997, sets out the progress made in the member states on measures to deal with illegal and harmful content and summarises activities since then in the EU institutions.

The Council Resolution on illegal and harmful content on the Internet [58] was adopted on 17 February 1997. The Council and representatives of member states invited the member states to encourage and facilitate self-regulatory systems, encourage the provision to users of filtering mechanisms and the setting up of rating systems, and participate actively in the Bonn International Ministerial Conference in July 1997. They requested the Commission, as far as Community competencies are concerned, to: ensure the follow-up and the coherence of work on the measures suggested in the report; foster co-ordination at Community level of self-regulatory and representative bodies; promote and facilitate the exchange of information on best practice in this area; foster research into technical issues, in particular filtering, rating, tracing and privacy-enhancing technologies, taking into account Europe's cultural and linguistic diversity; and consider further the question of legal liability for Internet content.

They recommend that the Commission and member states take all necessary steps to enhance the effectiveness of the measures referred to in the Resolution through international co-operation building on the results of the International Ministerial Conference and in discussions in other international fora.

On 24 April 1997, the European Parliament adopted a Resolution on the Commission Communication on illegal and harmful content on the Internet, based on a report[59] by M. Pierre Pradier. With respect to illegal content, the Resolution *inter alia* (1) calls on the member states to define a minimum number of common rules in their criminal law and to strengthen administrative co-operation on the basis of joint guidelines; and (2) calls on the Commission to propose, after consulting the European Parliament, a common framework for self-regulation at EU level. This framework should include:

- Objectives to be achieved in terms of the protection of minors and human dignity.
- Principles governing the representation of the industries concerned at EU level and the decision-making procedures.
- Measures to encourage the enterprises and industries involved in telematic networks to develop message protection and filtering software, which should be made available automatically to subscribers.
- Appropriate arrangements for ensuring that all instances of child pornography uncovered on computer networks are reported to the police and shared with Europol and Interpol.

Furthermore, the Resolution stresses the need for international co-operation between the EU and its main external partners, on the basis of conventions or via the application of new international legal instruments and it calls upon the Commission to submit proposals for a common regulation of liability for Internet content. Finally, it urges the member states and Commission to promote co-operation among Internet access providers, in order to encourage self-regulation. With respect to harmful content the Resolution calls on the Commission and the member states to encourage the development of a common international rating system compatible with the PICS protocol, and sufficiently flexible to accommodate cultural differences, which will benefit both users and content publishers.

The Rolling Action Plan on the Information Society adopted in December 1996 included a reference to an Internet action plan which will be presented to the Council in December 1997.

The "Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services"[60] (COM(96) 483 final) was adopted by the European Commission on 16 October 1996, together with the Communication on Harmful and Illegal Internet. The Green Paper has provided all those involved in the audio-visual and information sectors of Europe and beyond with a springboard for reflection and debate. Its scope is the much-needed adaptation of regulatory frameworks and attitudes in the context of the emergence of new audio-visual and information services across the spectrum from television to the Internet with a specific focus on "the protection of minors and human dignity". The Communication, on the other hand, whilst concentrating on the Internet, has a broader scope in terms of tackling "illegal and harmful content".

The Green Paper is the first stage of a medium- to long-term project in which a large number of public and private institutions and organisations are joining forces. On 18 November, the European Commission adopted a Communication on the follow-up to the Green Paper.[61] The Communication includes a proposed Council Recommendation which would provide common guidelines for the implementation of a self-regulatory framework for the protection of minors and human dignity in audio-visual and online information services.

In the field of Justice and Home Affairs, the Dutch Presidency of the EU has launched, in the context of the structures of the Justice and Home Affairs Council, a reflection exercise on the Internet issue. It produced a working document, within the police co-operation working party, to allow for legal interception of Internet communications. A more general paper was also produced containing a number of further recommendations, still to be examined by the experts, with a view to developing practical co-operation among the law enforcement authorities concerning Internet-related activities. In the process of drafting a convention on mutual assistance, which concerns judicial co-operation in criminal matters, the question of possible need of a specific provision for Internet was raised. The working group considered that to be premature at this stage, since most member states have at present little or no experience of particular difficulties in the field of judicial co-operation in relation to offences perpetrated by the use of the Internet. Hence, work is being carried out with a view to investigating any measures which can be considered in the context of the "third pillar" comprising both the Police and mutual judicial assistance in criminal matters involved in the use of the Internet.

The European Commission, DG XV, has published a call for tenders for a study on legal liability systems in member states regarding information society services. The study will draw up an inventory of laws, regulations, administrative practices and forms of self-regulation which are in existence or in preparation in the member states, and which establish forms of legal liability applicable to operators and users of information society services, including copyright and neighbouring rights.

The European Community respects the fundamental rights and freedoms of citizens such as their right to privacy, including secrecy of communications, as well as freedom of expression and speech as laid down in international and European Human Rights Conventions, and the constitutions and traditions of its Member States. In the particular context of illegal and harmful content on the Internet, together with these fundamental texts, the European Data Protection Directive 95/49/EC lays down general principles for the processing of personal data. In addition, the draft directive on privacy in the telecommunications sector contains complementary requirements for the protection of privacy and the processing of personal data in the context of public telecommunication networks. These principles strike the necessary balance between different interests: the right of the individual to remain anonymous in the online world and limitations to that right only in so far as it is strictly necessary in a democratic society, for example to prevent, investigate and prosecute criminal offences. These legal requirements have also to be implemented by technical means, such as the provision of anonymous reading, browsing and e-mail facilities and in general the concept of privacy-enhancing technologies for access to, use of and payment for online services.

Council of Europe

The issue of "content on the Internet" relates to a range of subjects, which have been or are currently being examined within the Council of Europe, particularly in the areas of freedom of expression and information, right to privacy, harmful and objectionable content and conduct, illegal content and conduct, and pluralism of content.

Article 10 of the European Convention on Human Rights guarantees the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. Therefore, any regulation which limits freedom of expression via the Internet or other new communications technologies and is applied within the jurisdiction of the Convention, must be in conformity with Article 10 of the Convention. The European Court of Human Rights is charged with supervising the application of Article 10 of the Convention and has developed a strong body of case law.

The Committee of Ministers of the Council of Europe reiterated, in its Declaration on the Freedom of Expression and Information of 1982, the firm attachment by member states to the principles of freedom of expression and information as a basic element of a democratic and pluralist society and declared that in the field of information and mass media member states must seek to achieve "absence of censorship or any arbitrary controls or constraints on participants in the information process, on media content or on the transmission and dissemination of information".

The 5th European Ministerial Conference on Mass Media Policy (Thessaloniki, 11-12 December 1997) on "The Information Society: A Challenge for Europe" will address the exercise of freedom of expression and information within the framework of new information services and put it in relation to other rights and interests possibly at stake by the use of these services. On the basis of the political decisions taken at the Ministerial Conference, the Steering Committee on the Mass Media and, in particular, its Group of Specialists on the Impact of New Communications Technologies on Human Rights and Democratic Values will continue to examine the various issues raised in this respect with a view to formulating possible pan-European standards. Canada has requested to participate in this work as a non-member state.

The right to one's private and family life, home and correspondence is guaranteed by Article 8 of the European Convention on Human Rights and safeguarded by the European Court of Human Rights. In addition to this general norm, content and conduct on the Internet can fall under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)[62] as well as Recommendation No. R(95)4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services.[63] The implications of the development of new information and communications technologies on privacy and data protection are currently being examined within the Council of Europe by Working Group No. 15 of the Project Group of Data Protection and the Group of Specialists on the Impact of New Communications Technologies on Human Rights and Democratic Values.

The work of the Steering Committee on the Mass Media related to freedom of expression and illegal, harmful or objectionable content led to the adoption of Recommendation No. R(89)7 concerning principles on the distribution of video-grams having a violent, brutal or pornographic content and Recommendation No. R(92)19 on video games with a racist content. Although focused on a different type of media, both Recommendations can also serve as guidelines for the Internet. The Internet is expressly included in Recommendation No. R(97)19 on the portrayal of violence in the electronic media, which sets up guidelines for the responsibilities and means of action of the media sector as well as of states. Recommendation No. R(97)20 on hate speech (*i.e.* "all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin") addresses measures to combat such hate speech, while respecting freedom of expression. Guidelines for the promotion of a culture of tolerance in the media are laid down in Recommendation No. R(97)21 to encourage positive action by the media conducive to the promotion of tolerance. These Recommendations have been drawn up in co-operation with media professionals and the media industry and apply in a technology-neutral way to all types of media.

Where the cross-border character of the Internet requires international rules on the applicability of national laws and the jurisdiction of national courts, the European Committee on Crime Problems elaborated Recommendation No. R(89)9 on computer-related crime[64] and Recommendation No. R(95)13 on the problems of criminal procedural law connected with information technology.[65] The European Committee on Crime Problems has established the Committee of Experts on Crime in Cyberspace, which has been mandated by the Committee of Ministers to examine the feasibility of drawing up a convention on this subject. The wider than pan-European character of cyberspace is reflected in the composition of the

Committee, which comprises also the non-member states Canada, Japan and the United States. Council of Europe conventions can also be open for signature by non-member states.

Recommendation No. R(91)11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults addresses issues of relevance to the current international discussion on the misuse of the Internet in this respect.

The cultural challenges of new information technologies are currently being examined by the Project Group on New Technologies of the Culture Committee of the Council of Europe. Fields of action comprise, for example, the issues of artistic expression, electronic book publishing and cultural pluralism.

The Second Summit of Heads of State and Government of the Council of Europe's 40 member states (Strasbourg, 10-11 October 1997) adopted a Declaration and Action Plan which calls for the development of "a European policy for the application of new information technologies, with a view to ensuring respect for human rights and cultural diversity, fostering freedom of expression and information and maximising the educational and cultural potential of these technologies".

Other international initiatives

International Working Group on Content Rating

The International Ministerial Conference entitled "Global Information Networks: Realising the Potential" was held in Bonn on 6-8 July 1997. The Conference was hosted by the Federal Republic of Germany and organised in co-operation with the European Commission. Ministers from 29 European countries took part (European Union, EFTA, Central and Eastern European countries and Cyprus), as did government representatives from the United States, Canada, Japan and Russia as guests; businesses which are global players (content providers, access and service providers, network providers, equipment manufacturers); representatives of users; and as observers, representatives from European Union institutions or organs and from other European and international organisations. Among themes dealt with were: preventing and combating misuse of the global information networks; the importance of industry self-regulation; the availability of technical solutions to provide user empowerment; and responsibility of the actors. The Conference was concluded by three Declarations: by European Ministers, by industry and by users.[66]

Following upon the Global Information Networks Conference in Bonn, an international working group was formed to initiate a dialogue on international rating issues. The International Working Group on Content Rating, sponsored by INCORE,[67] the Internet Watch Foundation (IWF), RSACi, ChildNet International[68] and the Australian Broadcasting Authority, held a first organisational meeting on 29-30 September 1997. The Group proposed a set of principles and an outline structure for creating a new global system for rating Internet content. The idea is that the rating description will be contained in a PICS-compatible label generated by a content producer using guidelines and software developed by the new International Working Group for Content Rating. The descriptions will be designed in objective terms so as not to be specific to any one country or culture. The Group will encourage individual countries to develop profiles which will match the categories and levels in the internationally agreed labelling system to existing familiar standards in their countries.

INHOPE Forum

As a number of countries have set up or are considering setting up hotlines or information points for the reporting of illegal material, some of the already established hotlines have recognised the value of looking at possible co-operation at the international level. The Internet Hotline Providers in Europe Forum (INHOPE Forum) is an initiative being implemented by the UK-based organisation "Childnet International" to bring together hotlines throughout Europe to consider common issues of concern and the scope for co-ordination.

P8 Senior Level Group on Transnational Organised Crime

The P8 Senior Level group on transnational organised crime (Lyon group) has started work to develop legal and technical mechanisms that allow for timely international law enforcement response to computer-related crimes, *i.e.* to enhance abilities to locate, identify and prosecute criminals; co-operate with and assist one another in the collection of evidence; and commit resources to training law enforcement personnel to fight high-tech and computer related crime. The COMCRIME study on legal aspects of computer-related crime in the information society will be reporting in autumn 1997. The report will provide an in-depth analysis of the substantive law aspects describing the situation in the European Union, the United States of America, Canada and Japan, as well as a description of procedural law aspects. Its results will feed the on-going work on the implementation of the Action Plan to combat organised crime endorsed by the European Council in Amsterdam,[69] which includes a recommendation to combat the use of new technologies and means of communication, including the Internet, by organised criminals.

UNESCO

The United Nations Educational, Scientific and Cultural Organisation (UNESCO) commissioned a report on "The Internet and some International Regulatory Issues Relating to Content"[70] which was conducted by the Australian Broadcasting Authority. The study examined the impact of online services, particularly in relation to content, in Australia, Malaysia, Singapore and the United Kingdom. The study found that despite differences in approach due to different political, cultural and religious values, all four countries have placed an emphasis on industry responsibility in the way they are approaching the issue.

III. Common issues

The inventory shows a variety of approaches to addressing issues related to content on the Internet. Many countries have actively engaged in a process to identify and implement solutions. Some countries are focusing on specific areas of concern, while other countries are studying the broader issues. The inventory reveals that, despite the various stages of policy development, there are some "common threads" which appear in most national approaches in one form or another. These common issues are outlined and discussed below.

Without intending to be exhaustive, and without implying any kind of ranking in the order they are presented, the following list presents a number of common points which are frequently taken into consideration as OECD countries develop and implement approaches to Internet content issues:

- Defining the diverse services and technologies available and identifying main actors in terms of the functions they perform.

- Clarifying liability and responsibility for various parties.
- Reaffirming the application of existing law to the new medium.
- Achieving jurisdiction and enforcement in the global network environment, including technological capabilities and limitations to control or enforce, and the choice of law.
- Respecting fundamental rights, common values and community standards.
- Recognising cultural diversity.
- Protecting special groups (especially children).
- Protecting privacy and personal data.
- Recognising intellectual property rights as a distinct category of content issues.
- Focusing on technological solutions, and the importance of the industry role.
- Focusing on education and empowering users.
- Determining whether international co-operation is necessary, what it could entail, and how it might be accomplished.

Defining the diverse services and technologies available and identifying main actors in terms of the functions they perform

Because the definition and scope of the terms employed ultimately affect how they approach Internet issues, all OECD Member countries have addressed the need to identify the services, technologies and actors involved in Internet transmissions, as they work to develop their policies on these issues. The seemingly simple matter of definitions can be contentious, as the fast-paced changes in the electronic world have required an evolution in the thinking on these points. However, there is wide recognition that any discussion of content issues -- whether at the national or international level -- requires some common understanding of the diverse services and technologies available on the Internet and the functions performed by the primary actors involved. Common working definitions are an important element of any national approach, and may also move the process forward towards international understanding and examination of the issues.

The different applications used on the Internet -- in particular the World Wide Web -- are often mistaken for the Internet itself. Most countries agree that a clear understanding of the technologies is critical to policy making in this area and have begun by recognising the variety of Internet applications and technologies and how they can be used to distribute or access content, and by developing an understanding of the different actors that play a role in the content "transmission chain". A number of countries use analogies from the physical world to describe the functions of actors in the online world, such as librarian, bookstore, telecommunications carrier, news-stand, broadcaster or shop owner. In general, countries are moving toward defining actors in terms of the functions they perform in relation to content, such as:

- Different kinds of information carriers: *e.g.* network access providers, network service providers and Internet access providers.

- Different kinds of client-side actors: *e.g.* software providers, system owners, system administrators, system operators, and users.

- Different kinds of server-side functions: *e.g.* Web master, Web site host, Web site owner, Internet service provider, intermediate service providers, content provider, value-added provider, quasi-editorial functions such aggregation and packaging of content, navigation assistance, or other.

Clarifying liability and responsibility for various parties

The importance of allocating liability and responsibility for parties that have contact with content on the Internet is widely recognised among the countries that participated in this study. Most countries are actively discussing this issue within their national consultations in this area, but few have taken any action in this regard to date. However, there seems to be a general recognition that allocating risk in open distributed systems is not going to be simple -- because content sources are often hard to trace, and intermediaries may have contact with content but not have direct responsibility for it.

Businesses and users have an interest in clarifying the liability issue because they want to have an expectation of the consequences of their online behaviour. Businesses in particular are interested in determining what kind of risk they may be taking by engaging in online activities that involve content, as uncertain liability risks could act as an economic disincentive. Many OECD countries are working to clarify liability and responsibility in order to promote the wider development of network technologies and electronic commerce.

Traditional concepts of liability are generally based on the "fault" of the parties -- that is, the party that performs the act is responsible for resulting damages. In the context of the Internet, the question of whether or not the party had control over the content is a key factor in determining liability. "Control" could be determined by whether the party was merely a pure conduit or supplied input (whether the party intervened in the Internet transmission chain), or it could be determined by the party's connection to knowledge about the content (whether the party knowingly vouched for the content or edited it). As a consequence, the responsibility of the parties might depend on their actual activities and abilities to interact with content at various stages in the distribution and access process. An Internet service provider, a Web master, or any other actor in the Internet content transmission chain can have different degrees of control over information, in various circumstances. Depending on the degree of control effectively exercised, their liability could be lesser or greater. Also, the longevity of the information might be related to the ability to exercise control over it; that is, liability might not be evaluated in the same way for information that is stable as for information which varies continuously.

Some countries have determined that users may need to be encouraged to take responsibility for themselves and their actions online. In the early stages of the development of the Internet there were only a limited number of users, and information content and online conduct had little effect on the public at large. In many instances, network operators and users developed their own systems for acceptable behaviour ("Netiquette"), and there was little concern for government intervention in the public interest. The explosive growth in the number of network users in recent years has greatly increased the potential social impact that content may have today, and this poses a number of new issues. Some have suggested that these issues might be addressed by a collective approach to rules for online etiquette, such as a code of good conduct for online user behaviour.

Reaffirming the application of existing law to the new medium

While it is true that the emerging Internet brings with it enormous changes, it also offers an element of continuity, because many of the issues it raises have been addressed before in other contexts. Perhaps the most widely accepted point which emerged from the inventory is that most countries begin their examination of content on the Internet from the position that existing law should be the context for addressing these issues. What is illegal in the surrounding society should be illegal on the Internet as well: the Internet is not a legal vacuum and existing laws apply. Even those countries which believe that existing law might not be completely sufficient do agree that the new issues arising from the development of the Internet should be addressed by adapting and amending existing law. All countries seem to agree that it is important to identify existing legal and self-regulatory rules and practices and determine how they can be applied to the online environment before considering whether to revise laws or draft new ones.

Governments have found themselves challenged to achieve a balanced approach to address these issues which will protect the various interests at stake. Some countries are considering whether they need to review the traditional concepts underlying their legal frameworks before updating laws or making new laws. There is a concern that national laws lag behind technological development, making it necessary constantly to update legal provisions. Some countries suggest that there might be a need to rethink the basic concepts in a technology-neutral way. For example, the distinction between private correspondence and public broadcasting that underlies much of the traditional media law might not be as relevant in the context of interactive technologies.

Achieving jurisdiction and enforcement in the global network environment, including technological capabilities and limitations to control or enforce, and the choice of law

The issue of jurisdiction and enforcement in the global network environment opens up an enormous and complex topic with implications that extend far beyond the discussion of content. The implications of the inherently international nature of the Internet is an issue considered by all countries, not just in this context, but in the broader context of global information infrastructure and global information society policy. At this point, countries are asking questions about the legal and technological limitations for enforcing their national laws against actors on the Internet who violate them, but few have answers yet. Many countries are optimistic that technological solutions can help resolve some of these issues, and they are focusing efforts on facilitating and encouraging the development of technologies to help empower users to protect themselves against illegal acts in the online environment. For example, cryptography and certification technologies may make fraud and misrepresentation online more difficult and the use of filtering and rating technologies and monitoring by parents can help to shield minors from adult material. Questions still remain with respect to enforcing laws against adults who want to access or distribute illegal content.

Some countries point out the need for legal, regulatory and policy frameworks to support the technology, particularly in terms of enabling law enforcement capabilities to exist within the context of technological solutions. From this perspective, the issue is not related to the applicability of substantive laws, but rather to the ability to enforce national laws in the inherently global environment. Many countries have noted that international co-operation between law enforcement agencies is a vital element for addressing illegal content on the Internet, and they have called for efforts to ensure that ISPs, law enforcement agencies and hotlines in various countries co-operate efficiently.

Other countries note that where national laws are different, making something illegal in one country and legal in another, it is particularly important to be careful when trying to enforce national laws in another jurisdiction. These countries express the view that governments may need to change the way

they think about enforcing their national laws in the global context. In such a case, again, the best solutions might be those based on technologies which empower users to protect themselves. Like the physical world, the electronic environment will never be completely free of illegal and harmful activities, and technological solutions will not be able to resolve all the issues of enforcement in the electronic environment. Governments are also challenged to find an appropriate balance between their efforts to eliminate undesirable aspects of the Internet, and promoting the benefits desirable aspects of the medium.

Respecting fundamental rights, common values and community standards

In one way or another, most countries consider the implications of respecting the fundamental rights of citizens and community standards in developing their approaches to content on the Internet. Some countries have considered whether it is useful to attempt to reach an international consensus on basic common values that could be agreed upon for protection in the online environment. Freedom of expression and the free exchange of ideas are generally values which are fundamental building blocks in the national approaches of most countries. Many countries view freedom of expression as a fundamental right which can be protected by both technological and legal measures adapted to the specific characteristics of communications flows over open information and communications networks like the Internet. The free exchange of ideas could be promoted as a fundamental prerequisite for the continued expansion of global information infrastructures and an important element of democratic society.

Recognising cultural diversity

Cultural diversity can have a significant impact in the context of Internet content. On the one hand, the Internet offers great potential for the development of diverse communities by providing an environment where cultural diversity, community connections and languages can flourish, and many countries specifically promote this aspect of the Internet. However it also raises issues in the international context, where "community standards" can vary significantly -- and different types of content can be subject to different levels of control in different countries. Culture plays a role where the same content could be illegal in one place, only controversial in another place, and perfectly legal and acceptable in yet a third. Furthermore, some have argued that the value of the Internet to promote cultural diversity can also be used opportunistically to preserve nationalist policies and protect national industries. In this way, one of the greatest benefits of the Internet -- cultural diversity -- can also be one of the greatest points of contention, and these issues are being weighed by many countries as they work to formulate their national policies.

Protecting special groups (especially children)

Many governments have voiced a strong resolve to devote specific attention to the protection of special groups -- in particular children -- from certain kinds of content on the Internet. Children's issues have received a great deal of public attention recently; however, it is important to note that many of the same issues that apply to children also apply more generally to any group that requires special protection. Children and other people who are limited in ability to discern and make judgements may not be able to fully protect themselves from content on the Internet, and a number of governments are being called upon to help them. While noting the importance of protecting children from harmful content on the Internet, many policy makers also note the concern that the entire network not be run so that the only content available to adults is that which is fit for children. Most countries approach this issue by focusing on the importance of technology-based solutions to empower users to protect themselves and their children, and user education. Many countries are emphasising the importance of teaching parents about technology in order to: (1) protect their own children from what they think is important to protect them against; and (2)

gain a fact-based understanding of both the benefits and potential threats related to the use of network technologies.

Protecting privacy and personal data

Recognising that network transmissions will increasingly generate vast quantities of data that can be easily and cheaply stored, analysed, and reused, a number of countries have taken into consideration the protection of privacy and personal data in the context of the discussion of content issues. Solutions such as content filtering technologies rely upon the collection of personal preferences by software or the service provider and restricted access and user verification relies on the collection of personal information or certification of information about a user (*e.g.* certification of age, adult identification, etc.) by a certification authority. When these operations require proof of identity, the transactional data could leave detailed and perhaps irrefutable trails of an individual's commercial activity, as well as paint a picture of private, non-commercial activities. In both cases, users must weigh the costs of disclosing personal data with the benefits of enjoying the services that require data. There are also issues related to anonymity -- the desire for anonymity and protection of personal data might have to be balanced against the need for identifying content creators and responsible parties. Also the issue of anonymity arises in determining the role of ISPs and the need to reveal the identity of users when requested by law enforcement authorities.

Countries have also noted the emergence of another important privacy issue in the context of content on the Internet and the implications of the distinctions made between public and private communications in their national legislation. This distinction is important because "public communications" are protected by the right of free expression and "private communications" are protected by the right to secrecy of correspondence and privacy (including data protection). Again, countries have found that a general understanding of how the technology works is needed to determine whether different kinds of transmissions should be considered public or private. For instance, e-mail is often considered a private communication which cannot be subject to monitoring for content unless it meets some legal criteria for public interest. However, it is not always clear whether e-mail is a private communication, for example, where e-mail is circulated to a large number of recipients.

Recognising intellectual property rights as a distinct category of content issues

While open information and communications networks make the electronic transmission of all kinds of digitised data fast, cheap and simple, the ability to make and distribute perfect copies of all kinds of data creates a number of challenges for the protection of intellectual property in the online environment. Trade in creative content can provide economic incentives to fuel the development of information and communications technologies, and intellectual property protection is essential to stimulate the production of, and trade in, high-quality creative content. No discussion of content is complete without mention of intellectual property issues; however, the resolution of many other content issues may not be applicable in the intellectual property arena because there are different issues at stake. Furthermore, a number of well-established international standards already exist in the area of intellectual property protection.

Countries are finding that Internet technologies bring with them new intellectual property issues that are peculiar to the emerging medium. Intellectual property protection is a serious concern for policy makers in the public and private sectors and is under consideration at the highest levels. There are two main points which countries are addressing: on the one hand, it is important to preserve the intrinsic value in the author's creation, however, there is also an important economic issue at stake because people want to make money by selling content on the Internet. Governments are finding the issue to be a complex one that involves technology, economics and legal analysis. It is recognised as an important issue by all

countries in their national policy making, and it has been the subject of considerable negotiation at the World Intellectual Property Organisation (WIPO).

Focusing on technological solutions, and the importance of the industry's role

There seems to be a strong consensus among the countries that responded to this survey that a focus on technological solutions is a fundamental element of approaches to content issues. In the same way that many of the issues arise from technology, solutions must be drawn from technology as well, and technological development must be pursued and supported. Most countries put considerable emphasis on the promotion of technological developments which can empower users to protect themselves against harmful content on the Internet (*e.g.* filtering, self-rating, stand-alone software, and user verification mechanisms). Several countries noted the need for balance in that context: empowering users, while at the same time avoiding excessive government interference and enabling the free flow of information. Furthermore, all governments seem to recognise the importance of the industry's role in that regard. Many governments are making efforts specifically to encourage industry development of technological solutions. There is also considerable emphasis on industry's role in developing self-regulatory initiatives. It is widely recognised that if industry develops effective technological solutions and businesses applies self-regulatory measures, conditions for governments to take a minimalist approach to government intervention would be more favourable.

Focusing on education and empowering users

The need for a focus on education is highlighted in most national approaches in terms of educating users and policy makers and the promotion of digital literacy generally. Increasingly, individuals, enterprises and governments are affected by information and communications technologies, in particular the Internet, and there is a need for a clear understanding of how technologies work and their implications. A lack of understanding could hinder the development and use of new information and communication technologies. Digital literacy will foster an environment where users take responsibility to protect themselves and actively engage in technology solutions.

There are a number of national initiatives under way along these lines, to teach about using the technology, understanding its implications, and engaging technology solutions. Educational measures could also aim to:

- Raise public awareness of the Internet as a valuable educational tool.
- Promote the responsible use of the medium and inform the general public about the benefits of the Internet, so that concerns about misuse of the Internet are not be exaggerated and can be addressed with factual information.
- Educate users on ways to protect themselves and their children from illegal or unwanted material on the Internet.
- Educate users about the legal framework governing their online activities.
- Educate system operators about securing their systems, and the importance of detecting and reporting criminal activities.
- Advise policy makers.

– Educate law enforcement authorities.

Determining whether international co-operation is necessary, what it could entail, and how it might be accomplished

One common element that emerges from each of the issues identified above is their international nature. All of these issues are being considered by Member countries as they work to develop national policy approaches, but each one could also be considered in the context of the broader international implications. Many countries have found that the increasingly global flow of data on information and communications networks suggests a need for an internationally co-operative approach to these issues. Given the inherently global nature of the developing networks and the difficulties associated with defining and enforcing jurisdictional boundaries in this environment, many governments have pointed out that these issues may be addressed most effectively through international consultation and co-operation. Furthermore, in framing national strategies and designing regulatory structures for the information infrastructure, governments are recognising that the impact of such activities will, in many instances, extend far beyond their frontiers. This may be particularly relevant in the case of content on the Internet, given the significant role of cultural norms and social values with respect to these issues. A number of countries have pointed out the need for international awareness of the issue in order to develop a common understanding of the various norms and rules that apply in different countries.

ANNEX I: SUMMARY TABLE OF NATIONAL APPROACHES

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Australia	Australian Broadcasting Authority (ABA)	*Investigation into the Content of On-line Services* (ABA, June 1996) and ongoing studies by the ABA	Amendments to some state censorship legislation to include online offences; general agreement to develop uniform state/territory laws to regulate content	Under proposed framework (July 1997): prime responsibility on content creators; access providers only liable with knowledge	Yes, with supervision by the ABA who is investigating issues related to codes of practice		Emphasis on "co-regulation" (self-regulation within a legislative framework), neutrality between online and off-line regulation and international collaboration.
Austria	Working groups have been established to consider issues relating to content on the Internet		Planned law to address illegal use of the Internet	ISPs only liable if they knowingly ignore illegal content; Austrian law applies to content downloaded in Austria regardless of its origin		Yes	Emphasis on the application of existing rules to the online environment. The major challenge is seen as enforcement across national borders.
Belgium	Various including: Telecomms. Ministry, Prime Minister's Office, Ministry of Scientific, Technical & Cultural Affairs, Belgian Institute of Postal Services & Telecomms., and National Commiss. against the Sexual Exploitation of Children		No new laws, hasty regulation is considered undesirable and existing criminal laws are applicable to the online environment		Internet Service Providers' Association of Belgium (ISPA) which, following consultation between public authorities and ISPs, is preparing a code of conduct	Yes	Emphasis on initiatives at the European and international levels. The basic approach is to use technological solutions and self-regulation with legal backup provided by state authorities and existing criminal laws.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Canada	Information Highway Advisory Council (IHAC)	*Illegal and Offensive Content on the Information Highway* (June 1995, Industry Canada), *Connection, Community, Content: The Challenge of the Information Highway* (Sept. 1995, IHAC), *Undue Exploitation of Violence* (March 1996, Dept. of Justice), *Building the Information Society: Moving Canada into the 21st Century* (May 1996, Canadian Govt), *The Cyberspace is not a "No Law Land."* (Feb. 1997, Industry Canada) and *Preparing Canada for a Digital World*, (April 1997, IHAC)	No new laws, existing laws are generally technologically neutral.	Existing laws apply to content providers and end-users; there is uncertainty as to the extent of liability for access and service providers			Emphasis on the application of existing laws to the online environment in conjunction with research, consultation with the private sector and the promotion of education programmes.
Czech Republic		Parliamentary Report on Introductory Information on the Use of the Internet in the Czech Republic (May 1997)	Legislative changes are expected, probably in 1998	Responsibility for observing existing laws is primarily on the content provider; use of the Internet for private correspondence and public communication are distinguished			Emphasis on imposing responsibility for observing the laws on the content provider.
Denmark			Existing laws are currently being reviewed with respect to their online application	Existing laws apply to content providers and end-users; access and service providers generally only liable with knowledge			Emphasis on applying the same rules regardless of the media, international co-operation and use of technological tools.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Finland	Working Group on Information Networks	Report on freedom of speech in mass communications (February 1997), and *Privacy and freedom of speech on information networks* and *Public communication on information networks* (Working Group on Information Networks)	Proposal for a law on the responsibility of different online actors	Existing laws distinguish between content providers and technical intermediaries according to their roles and functions		Proposed	Emphasis on education, allowing private sector solutions to develop and use of the existing criminal law.
France	Conseil d'Etat	Report on the legal issues raised by the development of the Internet (1996)	The Conseil d'Etat is currently considering the need for changes to be made to existing laws	Distinctions are drawn between use of the Internet for private correspondence and public communication, and between the functions performed by the various Internet actors		Proposed	Emphasis on self-regulation with enforcement of existing laws as a backup, the development of technological solutions and international co-operation.
Germany			Information and Communication Services Law (1 August 1997, "IuKDG"); Media Services Interstate Agreement (1 August 1997); and amendments to various penal laws to broaden the term "writings" to include data carriers and working memories	Under the IuKDG, responsibility is placed primarily on content providers; access providers are responsible if they have knowledge of the content and are technically able to, and can reasonably be expected to, block it	Multimedia Service Providers Self-Regulation Organisation		Emphasis on creating a broad framework for the use of information and communication services through the IuKDG. In terns of content control, there is support for self-regulation, the application of existing penal and administrative laws to the Internet, and the review of content by the Federal Board for the Review of Publications Harmful to Youth.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Greece	Ministry of Transport and Communication and the National Committee for Telecomms. (NCT)				A working group is preparing a proposal for the implementation of a self-regulatory system	Proposed	Emphasis on the application of existing laws, the development and application of a self-regulatory system and broad international co-operation.
Hungary	Interdepartmental Committee for Information Technology and Telecomms	A study has been commissioned by the Ministry of Culture and Education on copyright and content issues relating to the provision of Internet access in secondary schools		Prime responsibility lies with content providers; access providers are only liable with knowledge		Yes	Emphasis on applying the existing laws and regulations to the online environment.
Iceland			Parliamentary proposal to make the penal code definitely applicable to computer fraud	Content providers are responsible under existing laws; the liability of service providers is yet to be determined	A code of acceptable use is being prepared for official Web sites		Emphasis on the application of existing laws, reviewing legislation where required, and the use of codes of practice.
Ireland	Working Group on Illegal and Harmful Use of the Internet						Emphasis on studying the issues and following international developments and controlling content through self-regulation and technological solutions.
Italy			The Senate is considering draft Law No. 2625/S on the sexual exploitation of minors over telecomms networks		Italian Minister of Communications has initiated an informal project with the goal of producing a code of conduct for service providers		Emphasis on the application of existing laws, the introduction of new laws, self-regulation and the development of codes of conduct.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Japan		Study groups include the Study Group for the Legal System on Electronic Commerce (Ministry of Justice), Study Group for the Advancement of the Condition for the Use of Telecomms (Ministry of Posts and Telecomms), and New Media Development Association (supported by Ministry of International Trade and Industry).			Electronic Network Consortium has published codes on *General Ethical Guidelines for Running Online Services* and *Recommended Etiquette for Online Service Users* (February 1996) and an association of ISPs is also working on guidelines		Emphasis on the application of existing laws, formation of guidelines for ISPs, the use of filtering technology rating of illegal and harmful content, co-operation with educational institutions and the private sector, and co-ordination with electronic commerce projects.
Korea	Information Communications Ethics Committee (ICEC)				ICEC has set out an ethics code for service providers	Yes	Emphasis on self-regulation, the application of existing criminal and civil laws, and technological solutions.
Luxem-bourg							Emphasis on the application of existing general laws, consideration of legislative amendments, and international co-operation.
Mexico	Ministry of Communications and Transport and Federal Telecomms Commission						Emphasis on the free flow of information, considering the need for legislative changes, and international co-operation.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Nether-lands		*Not for All Ages* (Parliamentary Policy Paper on the protection of minors, May 29, 1997). Research on possible government action is also being conducted within the framework of the National Action Program for the Electronic Highway.	Amendments to the Media Law and the Criminal Code are anticipated	Internet providers of illegal or harmful content first receive a warning to remove the material and, if they do not react, law enforcement action is taken	Codes have been developed by Internet industry groups	Yes	Emphasis on self-regulation and the enforcement of existing criminal laws as a backup. The transmission of content across national borders is recognised as a problem.
New Zealand					Internet Society of New Zealand (ISOCNZ) who, with government encouragement, has developed a code of conduct		Emphasis on self-regulation and the application of existing laws which do not distinguish between the Internet and other media.
Norway					*Internettforum* and the *Internett etisk rld*	Yes	Emphasis on the application and updating of existing laws, co-operation between authorities, business and the public, international co-operation
Poland							Emphasis on application of existing laws and consideration of amendments.
Portugal			Law No. 109/91 (17 August) relating to computer crimes				Emphasis on delimitation of responsibilities and terms of access to data networks. Education, technology and self-regulation are seen as being of assistance.
Spain			Penal Code (Organic Law 10/1995) covers crimes related to electronic media				Emphasis on the application and updating of existing laws, self-regulation and international co-operation.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
Sweden			Proposed law on electronic mediation services covering ISP liability	Under the proposed law, service providers liable for failing to prevent distribution of certain illegal and harmful messages	Swedish branch of the international Internet organisation ISOC is working on codes of conduct and hotlines		Emphasis on the introduction of new legislation to clarify liability in conjunction with self-regulatory initiatives such as codes of conduct.
Switzer-land	Interdepartmental Working Party on penal data protection and copyright aspects of the Internet (under the Federal Office of Justice)	*A New Medium: New Legal Issues* (Interdepartmental Working Party on penal data protection and copyright aspects of the Internet, May 1996)	Provisions of the Swiss Penal Code relating to violence and pornography apply to electronic media		The *New Medium* study assists ISPs in drafting codes of ethics by providing recommendations relating to dealing with illegal conduct, hotlines and access contracts.	Recom-mended in the *New Medium* study	Emphasis on the application of existing laws in conjunction with self-regulation and the creation of codes of conduct which follow the recommendations of the *New Medium* study.
Turkey	Internet Higher Council		Proposed law on Protection of Personal Data is before Parliament	Existing regulations and laws apply to content and service providers			Emphasis on the application and review of existing laws.
United Kingdom	Department of Trade and Industry		Some laws have been amended to apply to the online environment (*e.g.* Obscene Publications Act 1956 and Protection of Children Act 1978)	Content providers face liability and service providers will be liable as accessories if they are informed of illegal material and fail to remove it	Internet Service Providers Association (ISPA) and London Internet Exchange (LINX) have created the Internet Watch Foundation (IWF) as a framework for dealing with content issues	Yes	Emphasis on self-regulation through the IWF with sanctions provided by the application of existing technologically neutral laws. Rating and filtering systems are seen as important tools and international co-operation is seen as a priority given the transborder nature of the Internet.

COUNTRY	GOVERNMENT INITIATIVES				SELF-REGULATORY INITIATIVES		BRIEF SUMMARY OF NATIONAL APPROACH
	Lead agency (where reported)	**Reported studies**	**Reported new laws**	**Responsibility for content**	**ISP organisations and codes of conduct (where reported)**	**Hotlines (where reported)**	
United States			Communications Decency Act of 1996 (certain provisions of which were later declared unconstitutional by the US Supreme Court)				Emphasis on market forces and self-regulation in conjunction with the application of the existing legal framework governing freedom of expression and content control. Blocking, filtering and labelling technology, and education, are also seen as being of importance.

ANNEX II: SUPPLEMENTARY INFORMATION TO NATIONAL SUBMISSIONS

Australia[71]

Introduction

The Australian Federal (Commonwealth) Government announced principles[72] for a national approach to regulate the content of online services such as the Internet on 15 July 1997. In broad terms the scheme focuses on the protection of minors from objectionable material and involves:

- A self-regulatory framework for online service providers supervised by the Australian Broadcasting Authority (ABA) with provision for investigation of unresolved complaints by the ABA.

- A sanctions regime that includes fines for serious breaches of the Broadcasting Service Act 1992 by online service providers.

- A framework that will not hold online service providers responsible for the content accessed through their service where the online service provider is not responsible for the creation of that content or does not knowingly allow a person to use an online service to publish illegal material.

- A commitment that the Commonwealth will encourage the co-operative development of uniform State and Territory offence provisions regulating online content users.

Specific questions

Definitions

The proposed regulatory framework involves degrees of regulation recognising the characteristics of the various services offered and responsibilities of the various actors. The principles endorsed by the Australian Government contain definitions which are summarised below.

Services

- An online service is a service that makes content accessible on demand to the public by means of a telecommunications network, whether or not the service is available for a fee.

- The definition of an online service is intended to encompass only those online services with interactive capability, *i.e.* where the service allows the multi-directional transfer of content upon demand between an end-user and other end-users connected to the network.

- The definition of a telecommunications network is that contained in the Telecommunications Act, *i.e.* a system, or series of systems, that carries, or is capable of carrying, communications by means of guided and/or unguided electromagnetic energy.

- The definition of a telecommunications network should be technologically neutral and cover online services provided by way of fixed links, radio communication links, satellite, fibre and cable.

- As a general rule, where a service involves private or restricted communications (such as e-mail and intranets), it will not be subject to the regulatory framework, except to the extent that current provisions in the Crimes Act relating to the use of a telecommunications service in an offensive or harassing manner apply.

Actors

The responsibilities of the various actors are recognised through the principle that online service providers will not be liable for content accessed by means of their service where the provider is not responsible for the creation of that content. Prime responsibility for content is intended to lie with the act of publishing or transmitting material by online users, and is intended to be regulated by proposed State and Territory legislation. However, online service providers will be required not to *knowingly* allow a person to use their service to publish proscribed content.

- An online service provider will be a carriage service provider (as defined in the Telecommunications Act) providing access to a member of the public to an online service.

- A content originator or end-user of an online service not providing access to that online service will not be an online service provider for the purposes of the regulatory regime.

- A provider of network infrastructure (carrier) will only be subject to the regulatory regime applying to online service providers to the extent that they are also providing access to an online service.

- The legislation will allow a person who is providing, or proposing to provide, a service regulated under the Broadcasting Services Act to apply to the ABA for an opinion as to whether the service is an online service or a broadcasting service.

"Content" includes material transmitted in the form of:

(a) text;
(b) data;
(c) speech, music or other sounds;
(d) graphics or other visual images, whether static, moving or otherwise;
(e) software; and
(f) such other forms of content that are determined by the Minister by disallowable instrument.

An online service should not include:

(a) a service which transmits material solely by facsimile or voice telephony;
(b) a service which is not accessible to the public, such as an intranet;
(c) a service which only carries private or restricted distribution communications such as e-mail messages;
(d) a broadcasting or narrowcasting service within the definition of the Broadcasting Services Act; and
(e) such other services that are determined by the Minister by disallowable instrument.

Regulation of content

Authority

The Australian Constitution vests the power to regulate communications in the Federal government. This power is expressed principally through broadcasting and telecommunications legislation enacted by the Federal Parliament which in broad terms regulates "content" (Broadcasting Services Act) and "carriage" (Telecommunications Act), respectively. The censorship of non-broadcasting media, *e.g.* cinema films, video and publications is a shared federal-state responsibility with the states (and territories) enforcing classification decisions at the point of sale.

The regulation of Internet content is not specifically provided for in Federal legislation at this time, however some prosecutions in relation to child pornography have been launched under the Federal Crimes Act. Some state governments have amended their censorship legislation to include online offences but there is general agreement to consider a national approach with uniform state/territory legislation complementing the federal scheme (amendments to the Broadcasting Services Act) announced on 15 July.

As a general principle it is intended that material accessed through online services should not be subject to a more onerous regulatory framework than off-line material such as books, videos, films and computer games, that is, what is legal off-line should be legal online, subject to appropriate protection of minors.

The framework is intended to:

- Encourage online service providers to respect community standards in relation to material published by means of their service.

- Encourage the provision of means for addressing complaints about content published by means of an online services.

- Ensure that online service providers place a high priority on the protection of minors from exposure to material which may be harmful to them.

In particular, it is intended that the framework should encourage the development of self-regulatory mechanisms and avoid inhibiting the growth and development of the online services industry by placing unreasonable regulatory constraints on the online services provider industry regarding the publication and transmission of material.

At the Commonwealth level, content intended to be controlled is material that is equivalent to Refused Classification (RC) material (illegal to sell, exhibit or hire) under the Federal Office of Film and Literature Classification (OFLC) guidelines.[73]

Subject to negotiation with the states and territories, it is expected that offences will be created for the publication or transmission of RC material by online users and the publication or transmission of material unsuitable for minors on an online service where minors may have access to it. Material unsuitable for minors will be defined with regard to the X and R film categories, and equivalents for publications, in OFLC guidelines. In addition to sexual and/or violent material, the guidelines cover criminal and other illegal activities.[74] Privacy, fraud, defamation, and discrimination/vilification issues would dealt with under existing relevant legislation.

As a general rule where a service involves private or restricted communications (such as e-mail and intranets), it will not be subject to the regulatory framework, except to the extent that current provisions in the Crimes Act relating to the use of a telecommunications service in an offensive or harassing manner apply.

Non-regulatory initiatives

As outlined above, a co-regulatory approach (that is, industry self-regulation within a legislated framework) is proposed.

This is consistent with a number of studies and reports undertaken in recent years, specifically the Australian Broadcasting Authority (ABA) report "Investigation into the Content of Online Services" (June 1996).[75]

Industry initiatives

Pending the implementation of a national regulatory framework, a number of online industry associations have commenced the process of drafting codes of practice.[76] Industry associations which have developed draft codes to date include the following:

- Internet Industry Association of Australia (INTIAA)
- Committee of Australian University Directors of Information Technology (CAUDIT)
- Western Australia Internet Association (WAIA)
- South Australian Internet Association (SAIA)
- Eros Foundation

Most of these organisations have sought the ABA's comments on their drafts and have shown a willingness to meet the possible requirements of registration under a national regulatory regime. However, the ABA has made clear that it is unable to endorse any codes without appropriate legislative support and clear criteria.

In the ABA's view most (although not all) of the codes provide a good starting point for the development of responsible codes of practice for various segments of the Australian online industry.

International activities

Recognising the global nature of online services and the inherent limitations of national systems of regulation, the Australian Government will actively pursue in international fora collaborative arrangements for multilateral codes of practice in relation to online content and the development of online content labelling techniques. The ABA, an independent statutory authority within the portfolio of the Minister for Communication and the Arts has actively forged links with other national regulatory bodies and has been commissioned by UNESCO to report on comparative online content regulation.

The ABA's online services investigation

Online services, including the Internet, offer users an unprecedented level of variety, as well as quantity, of information, entertainment and educational services from all over the world. With the growth in the use of online services as a new communications medium, concerns have been raised about the content of some of these services. These concerns include the perceived ease of access to material which is of a "pornographic" nature or is considered to be unsuitable for children and young people ("Unsuitable material"). Also of concern is the availability of material which is generally illegal in Australia, such as child pornography ("Objectionable material").

Responding to this concern in Australia, the Federal Minister for Communications and the Arts directed the ABA to conduct an investigation into the content of online information and entertainment services, including services on the Internet. The ABA was also directed to consider the appropriateness of developing codes of practice for online services which, as far as possible, are in accordance with community standards. The ABA completed its report in July 1996.[77]

The Investigation identified a range of matters which should be addressed if online services are to be used in the most productive and effective manner. These went beyond concerns about objectionable and unsuitable material and included other content issues such as the potential for vilification, discrimination and harassment, and consumer issues such as standards of service, billing and credit management, and privacy.

It is important to note that the investigation also indicated overwhelming support for online services and for the opportunities they present for enhanced communication, information and entertainment by the Australian community.

ABA Recommendations

The ABA was conscious of the need to balance community concerns about online services on the one hand and not to stifle unduly a new and dynamic industry on the other. After giving detailed consideration to these issues, the ABA recommended that a substantially self-regulatory framework be developed for online services in Australia. The two main features of this proposed regime are codes of practice for service providers and the development of voluntary Internet content labelling schemes which will provide parents and supervisors with options to protect minors from material which may be harmful to them.

Summary

The ABA is very pleased to see proposals from bodies such as the OECD to discuss the complex issues relating to content and conduct on the Internet at the international level.

The ABA has recommended that a substantially self-regulatory framework based on codes of practice for service providers and voluntary content labelling be developed in Australia

With respect to codes of practice, the ABA is of the view that this emerging industry group provides an important intermediary function in the online environment and can achieve much in terms of finding practical and workable solutions to address community concerns.

The ABA is also of the view that the flexibility inherent in industry codes of practice may provide a useful framework for international discussion and possible consensus on the rights and responsibilities of participants in the international online environment

The ABA supports the role of voluntary content labelling, particularly in regard to the way it may be used to provide options for parents and supervisors to protect minors from harmful or unsuitable material. The ABA wishes to encourage discussion at international level about the potential for Internet content labelling and the possibilities of developing internationally accepted labelling schemes which address the major issues of concern around the world regarding Internet content.

The ABA acknowledges the important role of community education in ensuring that Internet users, including children, are able to maximise the advantages which the Internet offers as an enhanced educational, information and entertainment medium. The ABA also recognises the importance of informing parents and supervisors of the options available to them to manage the use of online services by minors, including options involving filter software products and content labelling and recommended a community education campaign to support those who are responsible for children's use of online services.

The ABA encourages research in the areas of online services to monitor the introduction of online services in our communities, examine the effectiveness of existing strategies for dealing with illegal and harmful material and determine the requirements of parents and carers in relation to those services.

Austria

Note: Throughout the following text, Austrian laws are specified by means of the number of their entry into the Austrian Federal Law Gazette (Bundesgesetzblatt, short: "BGBl") where Austrian legal instruments are first published.

Austrian federal laws on illegal content

Obscenity/sexually explicit materials

The basic legal provision concerning pornographic material is the *Pornographiegesetz* (Pornography Act, BGBl. Nr. 97/1950).

Sec. 1: Production, import, transportation, export, storage, offer, supply with, depiction, performance or any other procurement of pornographic writings, pictures, motion pictures or other such objects: up to one year and/or fine. These provisions apply only to "hard pornography", which is defined by the courts as excessively aggressive representations of sexual acts, representations of sexual violence, of sexual acts involving minors, animals or, according to partly outdated rulings, homosexual activities.

Sec. 2: Anyone who knowingly offers or makes accessible in return for payment, performs, depicts or procures to a person under the age of 16, writings, pictures or other representations that are apt to endanger the moral or physical development of such individuals: punishable by up to six months in jail or fine.

Protection of minors: child pornography, violence, abusive marketing

- Sec. 207a StGB (Penal Code, BGBl. Nr. 60/1974) - Child Pornography.

Production, import, transportation, export, offer, supply with, depiction, performance or any other procurement of pornographic representations of a sexual act in which a minor (person under 14 years, sec. 74 Nr. 1 StGB) is involved, if this representation conveys the impression that in the course of the production such a sexual act actually took place (which means that pseudo-pornographic representations

are also covered). Punishable by up to two years in jail if the criminal act is committed commercially (*i.e.* with Intent to obtain a regular criminal income) or by the members of a criminal gang (up to three years). In addition, the acquisition or possession of such pornographic representation is punishable by up to six months in jail or a fine.

This provision is the one most likely to apply to child pornography on the Internet.

Hate propaganda/hate speech

- Sec. 107 StGB (Penal Code, BGBl. Nr. 60/1974) - Dangerous Threat. Uttering a dangerous threat against an individual. The threat must be realistic, but there is no requirement that it is carried out. This provision might apply to radical groups that publish "black lists" of their enemies on the Net. Punishable by up to three years in jail.

- Sec. 188 StGB (Penal Code, BGBl. Nr. 60/1974) - Abasement of religious teachings. Punishable by up to six months in jail or fine.

- Sec. 283 StGB (Penal Code, BGBl. Nr. 60/1974) - Demagogy. Instigating hostile acts against the members of a religion, race, cultural group or state, or insulting such persons in a way that violates human dignity. This is the basic "Hate Speech" provision and is punishable by up to two years in jail.

- In the light of specific historic experience, Austrian law provides for a total ban of all activities of "Nazi" groups (*Verbotsgesetz*, BGBl. Nr. 13/1945). The maximum sentence for an attempt to reinstall Nazi organisations comes up to life imprisonment (sec. 3a *Verbotsgesetz*). Most likely to apply to Internet content is Sec. 3h which penalises denial, gross minimisation, approval or justification of Nazi genocide or other Nazi crimes against humanity, if committed publicly.

- Minor cases of Nazi propaganda (those that do not warrant prosecution in court) may be fined by the administrative authorities (Art. IX Abs. 1 Z 4 EGVG).

National security issues: sedition/terrorism/bomb production

Treason and espionage are treated in sec. 252-258 StGB. The most relevant laws for the Internet are:

- Sec. 275 StGB (Penal Code, BGBl. Nr. 60/1974) - "Landzwang". Causing fear and unrest in the population or a large part thereof by threatening with harm to life, health and property. A person who is believed to have sent false threats in the name of a real terrorist group has recently been investigated and might be charged with this provision. Punishable by up to three years in jail.

- Sec. 276 StGB (Penal Code, BGBl. Nr. 60/1974) - Spreading false, alarming rumours. Spreading lies which disrupt public order. Punishable by up to six months in jail or a fine.

- Sec. 281 StGB (Penal Code, BGBl. Nr. 60/1974) - Instigation to disobey laws. This means cases where people are publicly instigated to disobey the law in general, esp. by radical groups. Punishable by up to one year in jail.

- Sec. 282 StGB (Penal Code, BGBl. Nr. 60/1974) - Instigation to commit crimes or approval of crimes. Publicly instigating crime, or approving of a criminal act in a way which encourages similar misdeeds. Punishable by up to two years in jail.

Communication of erroneous information: fraud/unlawful advertising/defamation

Insult, defamation, slander:

- Sec. 111 StGB (Penal Code, BGBl. Nr. 60/1974) - *Üble Nachrede*. Accusing someone of dishonourable, immoral behaviour in a way which makes him appear despicable in the public eye. The defendant goes free if he can prove that the accusation is true or that he had good reason to believe the accusation to be true. The latter defence is only admissible if the accusation was not made before the general public (*e.g.* on live TV). Punishable by up to six months in jail or fine, or up to one year for committing the crime before the general public.

- Sec. 115 StGB (Penal Code, BGBl. Nr. 60/1974) - Insult. Calling someone vile names. Provocation is an accepted defence. Punishable by up to three months in jail or fine.

- Sec. 116 StGB (Penal Code, BGBl. Nr. 60/1974) - Public insult of parliament, the army or a government agency. Punishment is according to sec. 111 or 115 StGB. Sec. 116 just states that insults against these organisations carries the same punishment as if the deed had been committed against a person.

Some family members of a dead person may press charges against the perpetrator of an offence aimed at the dead person according to Sec. 111 or 115 StGB.

- Sec. 152 StGB (Penal Code, BGBl. Nr. 60/1974) - *Kreditschädigung*. Spreading lies that harm a person's career or credit rating. Punishable by up to six months in jail a fine or both.

Charges of the aforementioned offences may not be brought forth by the public prosecution but exclusively by the victim (sec. 117 StGB).

- Sec. 297 StGB (Penal Code, BGBl. Nr. 60/1974) - Slander. Knowingly spreading false allegations that expose the victim to prosecution by the law enforcement authorities, *i.e.* falsely accusing someone of a crime. Punishable by up to a year in jail or up to five years if the lie implied a crime punishable with imprisonment for more than a year.

Fraud:

- Sec. 146 to 148 StGB (Penal Code, BGBl. Nr. 60/1974) - generally applicable provisions against fraud. Up to six month for minor cases, up to ten years under aggravated circumstances (great extent of damage, commercial perpetration, *i.e.* with intent to obtain a regular criminal income).

- Sec. 148a StGB (Penal Code, BGBl. Nr. 60/1974) - Fraudulent manipulation of data processing systems with intent to obtain economic benefit. Punishable by up to six months in jail for minor cases, up to ten years under aggravated circumstances (great extent of damage, commercial perpetration, *i.e.* with intent to obtain a regular criminal income).

- Sec. 168a StGB (Penal Code, BGBl. Nr. 60/1974) - Fraudulent Pyramid Schemes. Initiation, organisation, advertising or commercial promotion of "profit expectation systems", where participants are induced to put money at stake, the promised benefit depending on ongoing recruitment and behaviour of future participants. Punishable by up to six months in jail a fine or up to three months for large damage.

This would apply to most "Get Rich Quick" schemes.

Unlawful Advertising:

The *Gewerbeordnung* (GewO) (Industrial Code, BGBl. Nr. 194/1994) covers the direct marketing trade and contains provisions against junk mail. This law would also apply to junk e-mail. The following is an English translation of sec. 268 *Gewerbeordnung*:

Direct Marketing:

sec. 268 of the Industrial Code 1994, Austrian Federal Law Gazette Nr. 194/1994
(Gewerbeordnung, BGBl. Nr. 194/1994)
"Section 268 - Direct Marketing

(1) Tradesmen who are permitted to perform the direct marketing trade may acquire the data material necessary for their trade from publicly-available sources and in accordance with (2), (5), (6) and (7) through their own investigations and from databases on Customers and interested parties of others.

(2) Tradesmen according to (1) are only allowed to collect data through their own investigations and from databases on customers and interested parties as far as this is necessary:

1. To prepare and carry out mailings for the products and services of others.

2. To organise and mail advertising material for the goods and services offered by others.

3. For their work as intermediaries between owners and users of databases on customers and interested parties (*Listbroking*).

(3) Tradesmen according to (1) are required:

1. To organise mailings in such a way that the origin of the data used to address the mailing can be determined to grant the right of access even after the deletion of the data material.

2. To inform data subjects according to sec. 3 lit. 2 of the Austrian Data Protection Act, Federal Law Gazette Nr. 565/1978 (*Datenschutzgesetz*, BGBl. Nr. 565/1978 idgF) (DSG) about the origin of the data if the data subject requests such information within three month of the mailing. This information is to be given free of charge and in writing, if so requested, based on the identifying characteristics of the mailing supplied by the data subject. The right to access according to sec. 25 of the Austrian Data Protection Act remains unaffected.

(4) Tradesmen according to (1) must delete all data on a given data subject free of charge within four weeks of the data subject's request.

(5) Owners of databases on customers and interested parties may only transmit the following data of data subjects to tradesmen according to (1):

1. Name,
2. Title,
3. Academic degree(s),
4. Address,
5. Date of birth,
6. Job, business branch and individual business,
7. why the data subject is part of this database on customers and interested parties.

(6) Owners of databases on customers and interested parties may only transmit data according to (5) as long as the data subject does not expressly object. If data are collected from the data subject in written form, the right to object must be pointed out expressly and in writing. The objection to the transmission shall have no effect on any contractual relationship to the owner of the database.

(7) The following personal data shall not be collected, processed and transmitted according to (1), (2) and (5) without the express and written consent of the data subject in accordance to sec. 18 p. 1 lit. 1 Data Protection Act (DSG):

1. data revealing racial origin, political opinions or religious or other beliefs, or
2. data concerning health or sexual life, or
3. data revealing previous penal convictions.

(8) Anybody shall have the right not to receive advertising material. The Trade Association for Advertising and Market Communication *(Fachverband Werbung und Marktkommunikation, Wirtschaftkammer Österreich, z.H. Mag. BACHMAYER, Wiedner Hauptstraße 63, 1040 W i e n, AUSTRIA)* shall keep a list on which all people who do not want to receive advertising material must be entered free of charge. This list shall be updated at least four times annually and must be transmitted to all tradesmen according to (1) on request. Tradesmen according to (1) must not mail or distribute any directly addressed mailings to any person on this list, or broker their data. The data in this list may only be used to prevent the mailing of advertising material."

The list of people who do not want direct advertising (sec. 268 p. 8 GewO) is also known as the "Robinson List".

Another applicable law is the *Gesetz gegen unlauteren Wettbewerb* (UWG) (*Unfair Competition Act*, BGBl. Nr. 448/1984). Competitors may sue for damages if they suffer damage due to unfair business practices that distort fair competition. Spreading lies about a competitor or his products is punishable with a fine (sec. 4 UWG) as well as publication of the verdict.

Protection of personal information/privacy

The *Datenschutzgesetz* (DSG) (*Austrian Data Protection Act*, BGBl. Nr. 565/1978) is the most important privacy law in Austria. It grants data subjects the rights of access, rectification and deletion (sec. 25, 26, and 27 DSG) against private data controllers. Furthermore, all data processing involving personal data must be notified to the Data Processing Register (sec. 22 DSG), which assigns a registration number to

each Data Controller. This number must be used in every data transmission (sec. 22 p. 3 DSG); failure to do so may result in a fine.

The DSG also contains two penal provisions, sec. 48 and 49. According to sec. 48 DSG, a person who discloses data that have been entrusted or made accessible to him exclusively because of his profession shall be punished in court with up to one year of imprisonment. According to sec. 49 DSG, anyone illegally causing damage to the rights of others by acquiring automatically processed data shall be liable to punishment by a court of up to one year in prison. There is a court decision which states that abuse of mailbox passwords by a technician who has set these passwords falls under sec. 48 DSG (OLG Wien 21. 11. 1989, 23 Bs 201/89).

The new *Telekommunikationsgesetz* (*Austrian Telecom Act*, BGBl. I Nr. 100/1997) contains two penal provisions, which also apply to e-mail and other telecom services:

- Sec. 102 prohibits recording, monitoring and disclosure of content and is punishable by up to three months in jail or a fine.

- Sec. 103 forbids the telecom operator to falsify, forward incorrectly, modify, suppress, transfer incorrectly or withhold a message from the intended recipient. Punishable by up to three months in jail or a fine.

Other

- Sec. 126a StGB (Penal Code, BGBl. Nr. 60/1974) - Damaging electronically processed data. Applies to anyone who destroys data (not just personal data) or makes data unusable. Punishable by up to five years in extreme cases. This law may be applied to virus programmers.

- Sec. 15 *Suchtgiftgesetz* (SGG) (Drug Act, BGBl. Nr. 234/1951). Publicly advocating drug abuse. Punishable by up to six months in jail or a fine.

- Sec. 56 *Glücksspielgesetz* (Gambling Act, BGBl. Nr. 620/1989) prohibits participation in games of chance outside Austria.

The above statutes are federal laws. The states of the Federal Republic of Austria have their own laws for the protection of minors.

Non-regulatory initiatives

An e-mail hotline for child pornography and hate propaganda exists, see above.

International activities

The work of the EU ("Green Book on the Protection of Minors") should be taken into account, as well as the initiatives of the Council of Europe: "Draft Recommendation on the Portrayal of Violence in the Electronic Media" and "Draft Recommendation on Hate Speech".

Belgium

Application of Existing Criminal Laws

Research has shown that the criminal law provisions concerning paedophilia have sufficiently general coverage to be directly applicable to new media such as the Internet. The diffusion of pornographic material is punishable under Article 383 of the Belgian Criminal Code. Where the acts take place with the presence of minors the sentences are more severe. The Penal Code covers all forms of pornographic material, be it printed matter, pictures, photographs or audio-visual material. The Act of 13 April 1995 inserts a new Article 383a in the Penal Code, punishing not only the provision, sale, distribution, dispatch and production of paedophilic material, but also the mere possession of it. This means that the diffusion of child pornography through a computer network (*e.g.* sending a message via a newsgroup) and storing it on the hard disk of a computer (*e.g.* through downloading Internet information) comes within the field of application of this law. Thus, Belgium believes there is no need for a change in the law as regards material criminal law. There is a problem, however, regarding the constraining force of the provisions when they are applied to international phenomena such as the Internet. If illegal information is found on the Internet which originates in Belgium, then legal proceedings can be instituted when such information comes from outside Belgium. The transfrontier nature of the Internet gives rise to problems with regard to criminal investigation, indictments and legal proceedings. From Belgium's perspective, it is clear that international collaboration is essential to resolve these problems.

International Collaboration

Belgium believes that ongoing efforts to develop technical solutions to these problems must continue. This would include blocking, rating and filtering systems for the content broadcast on the Internet, such as the Platform for Internet Content Selection (PICS). Belgium believes that such technological development must also be placed in a European or international context and that the final objective should be to be able to apply these techniques throughout the entire world. The development of the PICS platform shows that the need exists. PICS technology makes it possible to mark the content of network pages on the basis of a scale indicating the violent or sexual nature of the information. From the Belgian perspective, it quickly becomes apparent that these criteria are based on American standards and cannot be simply taken over "as is" for use in Europe, given the cultural differences. International collaboration for the creation of such systems would create the context necessary for refining the filtering and grading systems so that they can be applied in virtually universal fashion.

A qualified answer must be given to this question. Self-monitoring by individual users may be important up to a certain point and should be promoted by the authorities by means of specific training programmes. However, Belgium does not believe that this measure constitutes an adequate solution to the problems posed by the Internet. As parents attempt to monitor their children's online activities, they may find that they do not have sufficient technical knowledge or that their children can over-ride their technological decisions. In addition, this solution does not do anything to tackle the root of the problem, which is the presence of illegal information on the Internet. Industry self-regulation provides a much better response to this basic problem. From the Belgian perspective, in the final analysis, it is industry which provides access to the Internet and it is at this level that the solutions must be found. The installation or provision of filtering or blocking systems by access providers, for example, would already be a step in the right direction. However, self-regulation does not constitute a complete solution to the problem either. The fact is that it is by definition an initiative taken separately within each country. International collaboration is required to adjust and amplify the different initiatives and thus arrive at a satisfactory solution. It is also

vital that when a self-regulation system is being introduced, account should be taken of the link with the legal framework in force and with the legal services.

Self-monitoring

Advantages:
- Permits an individual approach for each user, taking account of his cultural identity.
- With the aid of the necessary software, self-monitoring is fairly easy.

Disadvantages:
- Does not constitute a basic solution for preventing the diffusion of illegal information via the Internet or other similar networks.
- If the self-monitoring is achieved using grading and filtering systems, technical knowledge is necessary.

Self-regulation

Advantages
- The initiatives come from the industry and can be very effective.
- Prevents excessive intervention by the public authorities, which could have negative economic consequences for the sector.
- Self-regulation permits much more flexible information flows than censuring systems.

Disadvantages
- Self-regulation may be very different from one country to another, depending on government directives and cultural and moral values, which will make international co-operation to find a solution to the problem more difficult.

Canada[78]

Regulation of Content

Policy Framework

The Canadian *Charter of Rights and Freedoms* recognizes freedom of speech as a fundamental right granted to all Canadians (Section 2(b)). Any limitations on freedom of expression must be measured by the Charter's Section 1, which permits only "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." Canada also recognizes its international obligations, *e.g.* Articles 19 and 20 of the *International Covenant on Civil and Political Rights*.

With respect to content issues as listed below, *i.e.* harmful content, defamation, communication of erroneous information, protection of personal information, trade secrets and copyright, Canada approaches Internet content issues in a number of ways.

In response to IHAC recommendations, a policy elaboration process has begun to clarify whether new policies are required with respect to intermediary liability and, as a result, what they would be. The government's recently published study on content-related Internet liability is part of this policy process.

In 1997, Canada has just completed a second phase of revisions to its copyright legislation. It was agreed among all parties and stakeholders that any required revisions dealing with the digital environment and the Internet would be part of a subsequent phase. In 1995, the Society of Composers, Authors and Music Publishers of Canada (SOCAN), on the basis of its role as representative of the composers, lyricists and music publishers with respect to the right to communicate musical works to the public by telecommunication, submitted a proposed tariff to the Copyright Board, an administrative tribunal created under the Copyright Act. If the tariff were approved by the Board, Internet access providers would be required to pay royalties on the basis of the number of subscribers or general revenues. It is under advisement at the Board.

To date, the government and the federal broadcasting and telecommunications regulator, the Canadian Radio-television and Telecommunications Commission, have not instituted any actions relating to content on the Internet.

In its Phase II Conclusions and Recommendations tabled in April 1997, the Information Highway Advisory Council, questioned "the effectiveness of any form of licensing of Internet-based services or the imposition of formal [Canadian] content rules or quotas."

The Internet, as a communications network, comes under the purview of the *Telecommunications Act* and the CRTC. Because facilities-based telecommunications carriers are obligated to provide non-discriminatory access to their networks, the CRTC has the authority, under the *Telecommunications Act*, to limit their financial liability in the provision of services. Canadian carriers, as defined in the *Act*, are the only ones eligible for this treatment.

In August 1996, the government issued a Convergence Policy Statement in order to provide an appropriate policy framework for the convergence of the Canadian broadcasting and telecommunications industries for the provision of facilities and services in a new competitive environment. The Convergence Policy Statement put forward the government's policy objectives and clarified a policy framework to allow cable companies and telephone companies to compete in each other's core markets, subject to the respective rules under the *Broadcasting Act* and the *Telecommunications Act*.

Criminal activities

Obscene material

The Criminal Code defines as obscene material whose dominant characteristic is the undue exploitation of sex, or sex together with crime, horror, cruelty or violence. The work as a whole is subject to a "community standard test". This test involves a consideration of what the community would tolerate others being exposed to on the basis of the degree of harm that may flow from such exposure.

There are three distinct offences:

- Publication of obscene material.
- Distribution of obscene material (including possession for purposes of distribution).

- Knowingly selling or exposing to public view obscene material (or having possession for such purposes).

With respect to publication and distribution, possible defenses may include lack of knowledge, if there were due diligence, reasonable mistake of fact or service of the public good. With respect to the third offence, a possible defense may include lack of "subjective" knowledge of the content and nature of the materials.

Relevant legislation
Subsections 163(1) and 163(2) of the *Criminal Code*
Section 1 and 2(b) of the *Canadian Charter of Rights and Freedoms*
Customs Tariff and *Canada Post Act*

Child pornography. The *Criminal Code* defines child pornography as including any visual representation, whether or not made electronically or mechanically, showing a person who is or is depicted as a minor (under the age of eighteen years) engaged in or depicted as engaged in explicit sexual activity, or having as its dominant characteristic the depiction, for a sexual purpose, of a minor's sexual organs or anal region, or any written material or visual representation advocating or counseling sexual activity with a minor that would be an offence under the *Criminal Code.*

The *Criminal Code* provides for an offence for publication, *i.e.* making, printing, publishing or possessing for purposes of publication, for distribution, including importing, selling, or possessing for purposes of distribution, as well as for simple possession of such material.

Possible defenses in the case of publication and distribution may be the following: service of the public good exclusively; reasonable mistake of fact as to person's age; artistic merit; educational, scientific or medical purposes; due diligence or reasonable care; and lack of subjective knowledge, if required (content test). Insofar as simple possession is concerned, a possible defense may also include the absence of knowledge of such material and of control over where the material is stored.

Relevant legislation
Sections 4(3) and 163.1 of the *Criminal Code*
Section 2(b) of the *Canadian Charter of Rights and Freedoms*
Customs Tariff and *Canada Post Act*

Hate propaganda. The primary legislation dealing with hate propaganda in Canada is the *Criminal Code* although Federal and some provincial human rights statutes also address the issue. The *Broadcasting Act* also contains regulations dealing with this issue.

The *Criminal Code* creates three distinct offences in regard to hate propaganda:

- Advocating or promoting genocide.
- Inciting hatred against any identifiable group by communicating statements in any public place where such incitement is likely to lead to a breach of the peace.
- Willfully promoting hatred against an identifiable group by communicating statements, other than in private conversation.

With respect to the first offence, the Criminal Code does not specify whether offences are limited to a public place or communications other than in private communication. The second offence requires first that statements be communicated in a public place and second that such incitement is likely to lead to a breach of peace. In the case of the third offence, the definition is broader since it applies to all statements "other

than in a private conversation," but more importantly it must be a willful act, which requires specific intent.

The Criminal Code also provides for four special statutory defenses, which an accused may raise if prosecuted for willfully promoting hatred. These are: a) the statements communicated were true; b) the statements expressed in good faith an opinion upon a religious subject; c) the statements were made on a subject of public interest which, on reasonable grounds, are believed to be true; and d) pointing out in good faith, for the purpose of removal, matters tending to produce feelings of hatred.

The Canadian Human Rights Act contains two provisions which deal with hate propaganda. Section 13 makes it a discriminatory practice to repeatedly communicate by telephone any matter that is likely to expose a person to hatred or contempt because they are identifiable on the basis of a prohibited group of discrimination such as race or religion. Section 12 of the Canadian Human Rights Act makes it a discriminatory practice to publicly publish or display a notice, sign, symbol, emblem or other representation that expresses or incites discrimination that, if it were engaged in, would be a discriminatory practice under the Act.

Relevant legislation
Sections 318,319 and 320 of the Criminal Code
Sections 1 and 2b) of the Canadian Charter of Rights and Freedoms
Section 13 and 14 of the Canadian Human Rights Act
Section 14(1) of the Saskatchewan Human Rights Code
CRTC Radio Regulations, 1986; Specialty Services Regulations, 1990; Television Broadcasting Regulations, 1987; and Pay Television Regulations 1990 under the Broadcasting Act
Customs Tariff and Canada Post Act

1.3 Civil liability

Under Canadian law, each person is responsible for statements he or she makes whether it be by post, telegram, facsimile or other mode of telecommunication, in print or electronic media or on the Internet.

There are in Canada two distinct regimes of private law: the civil law of the Province of Quebec and the common law regime applicable in the rest of Canada. Various provincial and federal statutes have also created regimes of civil liability, namely in the area of privacy.

Defamation, libel and harm to reputation

At common law, a defamation action is made up of three elements: a) offending statements made known by someone other than their author; b) the defamation refers to the plaintiff; and c) the statements are false and discredit the plaintiff. The situation is essentially the same under Quebec civil law although the analysis proceeds differently.

Once published, statements are considered to be false, intended to defame, and to inflict damages on the plaintiff. Possible defenses may include: statements were true; they constituted a fair comment; the defendant was protected by a privilege (conditions to be free to make public vary, *e.g.* parliamentarians and journalists); and there was "innocent dissemination." Rules for innocent dissemination require three conditions: there is no knowledge as to the libel contained in the work disseminated; nothing in the work or in circumstances under which it came to the defendant or was disseminated by him ought to have led him to suppose that it contained a libel; the work was disseminated without any negligence.

Relevant legislation
Charter of Human Rights and Freedom, Section 4.
Quebec's Civil Code, Article 3.

Communication of erroneous information. At common law and in the Quebec Civil Code, prudence and diligence are required of information providers, especially if they are objects of trust. In cases where information is provided by professional data banks, Canadian courts have demonstrated a tendency to be more severe in imposing liability standards, even going so far as to impose no-fault liability.

Relevant legislation
Quebec's Civil Code, Article 1457.

Violation of secrecy. It is well established, both under common law and the Quebec Civil Code, that violation of secrecy, whether it occurs on the Internet or through more traditional means, is subject to sanction.

Relevant legislation
Quebec's Civil Code, Article 1457 and 1612.

Protection of personal information. Personal information is any information about an identifiable individual.

There are data protection laws for the public sector in most provinces. Only the province of Quebec has data protection laws which apply to the private sector at this time. In addition, the federal government has announced its intention to put in place legislation to cover the federally regulated private sector.

All laws are based, more or less, on the 1980 OECD Guidelines on the Protection of Personal Information and Transborder Data Flows. They cover the collection, use and disclosure of personal information and usually provide for a right of access and correction and a degree of oversight by a data commissioner.

Canada adopted the OECD Guidelines in 1983 and since then some companies and sectors have written self-regulatory privacy codes. Canada has developed a unique standards-based approach to data protection with the development and adoption of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information which was adopted by the Standards Council of Canada as a National Standard in 1996. It is built on a consensus among the public sector, various industries, advocacy groups, unions and other general interest groups.

Relevant legislation (applicable to the private sector)
Quebec's R.S.Q., c. P-39.1.

1.4 Copyright

As a signatory to the Berne Convention and to the World Trade Organization's (WTO) Trade-Related Intellectual Property (TRIPs) Agreement, Canada's copyright laws are in many cases similar to those of other signatory countries. This brief summary does not purport to reflect key similarities or dissimilarities between the Canadian legislative framework and those of other OECD countries.

Copyright protection in Canada is provided pursuant to the Copyright Act. The Act affords protection to original works falling within four different categories: literary, dramatic, musical and artistic. Within each of these four main categories are a number of subcategories, *e.g.* computer programmes are protected as literary works. Compilations of different categories of works take on the character of their most substantial

constituent work. However, this does not in any way affect the rights attached to any of the constituent works.

The Act confers a "bundle of rights," which relate to acts that only the rights holder may carry out or authorise. Among the most important economic rights in the Internet context are the right to produce or reproduce the work, the right to communicate the work to the public by telecommunication and the right to publish the work. In addition to these economic rights, the author has certain moral rights, *i.e.* the right to the integrity of the work and the right to be identified or not identified with the work,

The Act attempts to limit overlapping rights. For instance, it specifically provides that the communication of a work to the public by telecommunication does not, of itself, constitute a performance in public of that work. (Both public performance and communication to the public by telecommunication are acts falling within the exclusive rights conferred by the Act). Similarly, neither public performance nor communication to the public by telecommunication, of themselves, constitutes publication.

The Act protects a work only if the author meets certain residency requirements or first publishes his/her work in a country with which Canada has a copyright treaty. For most works, the duration of protection is fifty years plus the life of the author.

Except in respect of certain types of works, the initial owner of copyright is the author, who may assign all or part of the copyright, either generally or subject to territorial, time, or use limitations, and to several different persons. The ability to assign or license rights, either partially or in whole, has been important for the development of collective societies, which administer particular rights on behalf of a large number of authors. Note, however, that authors may not assign their moral rights, though they may waive them.

In addition to the rights conferred on authors (and their assignees), the Act also confers more limited rights on performers and sound recording makers to carry out or authorise certain acts. In respect of performers, these acts include the fixation of their performances as well as the reproduction of any unauthorised fixations. They also include the communication to the public by telecommunication (usually by way of broadcasting) of unfixed performances. Makers of sound recordings have exclusive rights in respect of the rental, publication and reproduction of their sound recordings.

A new law amending the Copyright Act has been passed, which will entitle performers and sound recording makers to receive royalties in respect of the communication to the public by telecommunication (usually by way of broadcasting) and the performance in public of their published sound recordings. In addition to sound recording makers, performers will also have an exclusive rental right in respect of sound recordings which embody their performances. Moreover, there is now statutory recognition of the right of performers who have negotiated contractual remuneration rights in respect of the reproduction, performance in public or communication to the public by telecommunication of performances embodied in cinematographic works, to obtain payment from certain parties (who are not necessarily privy to the contract). Those parts of the amending law, which confer these new rights will be in force as of 1 September 1997.

Infringement occurs whenever a person does something, without the rights holder's authorisation, which only the rights holder has the right to do. As copyright is considered a property right, there is no defense of innocent or unintentional infringement. (On the other hand, remedies may be limited accordingly.) There are, however, certain exceptions, such as the right to deal fairly with a work for the purposes of private study, review, etc.

The case law in Canada is that, in order to "authorise," a person must sanction, approve or countenance something more than the mere use of equipment that might possibly be used to infringe copyright.

Indirect infringement generally involves commercial dealings with infringing copies. Since they affect the rights holder's ability to exploit his/her work, they are subject to legal sanction. Such dealings include: the sale or lease of a work or exposure or offer for sale or hire; the distribution for purposes of trade or to an extent that would affect prejudicially the owner of copyright; the exhibition of a work in public by way of trade; or the importation of the work into Canada for sale or hire. In the case of indirect infringement, there must be knowledge on the part of the infringer that the work infringes copyright or would do so if copies had been made in Canada. Of note, "knowledge," for the purposes of indirect infringement, is measured against an objective standard and may be imputed if the lack of knowledge was unreasonable in the circumstances.

Section 3(1.3) of the Copyright Act provides that a person does not communicate a work to the public where the person's "only act in respect of the communication of a work to the public consists of providing the means of telecommunication necessary for another person to so communicate the work". This provision applies solely to the activity described and not to any particular class or category of person.

Non-regulatory Initiatives

The government has been in close communication with the private sector regarding many aspects of liability on the Internet. With a view to assisting industry, a recent Statistics Canada survey of Internet service providers in Canada was conducted. ISPs were asked to indicate the significance of the "threat of litigation" as a barrier to growth and whether they had received customer complaints regarding offensive content.

The factor "threat of litigation" refers to fears that the company could be taken to court for possessing or providing access to materials that are considered illegal under the Criminal Code (*e.g.* child pornography, hate literature), the Copyright Act and other legislation, *e.g.* trademarks. Respondents were asked to rate, on a scale of one to five, how much of a barrier the threat of litigation was to their growth. It was rated quite low, with an average response of only 1.85, indicating a general lack of concern on the part of ISPs. Yet, actions by trade associations, such as the Canadian Association of Internet Providers, to adopt a model code of conduct for its members, express industry concerns about this issue.

Several factors can explain the low results: ignorance about potential liability regarding illegal materials; a feeling of confidence that since these matters have not been tested in Canadian courts, as they have in the United States, they will not be prosecuted; and/or a reflection of the libertarian, new frontier mentality of the Internet culture. As noted in the Industry Canada publication, "The Cyberspace is Not a No-law Land"; there is a lack of case law on such matters, which could affect the responses.

Part of the low concern with respect to liability issues on the Internet may be the low incidence of actual complaints and the proactive strategy many ISPs have adopted to stave them off. Across Canada, 32.4 per cent stated that they had received complaints. The companies were asked what their business practices were in response to offensive content complaints. Of the respondents surveyed, 82 per cent said that they had practices to deal with complaints, such as:

- 42 per cent said that they would "block access to the offending site/newsgroup".
- 61 per cent said that they would "remove the offensive material from [their] server".
- 50 per cent said that they would "discontinue the subscription of the offender".
- 52 per cent said that they would "consult with law enforcement officials".
- 52 per cent said that they would "establish a code of conduct for users."

In an "other" category, ISPs also said that they would "refer customers to blocking software, investigate, and advise customers of their responsibilities".

Overall, ISPs did not consider litigation to be a threat. The study also found that many had not received complaints about offensive or illegal materials. Those that had received complaints engaged in a variety of proactive approaches to combat potential problems.

In general, the federal government does not operate community education programmes on offensive content, but does support and promote them. The Media Awareness Network, linked to Industry Canada's SchoolNet site, is a national online organisation dedicated to media education and media issues affecting children and youth. It provides both a clearinghouse of information and an interactive network for the sharing of ideas and initiatives.

Studies in Canada

"Building the Information Society: Moving Canada into the 21st Century", (May 1996), Government of Canada.

"Connection, Community, Content: The Challenge of the Information Highway, Final Report of the Information Highway Advisory Council" (September 1995), Information Highway Advisory Council.

"Illegal and Offensive Content on the Information Highway" (June 1995), a background paper prepared by Gareth Sansom, Spectrum, Information Technologies and Telecommunications Sector (SITT), Industry Canada.

Preparing Canada for a Digital World, Information Highway Advisory Council, Phase II Conclusions and Recommendations (April 1997) Information Highway Advisory Council.

The Cyberspace is not a "No Law Land" (February 1997), a study of the issues of liability for content circulating on the Internet prepared for Industry Canada by Michel Racicot, Mark S. Hayes, Alec R. Szibbo and Pierre Trudel.

Undue Exploitation of Violence (March 1996), a consultation paper released by the Department of Justice, Canada.

As well as:
The Canadian Association of Internet Providers (CAIP)'s Code of Conduct.

The Canadian Standard Association (CSA)'s Standard Model Code for the Protection of Personal Information.

Industry Initiatives

The Canadian Association of Internet Providers (CAIP) has adopted a Code of Conduct, a voluntary code, which was previously tabled with the Secretariat, together with the Canadian Standards Association (CSA)'s Standard Model Code for the Protection of Personal Information (see above the section on protection of personal information). CAIP has also made itself available to develop an international code with industry representatives from other OECD countries.

As indicated in the results of the survey mentioned above, industry resorts to a number of initiatives to assist in addressing liability on the Internet. Hotlines are provided, *inter alia*, to assist commercial and individual subscribers in becoming more aware of technological solutions, such as filtering software, with a view to deciding what information they wish to obtain or avoid.

Some of these products work through the rating of sites by third parties utilising agreed standards, which have been established through an independent federation of Internet company representatives. Others function on the basis of word recognition. Closed proprietary systems for child-safe zones are also used by companies and organisations. Firewalls may also serve as content filters and be set to filter specific addresses of Web sites, chat lines and Usenet newsgroups.

Many of the ISPs also offer sessions to build greater awareness of how to avoid and deal with offensive content on the Internet. This again is part of their business strategy to create an acceptable Internet environment for their customers. A number of schools, as part of teaching children how to use the Internet, make class time available for "street-proofing" children on the Information Highway.

International Activities

Canada considers that international co-operation is vital with respect to the information highway. With respect to substantive law, liability, jurisdiction and enforcement, it participates in various intergovernmental forums that focus on activities it wishes to curtail, such as obscenity, child pornography, hate propaganda, defamation, and communication of erroneous information, and those it wishes to encourage, such as protection of personal information and trade secrets, as well as copyright.

The Information Highway is important to help achieve Canada's national social and economic policy objectives. The federal government and the Information Highway Advisory Council (IHAC) have done considerable policy work. Created in 1994, the IHAC is a private-sector group established to advise the federal government on carriage and content issues, including those related to the Internet, copyright, information controls and privacy. As part of its response to IHAC recommendations, the government recently published a study on content-related Internet liability.

Finland

Introduction

A recent report on freedom of speech in mass communications has tried to address the question of Internet content by proposing an online framework based on traceability of messages and storage of Internet publications. There is public discussion of its negative effects on the development of the information society. There is also a discussion paper entitled "Privacy and freedom of speech on information networks" prepared by a Working Group on Information Networks which stresses online content and conduct issues. Thus far, none of this activity has resulted in any regulatory measures.

The Finnish Government believes the development of the information society should not be hindered by heavy liability and economic burdens or by constant regulatory activities. This might include the compulsory use of filtering software -- which the Government views as counterproductive -- or compulsory use of labelling techniques -- which is considered too expensive and impossible to use effectively because of divergent cultures and values world-wide. Finland believes that the question of harmful content on the Internet (content which is not illegal but might not be suitable for certain categories of users) should primarily be dealt with through educational measures. The Finnish Government believes

above all that the creation of a viable economic online environment is in the interest of the market and that public administration should interfere only if it is absolutely necessary.

The Finnish government would like, however, to see Finnish Internet service providers create a self-regulatory mechanism and has made an initiative to that end. The initiative is in line with EU recommendations and the Finnish government's basic approach of liberalism and trust in market forces. The extent of co-operation would be decided by those concerned.

Regulation of content

Finland believes that Internet, which is only a new means of accessing and providing information, is subject to the same laws and regulations as the off-line world. Therefore, the Criminal Law in force is applicable to Internet content issues. Similarly, Internet content is subject to civil liability.

Industry initiatives

On the commercial side, the principal advertising agencies and professional content providers in Finland have created an association intended to establish common rules on advertising online and on the follow-up of the efficiency of the ads.

International activities

Finland sees that the work undertaken in European Union and in the Council of Europe should be taken into account.

France

Introduction

French legislation applicable to online services is partly shaped by the nature of the services offered. It would therefore be advisable to learn more about the type of services offered on the Internet, even if the diversity and rapid evolution of such services makes any attempt to classify them inconsistent if not meaningless. In this respect, the distinction between Web-related services and electronic mail is taken in France as a fundamental dividing line between broadcast communications and private correspondence. Nonetheless, the legal status of a number of services, notably forums, remains unclear.

With regard to services, it would be useful to distinguish between: Internet servers, including not only conventional technologies (http, ftp) but also the more recent "push" servers; electronic mail; forums; and online discussions (Internet Relay Chat).

It is hard to distinguish between actors who perform several different service functions. It is for this reason that defining service functions would seem to be a second line of approach worth pursuing in view of the implications in terms of existing legislation and particularly in terms of liability. It was decided that the definitions should relate to functions rather than to individual types of actor on the grounds that, in providing services, actors may have combine several different functions. In this respect, observation of how services are provided in practice allows a distinction to be drawn between the following functions:

- Infrastructure operator, which for an IP network operator consists in providing subscribers with a connection to other operators at the same grade.

- Access provider which for an operator consists in marketing the service and providing subscribers with a connection between the subscribers PCs and an IP infrastructure.

- Service provider, which for an operator consists in acting as an intermediary between a supplier of information content and the service provider's subscriber. Note that this does not match the standard definition of an ISP, a concept which combines the function of service provider with that of an operator providing a range of services.

- Operator providing a range of services, which for the operator consists in assembling several services offered by content suppliers into a single commercial package.

- Host provider, which consists in the technical management of the information resources connected to the Internet and in making these resources available to subscribers.

- Content publisher, that is to say the publication of information content available via the Internet. It should be noted that the actors covered by the publishing function also include individuals.

Regulation of Content

France, like other countries, is concerned about certain undesirable developments which constitute the negative aspect of Internet growth. Although there is no legal vacuum in this field in French legislation, there is nevertheless a need to adapt some of the existing rules in order to stop the dissemination of illicit and harmful content as soon as possible. This action can be fully implemented only in the framework of international co-operation.

The general approach adopted by the French authorities to new services is as follows. Article 2 of the amended French Act of 30 September 1986 on freedom of communication stipulates that "audiovisual communication is understood as any provision to the public or to categories of public by a telecommunications process of signs, signals, texts, images, sounds or messages of any nature which are not of the character of private correspondence". Thus what characterises communications services in the terms of French law is the fact that they target a "public" or "category of public", *i.e.* a number of undifferentiated individuals. The definition given in Article 2 of the amended Act of 30 September 1986 includes Internet services made available to the public such as Web pages or certain newsgroups.

In this context, a distinction should be made between what belongs to the category of private correspondence, which is protected by secrecy of correspondence, and what belongs to the category of public communication where freedom of expression, a fundamental principle, nevertheless has to be reconciled with the respect of certain imperatives of general interest, such as the protection of public order.

In addition, the characteristics of the services and messages should take precedence over their method of transmission, *i.e.* the "carrier medium". In the communications field, where technological progress is extremely rapid, it is essential that the legal rules should be "technologically" neutral.

On the legislation in force and practices

The right to communication applies on the Internet. Article 1 of the Act of 30 September 1986 in fact stipulates that communication is free. This freedom stems from freedom of expression, one of the foundation stones of democratic societies consecrated by the *Declaration of Human Rights* and by the European Convention on Human Rights. Therefore, limitations formulated out of concern for public order or the protection of persons authorise intervention on the content by the authorities only after the event and not before.

As a result, a simple declaration regime applies to online services, which are subject to declaration to the State Prosecutor in application of Article 43 of the amended Act of 30 September 1986.

In addition, the criminal law makes it possible to institute proceedings against illicit acts committed on the network. In criminal matters, French law is applicable in the case of offences committed on the territory of the Republic, Article 113-2 of the Penal Code stating that the offence is deemed to be committed in France if one of its constitutive acts takes place on this territory. As a result, such acts can be prosecuted in French courts.

New legislation

In the context of the adoption of the Communications Act of 26 July 1996, the French legislature introduced a new Article 43-1 to the amended Act of 30 September 1986, requiring any person whose activity is to provide a connection service to one or more of the audiovisual communications services mentioned in paragraph 1 of Article 43 of the said Act (*i.e.* declared services such as online services) has to offer clients a technical means of restricting access to certain services and selecting them.

It is therefore appropriate to develop filtering systems integrating European concepts. In the light of existing filtering systems such as PICS and others, France believes it is necessary to determine common standardisation elements for the labelling of content. In any event, these elements must permit the respect of the cultural specificities proper to each State.

France also believes it is necessary to promote the use of encryption systems which constitute a means of protecting the confidentiality of correspondence. In the Act of 26 July 1996 France introduced regulations intended to reconcile the protection of correspondence with the protection of public order. It appeared necessary in fact to permit the introduction of powerful systems for protecting the secrecy of correspondence, a precondition for the development of electronic mail and the growing use of computerised transactions by administrations and enterprises. However, as part of their mission to maintain order and public safety, the legal and police authorities may need to access communications or stored data files.

The Act of 26 July 1996 in fact introduces the principle of the confidential third party, who holds keys that he manages for his clients and which he must hand over to the legal authorities in the case of investigations. This system also makes it possible to reconcile the protection of confidentiality and interception for legal or security reasons.

Protection of minors

- Article 227-24 of the new Penal Code prohibits the "production, carriage or dissemination, by any means and through any medium whatsoever, of a message of a violent or pornographic nature or one that offends human dignity, as well as commercial trade in such a message";

- Article 227-23 prohibits "the production, recording or transmission, with a view to their dissemination, of images of a pornographic nature depicting minors"; and

- In addition, a series of texts exist which describe parental approval, contractual rights, etc.

Protection of privacy

- Protection of privacy is primarily provided by Article 9 of the Civil Code which states that "everyone is entitled to have their privacy respected", as well as Articles 226-1, *et seq.*, of the new Penal Code which prohibit the deliberate violation of the privacy of others through the production, recording and transmission of the words or image of a person in a private context without the permission of that person.

- In addition, the Act on Information Technology and Freedom of 6 January 1978 addresses the problem arising from the use of personal data included in files by making it an offence to divulge or to have allowed to be divulged, either recklessly or through negligence, personal data that might damage the reputation or violate the privacy of the individual concerned.

- Furthermore, the confidentiality of correspondence is protected under Articles L 41 and L 42 of the Post and Telecommunications Code which provides for penal action in the event of violation.

Protection of the individual

The Act on the Freedom of the Press of 29 July 1881 makes provision for a number of specific offences designed to reconcile the freedom of communication with the protection of individual liberties and the safeguard of public order. These crimes and misdemeanours, which might be committed by any means of communication ("any written, spoken or visual medium") at the public's disposal, are as follows: incitement to racial discrimination, hatred or violence (Act of 1 July 1972 as amended by the Act of 13 July 1990); offences against society; offences against the person (slander, libel); offences against heads of State; distribution of proscribed publications (notices of criminal charges prior to their release to the public, etc.).

Self-regulation

Concomitant with the legislative measures adopted, a study was also undertaken by Internet actors to promote self-regulation, an initiative encouraged by the public authorities in France. The fact is that it is essential for operators and users to agree on a certain number of standards of conduct. Users have already developed a "Netiquette" intended to facilitate the proper use of the network through unwritten rules of behaviour (no advertising, no redundant questions in forums, etc.). In addition, certain contracts between access providers and their clients include ethical conditions. The drafting of codes of conduct fits into this logic by defining standards of good behaviour to be respected by the different actors. Self-regulation also has the advantage that judicial action can be limited to the most serious offences. However, its implementation requires the agreement of all the actors; this is becoming increasingly difficult to obtain given the divergent interests involved.

At the end of last year a working group was set up in France, bringing together Internet actors to draw up a code of conduct. This work led to the production of a draft Charter intended to ensure the respect of the following broad principles:

- Human dignity, protection of minors and public order.
- Fundamental rights and freedoms.
- Consumer protection.

These broad principles may serve as the basis for any international reflection on the implementation of self-regulation.

In addition, it would appear necessary to clarify the liability regime for actors in order to ensure the legal security necessary for the development of these services. In France, projects currently being studied envisage introducing an Article 43-2 to the Act of 30 September 1986 which would provide for exoneration from criminal liability of access providers for offences resulting from the content of messages transmitted by a communications service, unless it is established that they have knowingly committed the offence or participated in it. It should be pointed out that this exoneration applies only for the provision of technical services. These proposals are intended to take account of the characteristics of online services. The fact is that technical service suppliers providing access to the Internet do not interfere, as simple carriers, with the content of the services and do not control it. A parallel can be drawn here with France Telecom, the Court of Cassation having exonerated it from liability on the basis of the neutrality of the carrier of messages in a judgement of 17 November 1992.

International co-operation

The free circulation of information and the disappearance of international frontiers are causing certain difficulties, particularly with respect to the determination of the law applicable to servers and works of a transnational nature. This problem is particularly acute where content originating in a State where it is not actionable by law is actionable in another.

Obstacles to the application of existing law

The application of criminal law comes up against two major difficulties: one stems from the identification of the author (anonymity), and the other is connected with establishment of the offences, in view of the transitory nature of the messages disseminated.

The confusion of roles between the different Internet actors (access providers, infrastructures, services, hosts, users, etc.) does nothing to help determination of liability. Furthermore, when the site is outside France, the investigations necessary to establish liability and the enforcement of the penalty require acts of international co-operation (interrogatory letters, extradition) which prevent or make difficult the instigation of proceedings. International co-operation is based in fact on the principle of double incrimination (it is necessary for the act to be punishable in both the claimant State and the State called upon).

European and international initiatives

France believes that the proposal aimed at encouraging the co-ordination of self-regulation codes and charters should be supported. Legal co-operation could be dealt with in the context of the European Union

in the same way as the joint actions undertaken with respect to the fight against forced prostitution and the sexual exploitation of children.

European initiatives can also be enriched by the discussions carried out under the aegis of the OECD. These could be concerned in particular with questions relating to evidence, the identification of authors and anonymous rewriters.

Lastly, on questions connected with conflicting legislation and the determination of the applicable law, the OECD could be an appropriate body for discussion since the main countries where sites are located are Members. The initiatives required to establish international co-operation should be determined on the basis of the responses of the different States, their approaches and their expectations.

Identification of common values

France, for its part, is continuing its reflection on the necessary, but insufficient, development of self-regulation. This should lead to the establishment of a code of conduct recognised by all actors. At the international level, it is important to decide in advance the way in which international co-operation will be implemented before identifying common values. This might include the respect of human dignity, the protection of minors, the fight against racism and the fight against revisionism.

Germany

Information and Communication Services Act (IuKDG) - Brief Outline

The German Bundestag passed the Information and Communication Services Act *(*IuKDG) on 13 June 1997. The IuKDG entered into force on 1 August 1997 (with the exception of Art. 7: 1 January 1998).

The IuKDG subsumes the legal areas that need regulation at the present time under a total of 11 articles:

- Article 1: Teleservices Act - *Teledienstegesetz*
- Article 2: Teleservices Data Protection Act - *Teledienstedatenschutzgesetz*
- Article 3: Act on Digital Signature - *Gesetz zur digitalen Signatur*
- Article 4: Amendment of the Penal Code - *Strafgesetzbuch*
- Article 5: Amendment of the Administrative Offences Act - *Ordnungswidrigkeiten-gesetz*
- Article 6: Amendment of the Act on the Dissemination of Publications Morally Harmful to Youth - *Gesetz über die Verbreitung jugendgefährdender Schriften*
- Article 7: Amendment of the Copyright Act - *Urheberrechtsgesetz*
- Article 8: Amendment of the Price Indication Act - *Preisangabengesetz*
- Article 9: Amendment of the Price Indication Ordinance - *Preisangaben- verordnung*

- Article 10: Return to Uniform Order of Ordinance - *Rückkehr zum einheitlichen Verordnungsrang*

- Article 11: Entry into force

As regards the implementation of the IuKDG in entrepreneurial practice, the new provisions in Article 1 (Teleservices Act), Article 2 (Teleservices Data Protection Act), Article 3 (Digital Signature Act), and the additional provisions governing the protection of young persons are of particular significance.

This "Multimedia Law" is the first general regulatory framework pertaining to the information society in Germany. It is the first law to include--in addition to amendments to existing laws--provisions governing the responsibility of service providers (for example, on the Internet), digital signatures and data protection for the new services. The law thereby provides legal and planning security and creates a sound basis for electronic commerce. The law thus takes into account the recommendations issued by the Council for Research, Technology and Innovation (Technology Council), the suggestions made by the "Petersberg Kreis" as well as the results produced by the *Bund-Länder* Working Group on Multimedia, and implements the options suggested by the Federal Government's report on *Info 2000 - Germany's transition towards the information society*. In its report, the Technology Council identified an acute need for action to establish, to the extent necessary, uniform, adequate conditions for the new information and communication services, and recommended relevant regulations.

The IuKDG is breaking new ground. This applies above all to the provisions governing the responsibility of providers, area-specific data protection and digital signatures. Such provisions will help initiate and promote innovative developments in the legal sphere and in the field of new technologies, thus making an important contribution to broad-based acceptance of the new services and at the same time setting the stage for the development of guiding principles for international discussion.

Future developments in the field of new services and the experience gained with IuKDG need to be watched carefully, so that any adjustments and amendments to the legal framework that may become necessary can be initiated in a suitable form.

Italy

In Italy, the review of Internet content issues covers many aspects. There is an effort by the Parliament to gradually upgrade Italian laws, which at present are related to the following:

- Messages instigating hatred and racial discrimination: this offence is under Art. 3 of Law No. 654 of 13 October 1973, as amended by Art. 1 of Decree-law of 26 April 1993 No. 122, converted into Law No. 205 of 25 June 1993.

- Messages of defamatory nature: Art 595 of the Criminal Code.

- Messages/notices concerning prostitution: Art. 3 No. 8 and Art. 4 of Law of 20 February 1958 No. 75.

- Diffusion of access codes to data processing or telematic systems or networks: Art. 615 quater of the Criminal Code.

- Transmission of unlawfully copied software: Arts. 171 and 171bis of Royal Decree No. 633 of 1941 as amended by Legislative Decree No. 518 of 1992.

- Diffusion of virus programmes: Art. 615 quinquies of the Criminal Code.

- Obscene publications and performances: Art. 582 of the Criminal Code.

- Offences related to political or military espionage and to information the divulgence of which is prohibited by law: Arts. 256, 257, 258 of the Criminal Code; disclosure of State secrets: Art. 263 of the Criminal Code; disclosure of information divulgence of which is prohibited by law: Art. 282 of the Criminal Code.

- Instigation of delinquency and apologia for the commission of crimes: Art. 414 of the Criminal Code.

- Threats: Art. 612 of the Criminal Code.

- Protection of public e-mail service: Decree of 7 August 1990 No. 260.

- Responsibility of information providers on the legality of the information sent into the public telecommunication network: Art. 15 of the Decree of the President of the Republic of 4 September 1995 No. 420.

- Responsibility of audiotel and videotel information providers: Art. 18 of decree of 13 July 1995 No. 385.

- Protection of personal data on telematic networks: Art. 1 item 2(n) of Law of 31 December 1996 No. 676.

In addition to the above-cited laws, the following initiatives are under study:

- Chamber of Deputies: proposal from the Parliament No. 263, 2265, 2930, 1105 in order to combat the sexual exploitation of minors, through the addition of a new article (604 bis) to the Criminal Code.

- Senate: proposal from the Parliament No. 1820 and 2018 on the sexual exploitation of minors.

- The commission of the Justice of the Chamber has recently elaborated a co-ordinated text to combat the pornography of minors also on telematic networks.

Excerpt from Act No. 269 of 3 August 1998, "Norms against the exploitation of minors for purposes of prostitution, pornography and sexual tourism as new forms of slavery":

Article 3 (Child pornography)
I. After Article 600-bis of the Criminal Code, introduced by Article 2, para 1, of this Act, the following is inserted:

"Article 600-ter (Child pornography). Whoever exploits minors under 18 years of age for the purpose of producing pornographic performances or material shall be punished with six to twelve years imprisonment and with a fine of LIT 50-500 million.

The same applies to people trading in pornography as under para 1.
Whoever, beyond the conditions contemplated under §1-2, by any means (including telematics) distributes, divulges, or advertises pornography as under §1, or distributes/divulges information or messages directed to soliciting or exploiting sexually minors under 18 years of age, shall be punished with one to five years imprisonment and with a fine of LIT 5-100 million.
Whoever, beyond the conditions contemplated under §1-2-3, consciously gives or sells pornography featuring minors under 18 years of age, shall be punished with imprisonment of up to three years or with a fine of LIT 3-10 million ."

Article 4 (*Possession of pornography*)
I. After Article 600-*ter* of the Criminal Code, introduced by Article 3 of this Act, the following is inserted:

"Article 600-*quater* - (Possession of pornography). Whoever, beyond the conditions contemplated under Article 600-*ter*, consciously obtains, or disposes of, pornography produced by exploitation of minors under 18 years of age, shall be punished with imprisonment of up to three years or with a fine of no less than LIT 3 million."

Article 10 (Perpetration abroad)
I. Article 604 of the Criminal Code is replaced by the following:

"Article 604 (Perpetration abroad). Provisions under this section, as well as those under Articles 609-*bis*, 609-*quater*, 609-*quinquies*, apply also when the crime is perpetrated abroad by an Italian citizen or to the detriment of an Italian citizen, or by a foreign citizen in association with an Italian citizen. In the latter case, the foreign citizen is punishable when the maximum penalty foreseen for the relevant crime is imprisonment of no less than five years, when so requested by the Ministry of Justice."

Article 11 (Mandatory arrest in the act of the crime)
I. In Article 380, para 2, letter d), of Criminal Procedure Code, after the words "article 600" the following is inserted:

", crime of juvenile prostitution as under Article 600-*bis*, para 1, crime of juvenile pornography as under article 600-*ter*, para 1-2, and crime of tourist initiatives directed to the exploitation of juvenile prostitution as under article 600-*quinquies.*"

Korea

Background

As of 30 April 1997, there are 16 Internet service providers (ISPs) in Korea and 86 805 host computers are in service, providing services to about 1 860 000 subscribers.

Existing Legislation and Enforcement

Those who distribute pornographic materials online shall be imprisoned for up to one year or fined 10 million won (about $US 11 000) under the Telecommunications Basic Act.

Article 53 of the Telecommunications Business Act enables the Minister of Information and Communication to reject, suspend, or limit the activities by telecommunications service providers,

including ISPs, when they are involved in the dissemination of indecent materials related to crime, treason, or behaviour that undermines public order and security.

According to the Article 14 of the Law on Punishment of Sex Crimes and Protection of Victims, the person who transmits sexually indecent materials by electronic means will be punished when the victim of the offence reports to the authorities the transmission and the consequent damage inflicted on him or her.

The Information Communications Ethics Committee (ICEC)

The ICEC has been established in Korea to prevent the distribution of indecent materials via electronic media and to promote the proper use of information. The ICEC consists of 13 civil representatives from various professions and fields, who are appointed by the Minister of Information and Communication.

The ICEC has been undertaking a broad range of activities including:

- Setting out ethics code for service providers including ISPs.
- Reviewing of information on audio and video services that are being distributed for the purpose of public use, and requesting ISPs to prevent the distribution of unethical materials.
- Operating the hotline for handling suggestions and reports from the public.
- Campaigning for promoting positive and desirable "information culture".

Still, it is very hard to control the dissemination of indecent materials coming from outside Korea over the Internet. That is why the ICEC called on ISPs to establish voluntary regulations. Having accepted the request of the ICEC, ISPs voluntarily block access to some Web sites where indecent materials are posted. About 20 Web sites containing pornography have been subject to this voluntary blocking procedure. The ISPs, however, are experiencing difficulties in following the requests from ICEC because of the rapid increase of Web sites and the frequent changes in Internet addresses of the sites with indecent materials.

The Code of Conduct of the Internet Service Providers Association Republic of Korea

(Enacted on 29 April 1997)

As the leaders to the information and communication services in the information society, we duly swear that we shall carry out the responsibilities and duties of promotion of information culture and declare the Code of Conduct as follows:

- As Internet Service Providers Association (ISPA) members, we shall contribute to social progress and national prosperity by proudly providing sound and desirable information online.

- We shall promote an environment to help a free flow of healthy information and communication on the basis of social norms and ethics.

- We shall do our best to improve the quality of life by providing quality information.

- We shall regulate voluntarily illegal or harmful information online and serve the public interest and social good.

- We shall help preserve social order in the information society by honouring human rights and privacy, and protecting intellectual property rights.

- We shall take a leading role in promoting information culture by encouraging constructive critiques and co-operation among the members.

- We shall promote a sound information culture world-wide and develop world markets through fair competition.

- We shall try our best to carry out the duties and responsibilities as members of the online community by observing the rules, regulations and the code of ethics in information and communication.

United Kingdom[79]

Government Regulation

It has been the experience of the United Kingdom that the vast majority of reported material appears in the United Kingdom as newsgroup articles, which UK ISPs are able to remove from their news feeds, whatever the origin of the material. Material on UK-hosted Web sites is also able to be dealt with effectively, leaving only a small number of complaints about material on overseas-hosted Web sites which can only be addressed through international co-operation, whether through existing police channels or potentially via the IWF's overseas equivalents. It is particularly in this last context that international co-operation has a major role to play.

UK experience has shown that co-operation and partnership between police and industry can benefit everyone. With the assistance of ISPs and others the police can better trace and deal with originators and have illegal material removed. With sensitive legislation/police action, ISPs can assist police investigations without the threat of prosecution for holding material which they are incapable of monitoring at reasonable cost. Self-regulation with co-operation between government, police and industry can thus be a highly effective approach.

It must be remembered that all this is of course reactive--illegal content still appears for a short time and users may come across it--which underlines the importance of encouraging the development and widespread take-up of filtering and rating technologies.

The Internet is not a legal vacuum; for example in the United Kingdom, existing law applies to the electronic online environment in the same way as it does off-line. This has in some cases required some updating of existing law: for example, the Obscene Publications Act 1956 was amended in 1994 so that "publication" now explicitly includes the transmission of electronically stored information. The Protection of Children Act 1978, which contains provisions against child pornography, was similarly amended to apply to computer-generated "pseudo-photographs". Most law, however, is technology-neutral. Existing national law is thus applicable to content and activities across all media. This is fundamental in ensuring that technological developments do not outstrip the law's capacity to regulate them. The Internet does however present new issues of enforcement and responsibility, not least because of its inherently global nature.

The UK Government, police and the Internet industry began discussions in September 1996, with a view to developing a framework for dealing with these issues. The result is the industry-led and industry-funded

"Internet Watch" (IWF) framework. The framework was put forward by the two leading trade associations in the United Kingdom, the Internet Service Providers Association (ISPA) and the London Internet Exchange (LINX), supported by the UK Government and the police, and facilitated by the DTI.

Six months after its inception, IWF has delivered all that was expected of it in the starting phase, and is making good progress towards achieving the longer-term objectives set for it in the initial discussions. The UK police have emphasised their satisfaction with the framework, and it retains the support of UK Internet Service Providers (ISPs). Experience gained over the first six months of its operation has proven the benefits of self-regulation, in the expert technical knowledge which ISPs can bring to bear on the problem of upholding existing law on the Internet, and hence in its flexibility. The fact that IWF is based on voluntary action by service providers does not, however, mean that the framework lacks "teeth". ISPs have a clear liability under existing UK law for illegal material hosted on their servers, once they are informed of its existence. In effect, once alerted to illegal material or activity on their servers, ISPs will be liable as accessories if they fail to take reasonable steps to deal with it. What is reasonable is defined as industry practice as exemplified by the IWF model. Internet Watch therefore offers ISPs a service, facilitating their compliance with existing law. Any ISP declining to take action once informed of the existence of illegal material on his servers would risk prosecution.

The IWF framework has two main parts. First, ISPs take responsibility for the removal from their servers of material which is notified to them as being illegal in the United Kingdom (for example, material which it is considered breaches the Criminal Justice Act 1988, under which it is an offence to possess child pornography). In the case of Usenet Newsgroups, which have been found to be the chief source of illegal material, it was specifically decided not to block entire newsgroups, which could result in the displacement of material onto ostensibly harmless sites. Instead, individual articles are deleted from the local server, when IWF confirms to the service provider that the article contains material likely to be illegal according to statute and established case-law in the United Kingdom. IWF has now developed an automated system for the distribution of and action on information relating to illegal newsgroup articles. This enables illegal articles to be immediately removed from the news feeds of all subscribing ISPs, regardless of the material's origin (in the case of Web sites, IWF can only act directly against material hosted in the United Kingdom; see below). IWF is also routinely monitoring some newsgroups that have regularly been found to contain potentially illegal material, in order to provide a faster response.

A reporting hotline (via e-mail, fax and telephone) has been set up to which Internet users may report instances of material which they believe may be illegal. IWF has now taken over 200 reports, relating to more than 650 items, of which 480 (all involving child pornography) were actioned. Action varies according to the source of the material. In the case of newsgroup articles, which make up the vast majority of the material reported, IWF distributes details simultaneously to all subscribing ISPs, who then remove the material from their individual news feeds; this is done regardless of the origin of the offending message. In the case of material contained in a UK-hosted Web site, IWF will inform the ISP hosting that Web site, who will take steps to have the material removed. Of the small proportion of articles originating in the United Kingdom, details have been passed to the police for enforcement action against the originator. Thus the originator remains responsible for content; the police remain responsible for enforcement. In the case of illegal material hosted on a non-UK server, IWF currently simply passes details to the National Criminal Intelligence Service (NCIS--the body responsible for liaison between UK police forces and their international counterparts). NCIS then passes the information to the appropriate foreign authority. It is envisaged however that IWF will develop its own direct links to other national self-regulatory bodies, which will facilitate the exchange of information (see below).

As noted above, a key aspect of IWF is that it ensures that users retain responsibility for material which they post on the Internet. To this end, a further part of IWF's remit is to address the possible abuse of anonymity. Provision of an Internet pseudonym is not in and of itself a danger, and anonymity can serve a

useful purpose in a number of contexts. The difficulty only comes if this service is abused--if the pseudonym is actually untraceable and this anonymity is used to commit crimes. Under the IWF framework, UK ISPs are therefore working on proposals to maintain "audit trails", so that the real identity of the user can be traced, in the event that the police can show that they need this information in the investigation of a crime.

The second part of IWF's remit relates to material which, whilst not illegal, may be harmful to minors, or found offensive. The United Kingdom believes that rating systems and filtering/screening software must play a key role here. Such tools allow users to tailor their or their children's experience of the Internet to their own personal standards, without denying access to legal material to those who wish it, and therefore without harm to the Internet's traditions of free speech. IWF was therefore charged with developing a rating system for legal content suitable for application in the United Kingdom. An advisory board was convened early this year comprising representatives of children's charities, educationalists, and consumers' and civil liberties groups, with the aim of recommending a suitable system. The IWF's recommendations should be ready by September 1997. IWF is also working on ways of ensuring the take-up and use of ratings, for example by pre-installing the necessary software on PCs, and by creating off-the-shelf profiles to make filtering more user friendly for those with little computer knowledge, for example based on the approximate standard of a PG (parental guidance - for general viewing but some scenes may be unsuitable for small children) film, or the pre-9pm watershed on UK television.

IWF had originally intended to concentrate first on UK action. Their experience so far has shown however that the vast majority of the illegal material reported to them appears to have originated outside the United Kingdom, and they have therefore begun to look at international co-operation as a priority. IWF has developed a proposal for international co-operation between self-regulatory bodies, which includes measures to improve international co-ordination in dealing with illegal material, develop sampling software to facilitate the tracking down of illegal material, and develop a set of standard factual ratings which could be drawn on by any group wishing to use filtering technology.

IWF plans to take forward its proposals in two stages. First they will work on developing a framework within Europe: IWF held a first meeting for interested parties in Brussels on 26 March 1997 facilitated by DG XIII of the European Commission. A bid for funding for this part of the project has also been submitted to the Commission; IWF's partners in this are ECO, the German Electronic Commerce Forum, and Childnet International, a UK-based charity devoted to promoting the interests of children in international communications. Following the Global Information Networks Conference in Bonn, an international working group on rating issues has been formed and will hold its first meeting in September. Apart from the INCORE partners (IWF, ECO and Childnet International), the Recreational Software Advisory Council and the Australian Broadcasting Authority are also committed to this project. The UK supports this approach. The United Kingdom believes that the OECD could play a valuable role in encouraging wider participation.

Private Sector Initiatives

R[3]
Safety-Net

Rating
Reporting
Responsibility

For Child Pornography & Illegal Material on the Internet

An Industry proposal
Adopted and Recommended by

Executive Committee of ISPA - Internet Services Providers Association
LINX - London Internet Exchange
The Safety-Net Foundation

23 September 1996

Introduction

This paper presents an industry proposal for addressing, in the United Kingdom, the question of illegal material on the Internet, with particular reference to child pornography. It presents a package of measures developed by key players from the Internet Service Providers Association (ISPA), the London Internet Exchange (LINX) and the Safety-Net Foundation. The paper puts forward industry proposals developed in discussions facilitated by DTI between service providers, the Metropolitan Police and the Home Office.

The potential for exploiting the Internet to inform, educate, entertain and conduct business on a world-wide scale is enormous. At a relatively modest cost, vast quantities of information can be sent around the world in new multimedia communications. The proportion of illegal material on the Internet is in relative terms, very small. The benefits of the Internet far outweigh its negative aspects. Nevertheless, these aspects cannot be ignored; they are pressing issues of public, parliamentary, commercial and legal interest. Consumers and businesses must be reassured that the Internet is a safe and secure place to work, learn and play.

The immediate and particular focus of these proposals is on child pornography, though the approach may also be applicable in the future to other types of illegal material available on the Internet. The proposers are adamant in their desire to remove child pornography from the Internet.

The package of measures proposed is coherent and is addressed to a range of key technical and policy issues. This a starting point, not a final solution. A number of detailed technical issues remain to be explored, but this is a credible beginning. No single approach, in a single country can entirely "solve" the problem, but there is much that can be done. These proposals take the first concrete step for the UK industry, providing a platform on which the industry can build further.

The principles of these proposals have been adopted and are recommended by the Executive Committee of ISPA, by the LINX and by the Safety-Net Foundation. Working groups in ISPA and in LINX will work with Safety-Net to establish any technological or legal limitations arising from these proposals and to explore appropriate implementation vehicles. All responsible service providers, inside and outside these organisations, are encouraged to support and adopt this package of measures. The time for action is now.

Principles

"R^3 *Safety-Net"* is based upon a number of simple principles.

The Internet is not a Legal Vacuum

In general, the law applies to activities on the Internet as it does to activities not on the Internet. If something is illegal off-line it will also be illegal online, and vice versa. Responsible service providers wish to see that the law can be upheld online as well as off-line. A clear liability to prosecution exists in UK law in relation to child pornography on the Internet, for example.

Free Speech not Censorship

The issue addressed has nothing to do with censorship of legal material or free speech. The issue is how to deal with material or activity which society, through democratic process, has deemed to be unacceptable in law. The core issue is crime. Legal, but possibly offensive, material raises a quite separate issue. Here consumers should have the technological means to tailor the nature of their, or their family's, experience on the Internet according to their individual standards. Thus both individual responsibility and the Internet's traditions of diversity and free speech are supported.

Responsibility

Service providers must take a responsible approach to the provision of services. They need to implement reasonable, practicable and proportionate measures to hinder the use of the Internet for illegal purposes, and to provide a response mechanism in cases where illegal material or activity is identified. Service providers should not be asked to take responsibility for enforcement of the law. End users should retain responsibility for the content they place on the Internet, whether legal or illegal. The police should retain responsibility for law enforcement.

Self-protection

By taking appropriate measures across the industry, service providers can offer protection to the end user and to themselves. All responsible service providers wish to hinder the availability of child pornography, and to see it removed from the Internet. This clearly protects the public. Establishing a common understanding of what steps constitute a reasonable, practicable and proportionate approach can also provide a defence for service providers against prosecution on charges of knowingly permitting services to be used for the distribution of illegal material.

Establishment and Jurisdiction

The law that determines what material or activity is illegal is the law of the country in which the consumer is affected by it. These proposals relate to service providers offering access to the Internet in the United Kingdom. They are designed to avoid any extraterritorial effect. Service providers established in the United Kingdom will take the UK law as the relevant standard for their UK operation, whatever the source of the material. However, measures adopted by service providers established in the United Kingdom can only address the problem at source if the material or activity was initiated by their UK subscribers. It is hoped that similar approaches can be established in other countries to extend the protection afforded across the whole of the Internet.

Approach

The "R^3 *Safety-Net"* approach incorporates three key elements:

- Rating.
- Reporting.
- Responsibility.

Overview

The approach establishes an independent foundation to support the adoption, by Internet service providers and users, of responsible policies based on rating and reporting of illegal material. It gives priority in the first instance to child pornography, but may also be applicable to other forms of illegal material in the future. The approach also supports the rating of legal material so that users can tailor the nature of their experience on the Internet, according to their own standards.

The Safety-Net Foundation

The Safety-Net Foundation has been established, and offers to fulfil an independent role in receiving and processing complaints about child pornography (and other illegal material) on the Internet and to support the development of rating systems.

The Rating Service

The Foundation will provide a legality indicator, or rating, for the "normal content" of each Usenet news group. The rating will indicate whether the group normally contains illegal material and what sort of illegality is involved (child pornography, copyright infringement, etc.).

As a separate activity, the Foundation also intends to assist in, or sponsor, the classification of legal material, to enable users to make use of PICS-enabled tools to customise the nature of their experience on the Internet according to their own standards.

The Hot-Line Service

The Foundation will establish a hotline to accept complaints about illegal material which is accessible to the public, via automated telephone, mail, e-mail or fax. These complaints will be converted into a standardised form and immediately forwarded to participating service providers and other appropriate bodies. A similar approach has been taken in the Netherlands, where it appears to work well, and has been endorsed by the first World Congress against the Commercial Sexual Exploitation of Children, Stockholm, 27-31 August 1996.

The Foundation will verify whether complaints are justified using standardised checklist criteria. In effect, the hotline will provide a rating of legality for individual news group articles, or Web pages, in response to complaints.

The Notification Service

In the case of illegal material originating within the United Kingdom, the Foundation would attempt to trace the source, inform the authors of the position under UK law, and request that they remove the offending material. Where co-operation is not forthcoming, the Foundation will request action from the relevant service provider and pass details to the National Criminal Intelligence Service (NCIS). Confirmation of action will be reported to the complainant.

Where the material originates outside the United Kingdom, the Foundation will pass available details to the foreign service provider, where they can be identified, and to NCIS, who will liase with the police in the appropriate jurisdiction.

Other Services

The Foundation will also sponsor research and development into ways of improving the detection, traceability and removal of illegal material on the Internet.

Funding

The Safety-Net Foundation will seek funding through service provider trade associations -- in particular, ISPA and LINX -- and through other bodies supporting the removal of child pornography (and other illegal material) from the Internet. All responsible service providers in the United Kingdom are encouraged to support and fund the Foundation. Start-up funding of up to GBP500 000 has been made available by the Dawe Charitable Trust.

Responsible Service Provider Policies

The Safety-Net Foundation takes responsibility for establishing a rating and reporting service for illegal material. This has to be complemented by responsibility on the part of users for the material they place on the Internet and by responsible service provider policies in order to have the desired effect. In particular, policies on the rating of material by users, on removal of child pornography and on tracing the originators of illegal material are needed. These issues are of greatest urgency in relation to World Wide Web (WWW or W^3) pages and Usenet news groups. Other policies may need to be developed and extended over time.

Policies for World Wide Web Pages

The "R^3 *Safety-Net*" approach endorses the Platform for Internet Content Selection (PICS) and the RSACi rating scheme for W^3 pages. "R^3 *Safety-Net*" recommends that Service providers:

- Promote PICS enabled software for accessing the W^3.
- Require all their users to rate their own Web pages using RSACi.
- Remove Web pages hosted on their servers which are persistently and deliberately misrated.
- Remove Web pages hosted on their servers which are identified and verified to them as containing child pornography (or other illegal material) if the users fail to co-operate by removing them themselves.

PICS is an open industry standard, which has been, or is being implemented both by major Web browser developers and by developers of other leading access control software. RSACi provides a PICS-based rating scheme, which provides a framework to classify content according to Language, Nudity, Sex and Violence.

These measures interface with the service provided by the Safety-Net Foundation aimed at illegal material. In addition, they provide the means by which Internet users can protect themselves and their families from exposure to material which, while legal, they find offensive.

Policies for Usenet News groups

The approach extends the PICS standard to Usenet news groups and recommends that service providers should:

- Support the development of a new Internet Standard (RFC) for transmitting ratings for news groups according to their "normal content". (This is currently being developed by Demon Internet and RSAC.)
- Support the availability of rating sources for all Usenet groups.
- Modify news servers to deliver group ratings to end-user software, when the standard becomes available.
- Promote PICS-enabled news software, when available.
- Remove from their servers, within a reasonable time period, news articles identified and verified to them as containing illegal material.

These measures will interface with both the Safety-Net Foundation's legality ratings for the normal content of news groups, and with the ratings provided by users for material they have placed on the Internet. In keeping with the principle that users should remain responsible for the material they post, "R^3 *Safety-Net*" considers that, in the long term, users should be encouraged to rate their news group articles as they post them. The approach of using ratings for the "normal" content of groups, whether supplied by the Safety-Net Foundation or by other sources, is proposed as a first step. It will assist both users and service providers in understanding the nature of material within these groups, and help to inform responsible actions towards them.

Policies on Traceability

A key aspect of the "R[3] *Safety-Net*" approach is that it attempts to ensure that users take responsibility for material they post on the Internet. To this end, it is important to be able to trace the originators of child pornography and other illegal material. In this context, the anonymity that it is possible to achieve through some services can be abused to mask the identity of the perpetrator.

Anonymity itself can serve a useful purpose in a number of contexts. However, the abuse of anonymity in posting illegal material is a problem which has to be addressed. Allowing users to have truly anonymous (*i.e.* untraceable) accounts is a danger, while providing services which create pseudonyms which remain traceable if necessary, is not. It is therefore recommended that service providers should:

- Work with the Safety-Net Foundation to close known loopholes and to identify and investigate a range of appropriate measures to provide facilities for better traceability, including, for example:

- Provision of audit trails such as X-NNTP-Posting-Host; and X-Mail2News-Path.

- Reasonable steps which ensure users of "free trials" can be identified (probably the most significant source of anonymity which is abused) including, but not limited to: use of caller line ID, verification of credit card details at start of trial.

- Development of new and better forms of technical counter-measures

- Ensure that anonymous servers (*e.g.* re-mailers) that operate in the United Kingdom record details of identity and make this available to the police, when needed, under Section 28.3 of the Data Protection Act.

Development of Policies on other Issues

The nature of the problem of child pornography and illegal material on the Internet will evolve over time. The "R[3] *Safety-Net*" approach recognises this and recommends that service providers should continue to work, through their trade associations, with the Safety-Net Foundation, with the police, governments and with other interested groups. It may be necessary, from time to time, to adapt existing policies or to introduce additional policies to cover new services.

The Proposers

This is an industry proposal which all responsible service providers are encouraged to support and adopt. Brief detail on those behind these proposals is given below.

Executive Committee of ISPA

ISPA is a recently established trade association representing the interests of the Internet industry. It aims to offer members the chance to participate in a growing dialogue with government, the European Union and other international organisations. The intention is to encourage an open and competitive environment, and to resist anti-competitive policies and practices. ISPA currently has 60 members made up of access providers, Internet cafes and other enterprises associated with the Internet.

The London Internet Exchange (LINX)

The London Internet Exchange (www.linx.net) is a not-for-profit association representing the 28 largest Internet service providers in the United Kingdom. Since October 1994 it has been managing the hub at which they connect their networks together to exchange UK Internet traffic. Its members all operate their own international links to the global Internet, and a majority of them provide access services to UK customers.

The Safety-Net Foundation

The Foundation is the initiative of Peter Dawe, previously the Chairman of Pipex. It will be a not-for-profit company limited by guarantee.

In order to take the "R^3 Safety-Net" approach forward, the Foundation will approach other independent parties to form a management board. This could include approaching possible Directors from a range of backgrounds, including child protection groups, the police and the Internet service provider trade associations. Should the Safety-Net Foundation become self-supporting as envisaged in the R^3 Safety-Net approach, then it is Mr Dawe's intention to step down as Director.

Other Non-governmental Initiatives

Other non-governmental initiatives in the United Kingdom include:

- NCH Action for Children. See http://www.nchafc.org.uk/
- Childnet International's Launchsite for kids: http://www.launchsite.org/
- National Centre for Educational Technology. See http://www.ncet.org.uk/index.html
- For Information on Regulation of Child Pornography on the Internet, see http://www.leeds.ac.uk/law/pgs/yaman/child.htm

United States

General approach to Internet-based services

The United States considers the Internet an increasingly critical medium of information sharing, commerce, education, entertainment and communication, with both unique and emerging capabilities, and strongly supports the global expansion of Internet-based services.

The private sector has played the leading role in the expansion of Internet-based services and the Clinton Administration believes that market forces should continue to drive Internet developments. In our experience, policies and practices that encourage openness and flexibility help create markets, support diversity and fuel innovation, which in turn provide a range of social and economic benefits. For that reason, the private sector should be the primary source of solutions to Internet infrastructure and governance issues. Governments should support and encourage private sector initiatives, including the development of technical solutions and private dispute resolution mechanisms.

Governments should refrain from imposing unnecessary, inappropriate or burdensome restrictions on the provision and use of Internet-based services, as such regulations distort the further expansion of such

services. Where government involvement is deemed necessary and appropriate, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for the provision of Internet-based services.

Moreover, existing laws and regulations should be reviewed and amended or eliminated where they may hinder the further expansion of Internet-based services. In applying any existing laws or regulations, it is necessary to analyse whether the policies underlying the relevant law will be furthered by applying the law to the Internet.

The framework supporting the provision of Internet-based services should be governed by consistent principles that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides.

The Internet promotes cultural diversity and pluralism. Governments can foster this goal by ensuring open access to the Internet in a way that preserves such diversity, fosters pluralism, and enables multiple, diverse communities to co-exist.

Specific content-related laws and regulations

The starting point for understanding US regulation of content on the Internet (or elsewhere) is the First Amendment to the US Constitution. That amendment explicitly protects freedom of expression, and establishes a general presumption that neither the US government nor the governments of its states (pursuant to the 14th Amendment) may criminalise or burden speech on the basis of content. Over the years, US courts have crafted a large, complex body of law interpreting the free speech protection of the First Amendment, including the establishment of exceptions that allow limited regulation of speech.

US courts apply three levels of tests to determine whether speech can be regulated. The strict scrutiny test, applicable to restrictions that are clearly based on the content of speech, allows speech to be regulated if necessary to serve a “compelling state interest,” if the regulation is “narrowly drawn to achieve that end”. Government must generally employ the “least restrictive means” of regulating. Under the “intermediate” test, applicable to content-neutral regulations affecting speech, a regulation must be “narrowly tailored to serve a significant governmental interest and not burden substantially more speech than necessary to remedy the condition the government identified as needing correction”. A third test, the “rational basis” test, applies to regulation that does not directly implicate speech, such as economic regulation that affects a broad group.

Direct content regulation traditionally falls into five classes: advocacy of unlawful conduct, obscenity, threatening and offensive language, invasions of reputation and privacy, and commercial speech. Otherwise, US courts allow some content-neutral restrictions on the "time, place, and manner" of the speech, and some regulation of "public forums." Speech restrictions must also meet various legal requirements; *e.g.* they may not be excessively vague or overbroad.

Major categories of content found online that receive no or limited First Amendment protection include:

- Obscenity, which receives no protection, is defined according to a three-part test. Obscene speech is that which: 1) an average person, applying contemporary community standards, would find appeals to the "prurient interest"; 2) "depicts or describes, in a patently offensive way, sexual conduct specifically defined by . . . state law"; and 3) taken as a whole, lacks serious literary, artistic, political, or scientific value.

Obscenity is regulated both at the state and federal level. Relevant criminal statutes include 8 USC. § 1462, which forbids the transportation or importation (or transmission via interactive computer service) of obscene matter.

- Material that is "harmful to minors", sometimes known as "obscene as to minors". Such materials are those that fail the above three-part test when applied from the viewpoint of a minor (*e.g.* lacking in serious literary, etc., value **for minors**), but are not obscene *per se*. Such material may not be banned, but commercial sellers may be prohibited from selling it to minors or displaying it in a location accessible to minors. "Harmful to minors" statutes exist only at the state level, not at the federal level.

- Threats of harm and harassing communications. A wide variety of state laws proscribe such conduct. In addition, federal law criminalises extortionate threats of personal harm (18 USC. § 1951); transmission of threats or ransom demands (§ 875); transmission of extortionate threats to harm a computer system [§ 1030(a)(7)]; and repeated use of a telecommunications device solely to harass the recipient [47 USC. § 223(a)(1)(E)].

- Child pornography, defined in federal law as material depicting a person less that 18 years of age engaging in "sexually explicit conduct" [18 USC. § 2256(2)]. Federal law -- primarily 18 USC. § 2252 -- criminalises the knowing transportation, distribution (including via computer), or possession of such materials in any form (including computer graphics files). Numerous state laws impose criminal penalties for similar conduct.

- Enticement of minors to engage in prostitution or other illegal sexual activity [18 U.S.C. § 2422(b)]. This provision of federal law, enacted as part of the Communications Decency Act of 1996, remains in effect and would apply to such speech online.

- Fraudulent statements for the purpose of obtaining money or property from another. Federal law (18 USC. § 1343) prohibits wire transmission of communications in furtherance of a scheme to defraud. In addition, every state in the United States has criminal statutes relating to fraudulent statements.

Commercial speech (*e.g.* advertising) receives First Amendment protection, but may be subject to various regulatory requirements. For example, advertising relating to pharmaceutical products, securities, or professional legal services is regulated by agencies at the state or federal level.[80] Untruthful commercial speech, however, is not protected by the First Amendment. The Federal Trade Commission Act (15 USC. § 45 *et seq.*) prohibits deceptive or unfair commercial conduct, including false or unfair advertising. Advertising is also regulated at the state level by the individual state's attorneys general and consumer protection agencies, as well as through public and private enforcement of consumer protection, unfair competition, and deceptive trade practices statutes. The essential purpose of the regulation of advertising is to ensure fair competition and to protect consumers from false claims and representations.

Note that pure "hate speech" -- expression that disparages a person or group on the basis of race, religion, ethnicity, etc. -- receives full First Amendment protection and may not by itself be made the object of criminal sanctions, according to the US Supreme Court. See R.A.V. v. City of St. Paul, 112 S. Ct. 2538 (1992). If the speech rises to the level of personal harassment (see above) or is inextricably tied to unlawful conduct (such as physical assault), it loses its legal protection.

In addition, US courts apply different levels of scrutiny to different communications media. Because of the unique characteristics of each medium, the same standards are not applied to the print media, broadcasting, cable television, direct broadcast satellites, common carriers, information service providers,

and Internet service providers. For example, because of the scarcity of radio spectrum, broadcasters are considered public trustees, and US laws require them to air programming that serves the public interest. In contrast, the government cannot compel newspapers and magazines to provide such content.

Restrictions on "indecent" speech -- a category of sexual-related speech considered less objectionable than "obscene" speech -- are illustrative. While obscene speech can be restricted in any medium, indecent speech is allowed in some media but not others. For example:

- Broadcast (radio/television) restrictions on "indecent" material. The US Supreme Court has upheld federal restrictions on the hours during which broadcasters may disseminate material that describes or depicts, "in terms patently offensive by contemporary community standards for the broadcast medium, sexual or excretory activities and organs". The justification for this restriction is twofold: broadcast is viewed as "pervasive" (indecent material may suddenly confront an unsuspecting viewer/hearer, even in the home) and as "uniquely accessible to children".

- "Dial-a-porn" restrictions on "phone sex" services. The Supreme Court has stated that "indecent" material may not be banned entirely from for-pay telephone services. However, providers of such content may be required to take measures to screen out minors (for example, by requiring payment by credit card).

Although information privacy is not an unlimited or absolute right, concerns about the misuse of personal information have been reflected in a diverse set of laws and regulations to protect privacy. While there is no single statute or regulation that governs the collection, communication, and use of all types of information about individuals, the United States has a sectoral approach to privacy protection that relies on a mixture of legislation, regulation, and private sector self-regulation (such as codes of conduct and corporate policies). Federal law regulates the government's collection, use, and distribution of a significant amount of personal information. In addition, it is generally against the law to intercept the content of any communication without consent or specific authority. The 1996 Telecommunications Act extends comprehensive protection to transactional data held by common carriers. Online service providers and Internet access providers are not currently regulated by statute, but many contract with subscribers to provide privacy protection.

Medical records are governed traditionally by codes of professional conduct. Legislation passed in the 104th Congress, however, will produce important recommendations for comprehensive protection of medical records and will lead, at a minimum, to enforceable protection for medical records transmitted for insurance claim administration.

The Clinton Administration recognises that the increasing use of advanced information and communications technologies permits both governments and the private sector to transmit, process, and store vast amounts of information about individuals. While these capabilities are increasingly essential for governments to function effectively and for businesses to operate efficiently, questions continue to grow about an individual's right to privacy and the accompanying responsibilities of holders and transmitters of this information to safeguard this right. In 1995, the Administration's Information Infrastructure Task Force (IITF) released the NII Principles for Providing and Using Personal Information, which seek to balance individual privacy rights with the free flow of information. Drawing on these principles, the Commerce Department's National Telecommunications and Information Administration (NTIA) issued a White Paper, "Privacy and the NII: Safeguarding Telecommunications-related Personal Information" in October, 1995, which developed a framework for safeguarding personal information associated with subscribing to and using a telecommunications or information service.

In response to the growing public concern about personal information privacy in the "information age", the IITF issued a draft “Options for Promoting Privacy on the National Information Infrastructure” for public comment in April 1997. In June 1997, the Commerce Department's National Telecommunications and Information Administration (NTIA) released a collection of papers from recognised experts on privacy and self-regulation in the information age as part of the Federal Trade Commission's three-day conference on privacy protection. This collection of papers provide a more comprehensive examination of whether and how self-regulation can work, and is intended to advance the debate with respect to the different options and models under consideration for privacy protection in the information age.

Recent developments

As the widespread public use of the Internet is a relatively recent phenomenon, case law applicable to First Amendment rights on the Internet is limited. In a recent decision striking down key provisions of the Communications Decency Act of 1996, a US law that regulated online obscenity and indecency, the United States Supreme Court allowed obscenity restrictions to remain in place, but declared the Act's restrictions on indecent communications unconstitutional. The Court's decision does not convert the Internet into a no-law zone, however. On the contrary, many types of expression that may be regulated in the physical world -- such as threats, obscenity, and the other classes of speech discussed above -- may also be regulated on the Internet.

On 16 July 1997, President Clinton convened a meeting of industry, parent and teacher organisations, and government representatives to work together to create a family-friendly Internet without abridging the constitutional guarantees of free speech and free expression. The Administration's plan calls for: (1) the provision of easy-to-use blocking, filtering and labelling technology for parents and teachers by the Internet industry; (2) the enforcement of existing laws that protect children online by the Administration; and (3) greater involvement by parents and educators in the use of the Internet by children.

REFERENCES:

The following policy statements or studies have been commissioned or supported by the United States Government:

- A Framework for Global Electronic Commerce, Clinton Administration, 1 July 1997.
- *Cryptography’s Role in Securing the Information Society,* Kenneth Dam and Herbert Lin, (30 May 1996, Pre-publication Copy Subject to Further Editorial Correction), Computer Science and Telecommunications Board, National Research Council, National Academy Press, Washington, DC, 1996.
- Global Information Infrastructure: Agenda for Co-operation, Al Gore and Ronald Brown, February 1995.
- Information Superhighway: An Overview of Technology Challenges, General Accounting Office, (GAO/AIMD-95-23) January 1995.
- *Information Superhighway: Issues Affecting Development,* General Accounting Office, (GAO/RCED-94-285) September 1994.

- Intellectual Property and the NII, Information Infrastructure Task Force, Bruce A. Lehman, September 1995.

- NII Principles for Providing and Using Personal Information, Information Infrastructure Task Force (IITF), 1995.

- *Online Law*, Thomas J. Smedlinghoff, Software Publishers Association, 1996.

- *Options for Promoting Privacy on the National Information Infrastructure*, Information Policy Committee, National Information Task Force, Draft for Public Comment, April 1997[81].

- *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration (NTIA), Department of Commerce, June, 1997.

- *The NTIA Infrastructure Report: Telecommunications in the Age of Information*, National Telecommunications and Information Administration (NTIA), Department of Commerce, October 1991.

- *White Paper on Privacy and the NII: Safeguarding Telecommunications-related Personal Information*, National Telecommunications and Information Administration (NTIA), Department of Commerce, October, 1995.

US PRIVATE SECTOR SUBMISSION TO OECD INTERNET INVENTORY PROJECT

Attached is a compilation of information provided by the US private sector.

I. Content Filtering Software and Services

A. One hundred percent available

100 per cent availability today. There are a growing number of parental empowerment options available to families online. These options range from services that are part of commercial online services, to stand-alone software, to Web-based labelling services and filtering software building on the Platform for Internet Content Selection (PICS) specification. Today it is safe to say that every family using the Internet has ready access to filtering sufficient to shield themselves and their children from unwanted content. In the coming months, we can expect even more progress in several areas: PICS deployment in more major Web browsers, creation of additional third-party labelling services, broader use of self-labelling options, and increased availability of positive guidance services to help families find appropriate Internet content.

Today, those desiring to filter out certain materials when accessing the Internet have three distinct options:

- Stand-alone Filtering Software: Software which runs together with an Internet access programme and blocks access to whatever type of content the parent believes inappropriate for their children. In this category are products such as Surfwatch and Cyber Patrol, as well as Cybersitter, NetNanny, and over ten others.

– Commercial Online Service Blocking Features: Several major commercial online services offer blocking features integrated into their access software. These features are easy-to-use and part of the regular menu of options offered to users.

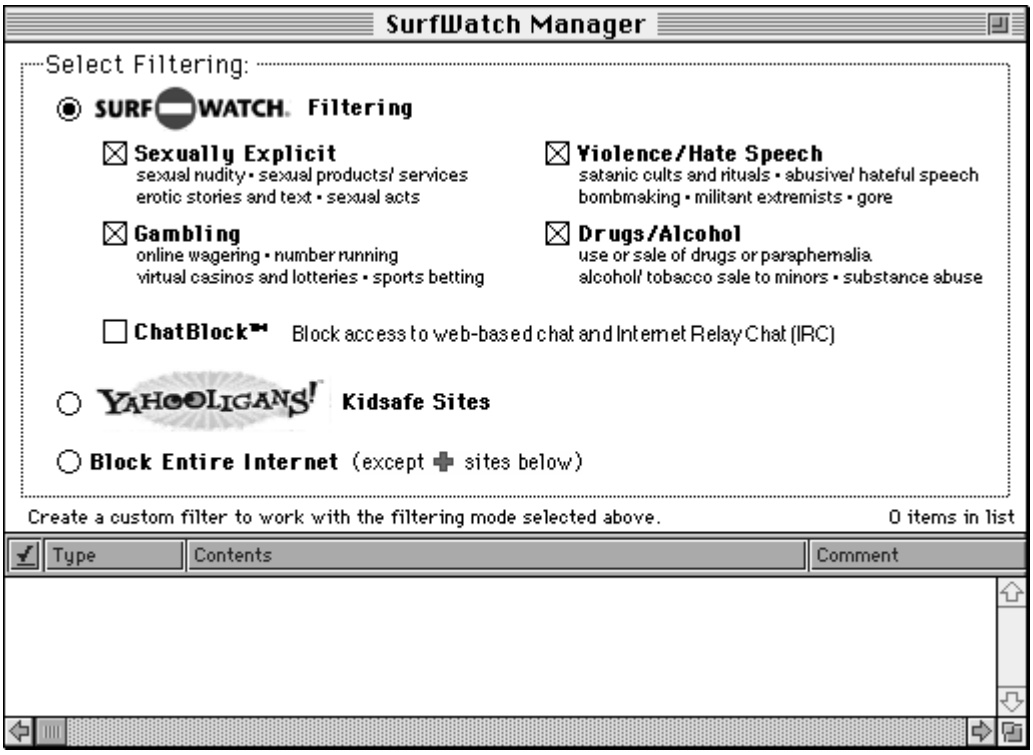
– Web-based PICS filtering: An integral part of major Web browsing software gives parents the ability to set up their Web software to block access to certain material on the World Wide Web through rating systems such as Net Shepherd, RSACi, and SafeSurf.

1. Stand-alone filtering software

Since the introduction of the first Internet filtering software in May 1995, a wide variety of software products have been offered which give parents (or other users) the ability to block access to various categories of objectionable content. This software is easy to use and available today to 100 per cent of Internet-connected households, often at no charge.

A variety of stand-alone, inexpensive, and easy-to-install software blocks access to material judged inappropriate for children. Most packages give parents the option of choosing what kinds of material to block such as sexually explicit material, violence, advertising, or extremist views. Each filtering software offers different choices of content categories to be filtered. For example, one product, SurfWatch, offers users the filtering choices indicated in Figure 1:

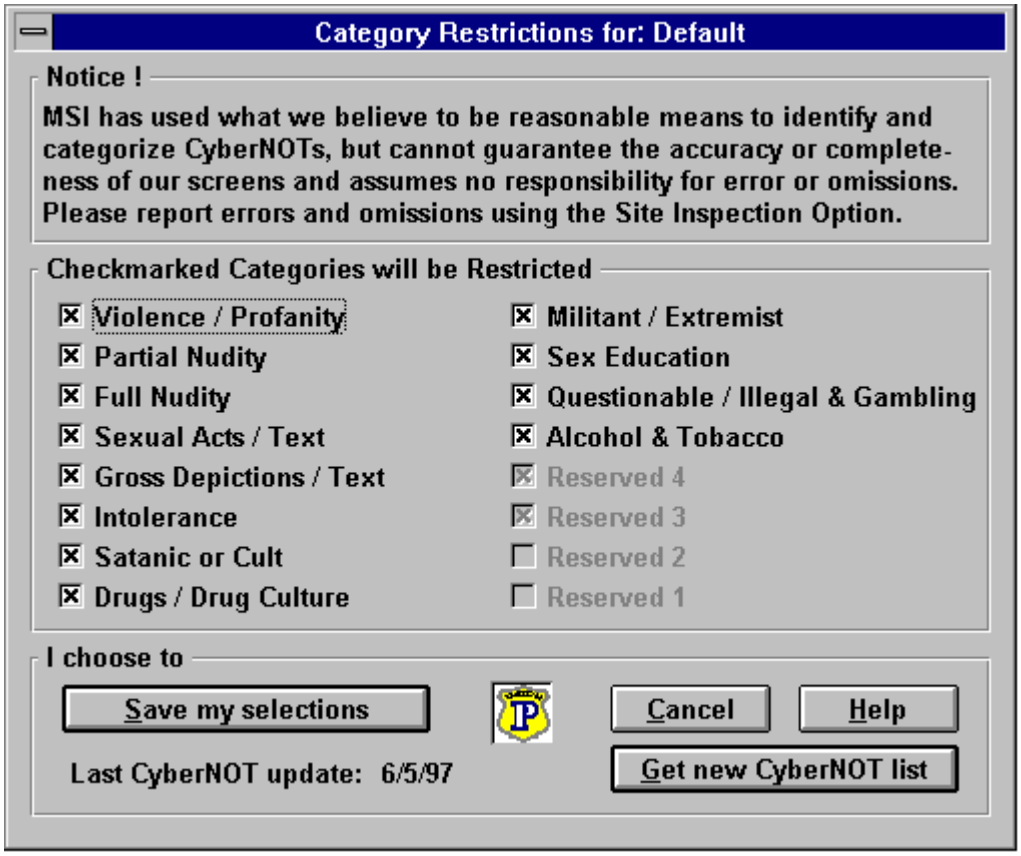
Figure 1. Surfwatch Setup screen



Different software also offers additional features such as the ability to selectively unblock blocked sites, track e-mail sent and received by particular children in the household, and even monitor the amount of time spent online.

The product Cyber Patrol offers the parent the choice indicated in Figure 2:

Figure 2. Cyber Patrol Setup Screen



In addition to the two software products described above, over ten such filtering software packages exist, blocking material based a diversity of editorial standards of the software developers (Figure 3).

Figure 3. Filtering Software Vendors

Filtering Software Vendors
Cyber Patrol
CyberSitter
CyberSnoop
The Internet Filter
Microsoft Plus for Kids
NetNanny
NetRated
Net Shepherd
PlanetWeb
Safe Surf
Specs for Kids
SurfWatch
Times Up!
Triple Exposure
X-Stop

Most filtering software vendors claim to filter based on objective criteria, but the blocking options do span the political spectrum. General interest software such as Cyber Patrol and Surfwatch exists along with software affiliated with conservative Christian groups such as CyberSitter, which has been endorsed and funded by Focus on the Family.

Though many filtering vendors disclose their general filtering criteria, they do not reveal the actual lists of blocked sites. This lack of transparency in blocking software is a deficiency of this approach. During the relatively short lifetime of these products there have been occasions where sites are blocked inappropriately (*i.e.* CDT's Web site was blocked for its discussion of bomb-making information and counter-terrorism policy). However, the filtering software vendors have been responsive to such complaints and corrected their blocking lists based on such mistakes. The critical issue is that consumers are aware of such possibilities.

The vast majority of households connected to the Internet today have easy access to filtering capability through a variety of avenues, either through offerings from their Internet service provider or because this software comes already installed on the computer that they purchased for their home.

All major commercial online services, as well as over 145 regional and local Internet service providers around the country, offer their customers filtering software either for free or for a small fee. As Figure 4 shows, nearly 14 million Internet households have access to online services which offer easy access to filtering.

Figure 4. Major national online services and internet service providers offering filtering software

Service Provider	Service Area	Software Offered	Cost	Number of Users
America Online	Global	AOL Parental Controls Cyber Patrol MS Internet Explorer with PICS	Free	8,000,000
AT&T WorldNet	Global	SurfWatch Cyber Patrol MS Internet Explorer with PICS	<$20 Free	900,000
CompuServe	Global	SurfWatch on kids service Cyber Patrol	Free	1,700,000
Earthlink	National	SurfWatch	<$20	280,000
Erols	National	SurfWatch	Free	200,000
MSN	Global	SurfWatch MS Internet Explorer with PICS	Free	1,600,000
Netcom	National	SurfWatch MS Internet Explorer with PICS	<$20 Free	590,000
Prodigy	Global	Cyber Patrol	Free	1,000,000
WebTV Networks	National	SurfWatch	Free	200,000
TOTAL				**14,470,000**

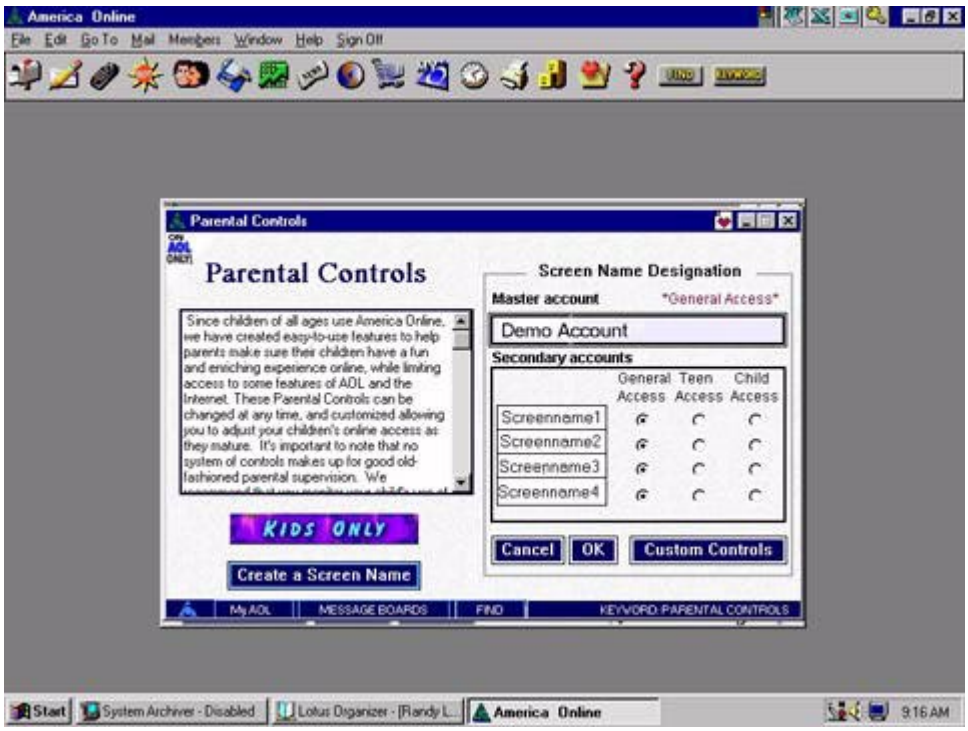
Whether offered for free or for a small cost, it is clear that every household which chooses to provide their children Internet access will have an opportunity to select some form of filtering software at the same time as they purchase Internet access service.

B. Easy-to-Use and Effective

1. Built-in online service parental controls

Major commercial online services also offer a variety of parental controls that include site blocking, limitation on receipt of e-mail, and restriction of children's accounts to limited areas of the online service's own content. These controls are available at no cost and easy to configure as part of establishing accounts for children (Figure 5).

Figure 5. AOL parental control screen



Taken together with the filtering options offered by other online services, we see that over 14 000 000 Internet households today already have easy access to filtering capability (see Figure 4 above).

2. Easy-to-access when bundled on home PCs

PCs purchased through retail outlets or by mail order often come "bundled" with a variety of software products. Many consumers who have purchased a PC recently will find that it will include not only software to allow immediate Internet access, but also some form of filtering software. This is especially true of PCs sold with modems already installed. The following chart illustrates just some of the bundling arrangements made between hardware vendors and filtering software companies (Figure 6).

Figure 6. Major PC manufacturers bundling filtering software with PCs sold into the home market

Hardware Manufacturer	**Filtering Software**	**Product Lines**
Acer	Cyber Patrol	Home PCs
Apple Computer	SurfWatch	All Macintosh
Compaq	SurfWatch	All Presario
IBM	Cyber Patrol	WorldBook & NetVista
Packard Bell	SurfWatch	Home & Small Office PCs

Bundled software is already loaded onto the computer's hard drive, so no complicated installation is necessary. In this way even parents who need their child's help to load software can employ blocking

software as they judge necessary. Through these arrangements many millions of users around the country have ready access to filtering if they desire it for any reason.

C. Services Accommodate a Diversity of Family Values and Needs

In response to a perceived need on the part of Internet parents to control child access to inappropriate material, the Internet community undertook the development of technical standards to facilitate the growth of an unlimited variety of rating and filtering systems for the Internet. The result in less than two years is that today there are three well-established independent rating systems accessible at no charge for all Internet families, plus a platform on which any interested party can create additional rating systems to meet the needs and values of their own community.

These three rating systems have been created using the technical tools made available by the Platform for Internet Content Selection (PICS), created through the efforts of the World Wide Web Consortium and a number of leaders in the Internet development community. Since the creation of PICS and the launch of these three labelling systems, virtually all leading Internet hardware, software, and services vendors have co-operated to give Internet-using families the ability to block and filter content based on PICS-formatted labels. Anyone on the Web can create third-party labels, self-label their own content, and use the labels that exist to filter Web access. Since 1996, Microsoft's Web browser, Internet Explorer, has enabled parental control through any PICS-formatted labelling service. With roughly 30 per cent of the browser market, a substantial number of users have PICS access today. Netscape has also recently announced its commitment to implement PICS.

In addition to PICS-compatible browsers, a number of stand-alone filtering products such as Cyber Patrol allow any Internet parent to filter based on PICS labels. Thus, today 100 per cent of Internet-connected families have easy access to all PICS labelling services. With these various PICS-enabled Internet software devices, parents have access to the following rating services:

Rating Service	# Web Sites Rated	URL
Net Shepherd	300,000+	www.shepherd.net
RSACi	35,000+	www.rsac.org
SafeSurf	70,000+	www.safesurf.com

1. Self-labelling

The PICS platform allows Web publishers to label their own content. Leading examples of this approach include RSACi and SafeSurf. Both RSACi (see Appendix 2) and SafeSurf (see Appendix 3) include standard rating vocabularies which allows Web publishers to describe the levels of sex, nudity, violence, and harsh language in a common format. To date, over 35 000 sites have rated their pages according to the RSACi labelling system and over 50 000 have rated their pages with SafeSurf. A number of major online content providers are working with RSACi to extend the reach of RSAC's ratings around the Web, including Disney, ESPN, and Playboy.

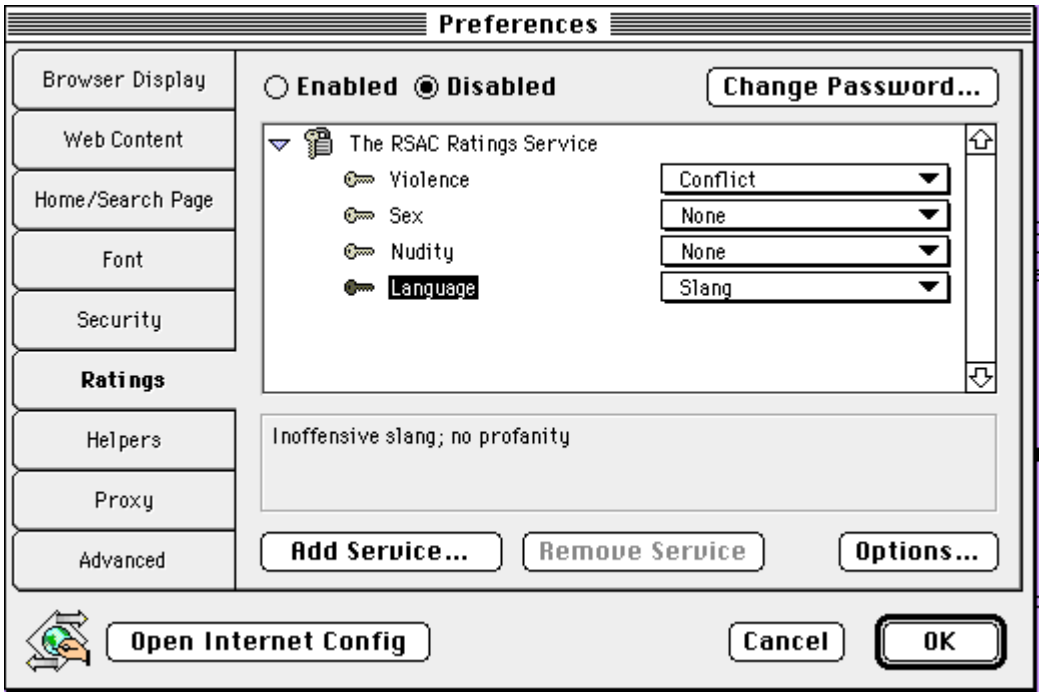
2. Third-party labelling

In addition to self-labelling, PICS also enables any individual or organisation to label any content on the Web. This feature of PICS supports the creation of multiple, diverse, independent labelling on content. Recently, the Net Shepherd has created independent labels for over 300 000 Web sites (see Appendix 4).

3. PICS filtering built into browsers

In August 1996, Microsoft shipped Internet Explorer 3.0, the first Web browser to support PICS. The Internet Explorer 3.0 browser was equipped with a feature called "Content Advisor" that enabled parents to limit their children's access to Internet content. The next version of Microsoft's browser, Internet Explorer 4.0, maintains this important functionality. By default, both versions of Internet Explorer use RSACi ratings, but other third-party rating systems may also be used. Microsoft has committed to rating all of its online content. As shown below, users of Microsoft's Internet Explorer have easy access to any PICS-formatted ratings, including Net Shepard, RSACi, and SafeSurf ratings.

Figure 7. Internet Explorer filtering screen



4. Filtered searches

Net Shepherd has teamed with Alta Vista to offer an Internet search service to find materials that Net Shepherd has labelled as appropriate for younger children. Using this service, children can search the Web and have results that include only those sites that meet rating criteria specified by parents.

II. Positive Guidance for Internet Resources

A. Yahooligans

Yahooligans!, the Web guide for kids from Yahoo!, is an Internet search engine for children to explore the wonders of the World Wide Web. Yahooligans! includes a directory of Web sites that are selected and individually reviewed for appropriateness, so parents and teachers can feel safe letting their children discover a delightful world of online education and entertainment. Yahooligans! can be found on the Web at www.yahooligans.com.

As the first online navigational guide to the Web, www.yahoo.com is the single largest guide in terms of traffic, advertising, and household reach, and is one of the most recognised brands associated with the Internet. Yahoo! Inc. can be found on the Web at www.yahoo.com.

B. Project OPEN: Internet resources for parents

Project OPEN (the Online Public Education Network) is a joint effort of the National Consumers League (NCL), the Interactive Services Association (ISA), and leading online and Internet service companies -- America Online Inc., AT&T, CompuServe Inc., Microsoft Corporation, and NETCOM Online Communication Services. Project OPEN's primary mission is to help consumers understand how to use online and Internet services in an informed and responsible way.

The partners of Project OPEN understand the importance of consumer education to maintain safe and productive online communities. To achieve this goal, Project OPEN provides educational tools and resources to promote safe computing for children and other users; facilitate understanding about privacy rights; promote the proper use of copyright-protected online content; and advance online consumer protection. Project OPEN's brochure, How to Get the Most Out of Going Online, provides an introduction to online safety issues and offers useful tips for people venturing online for the first time. The brochure introduces parents to software tools that can be easily programmed to restrict the sites children can visit on the World Wide Web and restrict the information they can divulge to others online, whether in a chat room or through e-mail. The software can also assist parents who want to limit the information that a marketer can collect from a child through an online survey or registration process.

The Project OPEN brochure has been featured in national publications such as USA Today, The Christian Science Monitor, Family Circle, Essence, Moneysworth and the 1997 Consumer's Resource Handbook. The publication is available at no charge through a toll-free hotline number. Over 100 000 copies of the brochure have been distributed to teachers, computer trainers, church groups and families. Many have requested bulk orders for distribution to students in their classrooms and computer labs. In addition, the brochure is posted along with additional privacy information at the Project OPEN Web site (http://www.isa.net/project-open). More than 70 Web sites have linked to the Project OPEN consumer education information. Project OPEN is working with representatives from leading educational associations to develop materials to acquaint teachers with the online and Internet medium. Some 40 000 copies of "How to Get the Most Out of Going Online" have been distributed to members of the National Education Association, the National Association of Secondary School Principals, the National Association of Elementary School Principals, the American Association of School Administrators and the National School Boards Association. In addition, AT&T includes Project OPEN materials in information kits distributed to nearly 20 000 Learning Network partners.

III. Next Steps: The Internet Community's Ongoing Commitment to Parental Empowerment

A. Librarian's Guide to Cyberspace for Parents and Kids

The American Library Association has launched an effort to develop an ongoing Internet collection for children and young adults which is built on the values and selection criteria of the library profession, is widely available to families through links in libraries and on the ALA site, and puts forth a vision of librarianship for the next century. The Librarian's Guide to Cyberspace for Parents and Kids will be a full and continuous service which will draw on the skills of librarianship and the work being done by librarians all over the country to develop and maintain a dynamic Internet collection for children and young adults.

There is a demonstrable need for guidance on the Internet. Unlike other media, the vastness of the Net coupled with its dynamic and fluid nature makes it very difficult for anyone to effectively select useful sites or be fully comfortable with the quality and veracity of the material presented on any site. The need to empower families in a positive manner to make good choices for their families is not currently being adequately met. While filtering and blocking technologies may help parents screen out sites that are offensive to their values, they do not determine whether those sites or any others are useful or valuable to children. What's more, the "positive" search engines that search key words and concepts to help identify sites are not linked to any set of selection criteria and are entirely value-neutral. They may help point the way to sites on a certain subject, but they cannot evaluate the quality of the site or the source material that supports it, or the usefulness to children.

For these reasons full family empowerment on the Internet must include guidance to materials that are of value for children and young adults. The role of the librarian is not only to provide society with access to information but to review information against a set of well considered "selection criteria", to create collections based on those criteria and then to guide library patrons to material that is useful and valuable. It is that core set of skills inherent in "librarianship" that need to be brought more fully to cyberspace.

Librarians around the country have been engaged in directing their patrons to sites that are valuable. Many have developed Internet sites for children and young adults. The ALA proposes to build on that work to develop a widely available collection for families. That collection (which will be featured on the ALA Web site) will include not only an evolving and growing list of sites that are valuable for children, but also linkages to libraries around the country that have already developed Internet collections for children. All librarians will be asked to assist in developing the collection and the links.

B. New Filtering Applications and PICS

As PICS labelling and filtering technology becomes more widely deployed in Web browsers, the Internet technical community will also help interested organisations and individuals to develop PICS-based labelling systems. Online providers of other sensitive content such as gambling, alcohol and tobacco advertising, etc., are also investigating self-labelling approaches in order to empower parents to shield their children from material judged by the parent to be inappropriate for the child. The University of Michigan School of Information will also launch a project to help incubate new content selection, labelling, and filtering services.

C. Internet Family Summit

In order to ensure that filtering and blocking tools keep pace with technology and that parents, educators and others responsible for the well-being of the nation's children understand the ease with which those

tools can be used, the Internet industry, together with organisations representing children, families, educators, Internet users and law enforcement will come together at a summit later this year. Together the summit participants will identify concrete ways to better educate parents about the tools that are available and how easy it is to use them. The summit will ensure that all interested parties work together to help equip parents and teachers with everything they need to supervise their children as they become more dependent upon the online world. Finally, summit participants will work with law enforcement to determine how industry can be of assistance in strengthening the enforcement of existing child protection laws and their application to the online environment.

IV. Conclusion

Finding the most effective means of protecting children online is a critical task for parents, policy makers, community groups, and the Internet industry. As in any other medium it is parental responsibility, not simple quick-fix technologies that will ultimately be the cornerstone of child protection. However, content blocking and filtering services available today do provide invaluable tools to assist parents in their efforts to ensure that their children's experience of the Internet is consistent with their own family values. The entrepreneurial genius of the Internet market, together with industry co-operative efforts such as the PICS rating platform, have already produced a wide range of options for parents. With creative partnerships between industry, government, and community groups, these options will multiply through both technology innovation and enhanced public education.

Appendices

Appendix 1 -- Local and Regional Internet Service Providers Offering Filtering Software

Service Provider	Service Area	Software Offered
A & S Technologies	Salt Lake City, UT	Cyber Patrol
A World of Difference	Charleston, SC	Cyber Patrol
Access Wisconsin	Madison, WI	Cyber Patrol
Accucomm	Irwington, GA	SurfWatch
Adhesive Media, Inc.	Austin , TX	SurfWatch
Alliance Network Internet Services		SurfWatch
Allstar Internet Services, Inc.		SurfWatch
Alpha Tech On-Line	Hendersonville, NC	Cyber Patrol
Altinet Dallas, TX	Cyber Patrol	
America's Computers		SurfWatch
American InfoMetrics	Modesto, CA	Cyber Patrol
Anet		SurfWatch
ANS	Global	Cyber Patrol
Applied Innovations, Inc.	Gainesville, GA	Cyber Patrol
Arden Computers, Inc	Sacramento, CA	Cyber Patrol
Association Assist	Dallas, TX	Cyber Patrol
AT&T WorldNet Services, Inc		SurfWatch
Avana Communications	Atlanta, GA	SurfWatch
Axis.Net	Milwaukee, Wi	SurfWatch
Badger Internet Services	Morgantown, WV	Cyber Patrol
Basin Office Systems	Pasco, WA	Cyber Patrol
Bell Atlantic	Regional	Cyber Patrol
BellSouth	Regional	SurfWatch
Berkshire Computer Consultants	Lenox, MA	Cyber Patrol
Black Box		SurfWatch
Bold Solutions Computing	Asbury Park, NJ	Cyber Patrol
BrighamNET Online Communications	Brigham City, UT	Cyber Patrol
CallTexas		SurfWatch
Cambridge Telephone	Cambridge, ID	SurfWatch
Cannon Communications	Hager City, WI	Cyber Patrol
CDS Internet	Medford, OR	SurfWatch
Century Telephone	Monroe, LA	Cyber Patrol
Chapelgate Media Centre	Mariettesville, MD	Cyber Patrol

Charm Net	Baltimore, MD	Cyber Patrol
Chibardun Telephone	Dallas, WI	Cyber Patrol
ClarkNet	Columbia, MD	Own service
CMS Automation	Richmond, VA	SurfWatch
CoastalNet	New Bern, NC	SurfWatch
Comp-U-Talk	North Bend, OR	Cyber Patrol
Compass Net, Inc.		SurfWatch
Compu-Net		SurfWatch
Computer & Network Services	Peterborough, NH	Cyber Patrol
Computer Land	Salina, KS	Cyber Patrol
Computer Pro Inc.	Duluth, MN	SurfWatch
Computer Super Centre	Paris, TX	SurfWatch
Comsource	Evansville, , IN	SurfWatch
Connect 2 Internet Networks, Inc.	Staten Island, NY	Cyber Patrol
Connect International	San Antonio, TX	Cyber Patrol
Connect! Communications Co		SurfWatch
Consultant (formerly Sonnet)	Tuolumne, CA	SurfWatch
Contact Network/In line Connections	Birmingham, AL	SurfWatch
Core Digital	Steven's Point, WI	Cyber Patrol
Cybercom	College Station, TX	SurfWatch
CyberRamp	Dallas, TX	SurfWatch
CyberShore, Inc.	Madison, CT	Cyber Patrol
CyberStation		SurfWatch
Dakota Internet Access	Williston, ND	SurfWatch
Data-Net Corp.	Fargo, ND	Cyber Patrol
Datacraft, Inc.	Chesterfield, MO	Cyber Patrol
Davis County School District	Woods Cross, UT	Cyber Patrol
DCCI Internet Services	San Antonio, TX	SurfWatch
DelNet, Inc.	Worthington, OH	Cyber Patrol
DFW Internet	Fort Worth, TX	SurfWatch
Digex	Beltsville, MD	Cyber Patrol
DNet Internet Services	Franklin, NC	SurfWatch
DomiNet, Inc.	Houston, TX	SurfWatch
E-Z Computer Services	Rochester, NY	Cyber Patrol
Eden Matrix Online	Austin, TX	SurfWatch
Edgenet	Westerly, RI	Cyber Patrol
Educational Software Institute	Omaha, NE	Cyber Patrol
Electrotex	Houston, TX	SurfWatch
ERI Net	Dayton, OH	Cyber Patrol

Erols Internet Services	National	SurfWatch
Family Net	Springfield, IL	Cyber Patrol
FastLane		SurfWatch
Fibrcom	San Antonio, TX	SurfWatch
Finite Technologies Service Corporation	Anchorage, AK	Cyber Patrol
Flashnet	Fort Worth, TX	SurfWatch
FlexNet,Inc	The Woodlands, TX	SurfWatch
Franklin Communication Services	Buffalo, NY	Cyber Patrol
Freeside Communications, Inc.	Austin, TX	SurfWatch
Fullnet Communications	Oklahoma City. OK	Cyber Patrol
Global Information Systems	Staten Island, NY	Cyber Patrol
Global Internet (INFOWEST)	St. George, UT	Cyber Patrol
Graphic Traffic	Ventura, CA	SurfWatch
Great River Systems	St. Paul, MN	SurfWatch
GreenNet Internet Service	West Newbury, MA	Cyber Patrol
Grove Enterprises, Inc.	Brasstown, NC	SurfWatch
GTE	National	Cyber Patrol
HA USA., Inc.	Santa Clara, CA	SurfWatch
Hawaii Online	Honolulu, HI	Cyber Patrol
Headwaters Telephone Company	Rhinelander, WI	SurfWatch
Hearst Corporation	Austin , TX	SurfWatch
I-Link, Inc.	Austin, TX	SurfWatch
IAmerica		SurfWatch
ID Entertainment Group	Nyack, NY	Cyber Patrol
Indiana Communications & System	Rushville, IN	Cyber Patrol
Industry Inet	Industry, TX	SurfWatch
InfiNET	Middletown, NJ	Cyber Patrol
InnerX Communications	Cartersville, GA	Cyber Patrol
Innovative System Design.	Tucson, AZ	Cyber Patrol
Insync Internet Services, Inc.	Houston,TX	SurfWatch
INTAP	Providence, RI	Cyber Patrol
Integrated Data Services	Duluth, MN	Cyber Patrol
Integrated Digital Network	Houston, TX	SurfWatch
Integrity Online	Aloha, OR	SurfWatch
Intellinet	Little Rock, AR	Cyber Patrol
Interglobal Communications	Niles, IL	SurfWatch
Internet 2000	Brainerd, MN	Cyber Patrol
Internet Concepts	Oklahoma City, OK	SurfWatch
Internet Direct	San Antonio, TX	SurfWatch
Internet of Asheville	Asheville, NC	SurfWatch

Internet Oklahoma Services INC	Oklahoma City, OK	SurfWatch
Interpoint Internet Comm.	Fort Lauderdale, FL	SurfWatch
Intex.Net	Dallas, TX	SurfWatch
Inturnet Inc.	Richardson, Tx	SurfWatch
Intx Networking LLC	San Antonio, TX	SurfWatch
K.3M. Inc. / Mirad Computers	Greensburg, IN	Cyber Patrol
Keystone Technology	Oklahoma City, OK	SurfWatch
Kids Unlimited / CyberPlay	Mount Dora, FL	Cyber Patrol
Klinknet	Northville, NY	Cyber Patrol
Komputer Kingdom	Gainesville, FL	Cyber Patrol
Lafayette News	Lafayette, CO	SurfWatch
LAN Lines Communications	White Plains, NY	SurfWatch
Landmark NETACCESS	North Conway, NH	Cyber Patrol
Leap Frog Technologies	Abilene, TX	Cyber Patrol
Learning Services	Eugene, OR	Cyber Patrol
Legendary Services	Royersford, PA	Cyber Patrol
Lightspeed Net	Bakersfield, CA	Cyber Patrol
Linear Internet Services	Dallas, TX	SurfWatch
Logical Micros	Albany, NY	SurfWatch
Macmillan Computer Publishing	Reno, NV	Cyber Patrol
Magic Soft	Flowery Branch, GA	Cyber Patrol
Mastermind Learning Centres	Tulsa, OK	Cyber Patrol
MediaOne (Continental Cable)	Regional	Cyber Patrol
Michael Ball	Denton, TX	Cyber Patrol
MicroServ Tele Computing	Idaho Falls, ID	SurfWatch
MicroServe Information Systems	Wilkes-Barne, PA	SurfWatch
Microsystems of Buckhannon, Inc.	Buckhannon. WV	Cyber Patrol
Mil-Tel Communications	Wichita Falls, TX	Cyber Patrol
MindSpring Enterprises, Inc.	Atlanta, GA	Cyber Patrol
Missing Link Communications	Galesburg, IL	Cyber Patrol
Mobile-Tech Computers	Whitefish. MT	Cyber Patrol
MPS Computer Services	Carrollton, TX	SurfWatch
MVI	Long Beach, CA	Cyber Patrol
NeoSoft		SurfWatch
Net Path	Burlington, N.C	SurfWatch
Net Solutions Corp.	Nashville, TN	Cyber Patrol
Netlink, Inc.	Chunky, MS	Cyber Patrol
NetNet	Green Bay, WI	Cyber Patrol
Netropolis		SurfWatch
NetSense	Wakefield, RI	SurfWatch

Network Management Group		SurfWatch
Networks	Wake Forest, NC	Cyber Patrol
Networks On-Line		SurfWatch
NORTEL	Durham, NC	Cyber Patrol
North Shore Access	Lynn, MA	Cyber Patrol
Nova Internet Services, Inc.		SurfWatch
NTR.NET Corporation	Louisville, KY	Cyber Patrol
Oasis Technologies	Tampa, FL	SurfWatch
Office Technology	Neenah, WI	Cyber Patrol
OKNET		SurfWatch
Online Network Enterprises, Inc	Boulder, CO	SurfWatch
OnLineXpress	Logan, UT	Cyber Patrol
Onramp Access, Inc.		SurfWatch
OnRamp Technologies	Dallas, TX	SurfWatch
OTW Inc.	Franklin, MA	Cyber Patrol
P.O.W.E.R. Net, Inc.	Spokane, WA	Cyber Patrol
Pacific Bell Internet	Regional	SurfWatch
Pacific Internet	Ukiah, CA	Cyber Patrol
Paulman Associates	West Hartford, CT	Cyber Patrol
PC Professionals	Wausau, WI	Cyber Patrol
Pencor Services (PenTeledata)	Palmerton, PA	SurfWatch
Peoples Communication	Randolph, WI	SurfWatch
Performix		SurfWatch
Perigee, Inc	Matthews, NC	Cyber Patrol
PERnet Communications, Inc.	Nederland, TX	SurfWatch
Phoenix DataNet		SurfWatch
Pittsburgh Online	Pittsburgh, PA	Cyber Patrol
PMH Network Services, Inc.	Emerson, NJ	Cyber Patrol
Primary Network	St. Luis, MO	SurfWatch
ProAxis	Corvallis, OR	Cyber Patrol
ProNET	Binghamton, NY	Cyber Patrol
RAM Technologies	Ashland, KY	SurfWatch
RapidRamp		SurfWatch
Red Rose SuperNet	Ephrata, PA	Cyber Patrol
Rhinelander Telephone Company	Rhinelander, WI	Cyber Patrol
ROMAN.NET	Rome, GA	Cyber Patrol
Sage Computer Systems	Temple , TX	SurfWatch
Signet Partners	Austin, TX	SurfWatch

Simple Computer	Greenville, SC	Cyber Patrol
Simply Interactive, Inc.	San Jose, CA	Cyber Patrol
Sojourn Systems Ltd.		SurfWatch
Solisys	Davis, CA	Cyber Patrol
South Carolina Supernet	Columbia, SC	SurfWatch
South Carolina SuperNet	Columbia, SC	Cyber Patrol
South Texas Internet Connections	San Antonio, TX	SurfWatch
Southwestern Bell Internet	Regional	
Spiff.Net	Granite City, IL	Cyber Patrol
Sprint Business Operations	Reston, VA	SurfWatch
StarNet Online Systems		SurfWatch
StoneGate Consulting	Chardon, OH	Cyber Patrol
Strategic Computer Solutions	Laredo, TX	SurfWatch
SysNet Corporation	Washington, DC	SurfWatch
TCA-LD	Amarillo, TX	SurfWatch
TDSnet		SurfWatch
TDSnet	Madison, Wi	SurfWatch
TechniX Micro Systems, Inc.	San Antonio, TX	SurfWatch
Technology Dimension, Inc.	Monroe, MI	Cyber Patrol
TEK Services & Resources Inc.	Hammond, IN	SurfWatch
Teleplex Communications	Roebuck, SC	SurfWatch
Teleport Internet Services	Portland, OR	SurfWatch
TeleTeam Internet		SurfWatch
Texas GulfNet	Brazoria, TX	SurfWatch
Texas Networking, Inc.	Austin, TX	SurfWatch
The Church Online!	Corona, CA	Cyber Patrol
The Computer Link Ltd.	Manitowoc, WI	Cyber Patrol
The Computer Shop NetLink	Paso Robles, CA	Cyber Patrol
The Edge Internet Services	Nashville, TN	Cyber Patrol
Thurber Technology Group	Portland, OR	Cyber Patrol
TNT Online,Inc.	Fort Myers, FL	Cyber Patrol
Total Software Resources	Lexington Park, MD	Cyber Patrol
Ultimate Internet Access	Ontario, CA	SurfWatch
Unicomp Technologies	Dallas,TX	SurfWatch
Upcom Internet Centre	Dana Point, CA	Cyber Patrol
Utah Wired	Salt Lake City, UT	Cyber Patrol
VidcomNet Inc.	Texarkana, AR	Cyber Patrol
Volcano Internet Provider	Pine Grove, CA	Cyber Patrol
Voyager Online LLC	Chattanooga, TN	Cyber Patrol

VPlus Network, Inc.	Chatsworth, CA	Cyber Patrol
Wachusett Programming Associates	Holden, MA	Cyber Patrol
WaterNet	Fort Myers, FL	Cyber Patrol
Web Fire		SurfWatch
Web Route Internet Service	Lake Oswego, OR	Cyber Patrol
Weidenhammer Systems Corp	Wyomissing, PA	SurfWatch
Wentworth Worldwide Media, Inc.	Lancaster, PA	Cyber Patrol
West Net	Rye, NY	Cyber Patrol
WestNet	Ventura, CA	SurfWatch
Whole Earth Networks		SurfWatch
Wildrose Net, Inc.	Camrose, AL	Cyber Patrol
WingNET	Cleveland, TN	Cyber Patrol
World Touch	Pleasant Hill, CA	SurfWatch
WorldNet	Norwood, MA	Cyber Patrol
WorldNet of Louisiana	Leesville, LA	Cyber Patrol
Worldpath Internet Services	Farmington, NH	Cyber Patrol
Z Land	Santa Ana, CA	SurfWatch
ZipLink	Hartford, CT	Cyber Patrol
Ziplink	Cambridge, MA	Cyber Patrol

Appendix 2 -- 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

Appendix 3 -- SafeSurf Ratings

The SafeSurf SS~~ Rating Standard
Designed by and for parents to empower each family to make informed decisions concerning accessibility of online content

Section One: Adult Themes with Caution Levels
0. Age Range
1) All Ages
2) Older Children
3) Teens
4) Older Teens
5) Adult Supervision Recommended
6) Adults
7) Limited to Adults
8) Adults Only
9) Explicitly for Adults

Section One: Adult Themes with Caution Levels

1. 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 artistic fashion
5) Graphic-Artistic
description: Non-sexual expletives used in a 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.

2. Heterosexual 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, medical references
4) Non-Graphic-Artistic
description: Limited metaphoric descriptions used in a artistic fashion
5) Graphic-Artistic
description: Metaphoric descriptions used in a artistic fashion
6) Graphic
description: Descriptions of intimate sexual acts
7) Detailed Graphic
description: Descriptions of intimate details of sexual acts
8) Explicitly 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.

3. Homosexual 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, medical references

4) Non-Graphic-Artistic
description: Limited metaphoric descriptions used in a artistic fashion
5) Graphic-Artistic
description: Metaphoric descriptions used in a artistic fashion
6) Graphic
description: Descriptions of intimate sexual acts
7) Detailed Graphic
description: Descriptions of intimate details of sexual acts
8) Explicitly 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.

4. 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 or revealing clothing
3) Technical Reference
description: Dictionary, encyclopaedic, news, medical 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 frontal nudity
7) Detailed Graphic
description: Erotic frontal nudity
8) Explicit Vulgarity
description: Pornographic presentation
9) Explicit and Crude
description: Explicit pornographic presentation

5. Violence
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Inviting Participation in Graphic Interactive Format
9) Encouraging Personal Participation, Weapon Making

6. Sex, Violence, and Profanity
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Explicit Vulgarity
9) Explicit and Crude

7. Intolerance
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Literary
5) Graphic-Literary
6) Graphic Discussions
7) Endorsing Hatred
8) Endorsing Violent or Hateful Action
9) Advocating Violent or Hateful Action

8. Glorifying Drug Use
1) Subtle Innuendo

2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Simulated Interactive Participation
9) Soliciting Personal Participation

9. Other Adult Themes
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Explicit Vulgarity
9) Explicit and Crude

A. Gambling
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Discussion
4) Non-Graphic-Artistic, Advertising
5) Graphic-Artistic, Advertising
6) Simulated Gambling
7) Real Life Gambling without Stakes
8) Encouraging Interactive Real Life Participation with Stakes
9) Providing Means with Stakes

Appendix 4 -- Net Shepherd Ratings

In December 1996, NSI launched an Internet event: We recruited over 300 Net aficionados to examine sites and rate them for maturity and quality using NSI's CRC (collaboratively rated content) rating scale.

The CRC rating scale has six maturity levels (General, Child, Pre-teen, Teen, Adult and Objectionable), and five quality levels (1 through 5 stars, with 5 stars signifying excellence). Quality on the CRC scale includes everything from content to navigation to graphics, and ultimately reflects the overall impression our raters have of the sites they visit.

VOLUNTARY LAW ENFORCEMENT

* Continuing efforts
  - Data base maintained by ISA and National Association of Att
  - orneys General listing law enforcement contacts (which are kept private)
  - NAAG has an interactive working group and subcommittees dealing with privacy, consumer protection, content regulation
  - Quarterly conference calls between ISA and NAAG
  - Information on online contacts in companies made available to the FTC by NAAG
  - Periodic meetings with FTC Bureau of Consumer Affairs attorneys and commissioners' staff
* Department of Justice Computer Crime Unit (headed by Scott Charney)
  - Periodic working group (nameless) of online companies to discuss issues of common concern affecting the Internet. The working group has held two meetings.
  - FBI (nominally part of the DoJ) is member of working group
  - No specific mandate but can cover a variety of issues from "mail bombing" to copyright infringement, paedophilia, financial white collar, etc.
* Company-specific programmes
  - AOL has contacted Interpol, police forces in Japan and elsewhere to outline protocols for ensuring rapid response to police inquiries.

AMERICA ONLINE, INC. (AOL) LAW ENFORCEMENT PROTOCOLS

	LAW ENFORCEMENT
Regulatory Objectives and Challenges	1. Stopping the transmission of child pornography. 2. Protecting public order/national security. 3. Stopping miscellaneous fraud and abuse, including hate speech, threats and harassment, and financial fraud over the AOL service.
Best Industry Practices	1. Identify and establish co-operative relationships with key law enforcement agencies both domestically and internationally. Relationships centre on the lead officials in the departments that have an interest in Internet related criminal activities and in the international arena, their liaison officials, attached to their government's Embassy in the US. This assures ready access to law enforcement officials in our international markets and an ally here for AOL, Inc. 2. Establish liaisons and official points of contact with and between national law enforcement officials and embassy officials. 3. Devise and implement investigation and compliance protocols, described further below, to: • Respond to. information requests from law enforcement officials. • Make prompt referrals to law enforcement officials regarding illegal activity of which it becomes aware. 4. Meet with policy makers and legal experts through national legislative, executive and judicial conferences, bar associations. 5. Educate users of responsibilities and responsible conduct (via its Terms of Service (TOS)/Rules of the Road (ROR)). 6. Develop internally, a specialised community action team to enforce the TOS and ROR.
Establishing Liaisons	• Appoint points of contact between AOL and the law enforcement community to provide follow-up to compliance and investigative requirements. • Meet with International officials from their respective polices agencies.
Representative Process	1. Int'l Law Enforcement (ILEO) Request for Subscriber and Billing Information : ILEO makes a request to the → AOL JV Compliance Specialist → who then provides the information to the ILEO. 2. ILEO Request for E-mail Contents: ILEO makes a request to → Host Country Ministry of Justice → US Dept. of Justice liaisons with Host Country Embassy Law Enforcement Attaché → AOL (US) Process Request. 3. AOL Referrals When It Becomes Aware of Illegal Activity: AOL US → Host Country Law Enforcement Official (see no. 2 for rest of process).
Existing Specialised Bodies	• Interpol. • The National Association of Attorneys General. • US governmental agencies including DOJ, Treasury, Commerce. • Lead police departments in each jurisdiction (*e.g.*, in the United States: New York, California, • Florida, Virginia, Maryland, New Jersey, and Massachusetts).
Industry Educational Efforts	• Training and educating law enforcement agencies about the operation of the service provider's network and law enforcement protocols. • Participating in seminars/workshops sponsored by the law enforcement network, with a focus on associations with broad-based membership, such as Interpol (*e.g.*, the 1996-97 Lyon and Buenos Aires conferences) and the National Association of Attorney Generals. • Conducting ongoing training sessions for these agencies, and continuing to serve as faculty for the DOJ prosecutors training program.

For More Information Contact:

John Ryan, Assistant General Counsel,
Compliance and Law Enforcement
America Online, Inc./Dulles, VA
703/265-2814 or 703/265-2305 Fax
JohnDRyan@aol.com

Bill Burrington, Assistant General Counsel
Director, Law and Public Policy
America Online, lnc./Washington, DC
202/530-7880 or 202/530-7879 Fax
BillBurr@aol.com

Submission by Online Public Education Network (Project OPEN) on US Private Sector Activities

Section I. Current Activities

Educating Parents and Teachers

The Internet and online world can be daunting to parents and teachers, who recognise the tremendous educational and cultural benefits the technology offers to kids, but worry about how to keep their experience safe and enjoyable. Parents and teachers recognise their role in helping children navigate the Internet, but often feel unprepared, especially when their children are more technologically savvy than they are. Fortunately, there are resources readily available to introduce parents to the new media, offer common-sense tips on parenting in the information age, direct them to information about online content controls, and help them to ensure that their child's online experience remains safe and enjoyable. The following information is representative of the resources currently available for parents and teachers in the United States.

1. Association Activities

The not-for-profit sector has been active in promoting the benefits of technology in schools and homes. Through research, workshops, training, educational outreach, and partnerships, each of the listed organisations provides information on how to restrict children's access to inappropriate content. While some promote content control software, others recommend parental supervision techniques, acceptable use policies, or a combination of the three. These organisations help parents choose an approach that is most appropriate in the context of their family's values and help librarians and educators choose policies which reflect their community standards.

American Association of School Administrators
1801 N. Moore Street, Arlington, VA 22209
(703) 528-0700
http://www.aasa.org

The AASA is the professional organisation for nearly 16 000 education leaders across the United States and Canada. The organisation provides support and resources for school superintendents and administrators, through conferences, workshops and publications.

American Library Association
50 E. Huron Street, Chicago, IL 60611
(312) 280-5044
http://www.ala.org

The American Libraries Association provides leadership and support for more than 100 000 school, public, academic and special libraries through a broad-based program of legislative advocacy, public awareness and professional education. Its mission is to promote the highest quality library services in order to ensure that all people have access to the information they need. "Kids connect @ The Library" is the message for a campaign to inform parents of how libraries can help connect their children with ideas, learning and fun through computers, books, and other resources.

Centre for Children and Technology
96 Morton Street, 7th Floor, New York, NY 10014
(212) 807-4200
cct@edc.org
http://www.edc.org/CCT/ccthome

The Centre aims to improve education by altering the circumstances of teaching and learning through basic, applied, and formative research and technology development. Much of its work is done in collaboration with schools, universities, libraries, community programmes, museums, and other institutions concerned with learning, teaching, and technology design.

The Centre for Democracy and Technology
1634 Eye Street, NW, Suite 1100, Washington, DC 20006
(202) 637-9800
info@cdt.org
http://websites.cdt.org

The Centre's mission is to develop public policies that preserve and advance democratic values and constitutional civil liberties on the Internet and other interactive communications media. CDT relies on a combination of staff expertise in relevant law and technology, along with a unique consultation process that brings together diverse interests from across the political spectrum, the public interest community, and the communications industry to address critical public policy issues.

Centre for Media Education
1511 K Street, NW, Suite 518, Washington, DC 20005
(202) 628-2620
cme@cme.org
http://www.cme.org/cme

The Centre educates the public about critical media policy issues. CME publishes InfoActive, a telecommunications bulletin for not-for-profit organisations.

Centre for Media Literacy
4727 Wilshire Boulevard, Suite 403, Los Angeles, CA 90010
(213) 931-4177
cml@earthlink.net
http://www.medialit.org

The Centre for Media Literacy is a not-for-profit organisation, membership organisation dedicated to a media-literate citizenry. The centre is the largest distributor of media literacy resource materials in North America, and conducts workshops and seminars in media literacy for teachers and parents in the Los Angeles area.

The Children's Partnership
1460 4th Street, Suite 306, Santa Monica, CA 90401
(310) 260-1220
kidspartner@earthlink.net

The Children's Partnership educates policy-makers and parents about technology issues affecting children. It also publishes briefing materials and operates a Web site for parents.

Community Technology Centres' Network
c/o Education Development Centre, Inc.
55 Chapel Street, Newton, MA 02158
(617) 969-7100
ctcnet@edc.org
http://www.edc.org

CTCN serves as a catalyst to strengthen community involvement with technology. It is creating an actual and electronic national affiliates' network of computer access and learning centres in resource-poor communities.

The Electronic Frontier Foundation
1550 Bryant Street, Suite 725, San Francisco, CA 94103
(415) 436-9333
eff@eff.org
http://www.eff.org

The Electronic Frontier Foundation seeks to find out how and to what extent new digital media fit into existing frameworks. While the free flow of information is generally a positive thing, serious problems can arise. Problems such as how to protect children and adults from exposure to sexually explicit or potentially offensive materials; how to protect intellectual property rights; how to determine which country's laws have jurisdiction over a medium that is nowhere and everywhere at the same time, and other difficult questions are the purview of this group.

KIDSNET
6856 Eastern Avenue, NW, Suite 208, Washington, DC 20012
(202) 291-1400
kidsnet@aol.com

KIDSNET is an educational not-for-profit organisation clearinghouse of information on children's media. The group generates a monthly database of audio, video, radio, educational software, television, and related multimedia programmes for children which is available in both print and electronic formats.

National Association of Elementary School Principals
1615 Duke Street, Alexandria, Virginia 22314
(703) 684-3345
http://www.naesp.org

NAESP is a professional association of principals, assistant, or vice-principals, persons engaged in educational research and in the professional education of elementary school administrators.

National Association of Secondary School Principals
1904 Association Drive, Reston, VA
(703) 860-0200
http://www.nassp.org

NASSP represents some 40 000 public and private middle and high school principals and assistant principals. The organisation sponsors the National Honour Society, and the National Technology Honour Society.

National Centre for Missing and Exploited Children
2101 Wilson Boulevard, Suite 550, Arlington, VA 22201-3052
(703) 516-6109
http://www.missingkids.org

The Centre publishes Child Safety on the Information Highway, an introduction to the Internet for parents that includes tips for children venturing online.

The National Education Association's Centre for Education Technology. The NEA has over 2.2 million members, including elementary, secondary, and university teachers, education support personnel and student teachers. The Centre for Education Technology is a clearinghouse of technology and online-related information for educators. The NEA partners with National Public Radio and Children's TV to produce "Science Friday -- Kids Connection".

National PTA
330 North Wabash Avenue, Suite 2100, Chicago, IL 60611-3690
info@pta.org
(312) 670-6782
http://www.pta.org

The National PTA is the oldest and largest volunteer association in the United States working exclusively on behalf of children and youth. For 100 years, the National PTA has promoted the education, health, and safety of children and families.

National School Boards Association
1680 Duke Street, Alexandria, VA 22314-3493
(703) 838-6722
itte@nsba.org
http://www.nsba.org/itte

The National School Boards Association supports school boards in their work to introduce technology in schools. The association publishes guides and resource materials.

National Urban League
500 East 62nd Street, New York, NY 10021
(212) 310-9000
info@nul.org
http://www.nul.org

The National Urban League is the premier social service and civil rights organisation in America. The League is a non-partisan, community-based organisation headquartered in New York City, with 114 affiliates around the country. The mission of the League is to assist African-Americans to achieve social and economic equality. The League implements its mission through advocacy, bridge building between the races, programme services, and research.

The Online Public Education Network (Project OPEN)
c/o Interactive Services Association
8403 Colesville Road, Suite 865, Silver Spring, MD 20910
(301) 495-4955
project-open@isa.net
http://www.isa.net/project-open

Project OPEN is a joint effort of the National Consumers League, the Interactive Services Association, and leading online/Internet service companies. Its primary mission is to help the American public learn how to use online and Internet services in an informed and responsible way.

2. Books

Bookstores and libraries are overflowing with information introducing parents and teachers to the Internet. In addition to providing how-to's and basics of the online world, these books provide information and referrals for readers interested in content control resources. They can be ordered over the Internet at shopping sites such as Barnes & Noble and Amazon.com.

- *Child Safety on the Internet*, Gregory Giagnocavo (ed), 1997.
- *Children and the Internet: A Zen Guide for Parents and Educators*, Prentice Hall Series in Innovative Technology, Brendan P. Kehoe, Victoria Mixon, 1997.
- The Connected Family: Bridging the Digital Generation Gap, Seymour Papert, 1996.
- Connecting Kids and the Internet: A Handbook for Librarians, Teachers and Parents, Allen C. Benson, Linda M. Fodemski, 1996.

- Danger Zones: What Parents Should Know About the Internet, Bill Biggar, Joe Myers, 1996.
- Everything You Need to Know (But Were Afraid to Ask Kids) About the Information Highway, Merle Marsh, Computer Learning Foundation, 1995.
- Exploring the Internet: A Cyberspace Odyssey, J. Alan Baumgarten, et al., 1996.
- Futurekids, the Internet Expedition, Ron Harris, 1995.
- Going to the Net: A Girl's Guide to Cyberspace, Marian Salzman, et al., 1996.
- *Internet for Kids*, Deneen Frazier, *et al*., 1996.
- Internet for Parents/Book and Disk, Karen Strudwick, et al, 1996.
- *Kids Do the Web*, Cynthia Overbeck Bix, *et al*., 1996.
- Leadership & Technology: What School Board Members Need to Know, National School Boards Association, 1995.
- *Mastering the Internet*, Glee Harrah Cady & Pat McGregor, 1996.
- New Kids on the Net: A Tutorial for Teachers, Parents, and Student, Sheryl E. Burgstahler, 1997.
- Online Kids: A Young Surfer's Guide Cyberspace, Preston Gralla, 1996.
- Paws Presents the Internet & the World Wide Web, Colleen Densley, et al., 1996.
- World Link: An Internet Guide for Educators, Parents, and Students (Original Works), Linda C. Joseph, 1995.
- The World Wide Web for Kids & Parents (The Dummies Guide to Family Computing), Viraf D. Mohta, 1997.

3. Brochures

Many organisations in the United States have developed timely and informative publications that are available at no cost or low cost to families and educators. They are promoted through mechanisms such as media outreach, public service announcements, and the Internet.

- "Child Safety on the Information Superhighway", National Centre for Missing and Exploited Children, 1994. Write or call: 2101 Wilson Boulevard, Suite 550, Arlington, VA 22201-3052; (703) 235-3900.
- "Making the Net Work for You: How to Get the Most Out of Going Online", Interactive Services Association and National Consumers League, 1996. Available free by calling 800-466-OPEN or on the Internet at http://www.isa.net/project-open.

- "Get CyberSavvy", Direct Marketing Association, 1997. Free single copies, with a cost of $2.50 for each additional copy by writing to the Direct Marketing Association, 1120 Avenue of the Americas, New York, NY 10036-6700. Also available free of charge at the DMA Web site http://www.the_dma.org.

- "The Librarian's Guide to Cyberspace for Parents and Kids", American Libraries Association 1997. A free copy of the brochure also is available by calling 800-545-2433, ext. 5044/5041, or no the Internet at http://www.ala.org/parentspage/greatsites.

- "The Parents' Guide to the Information Superhighway", The Children's Partnership, 1996. Available free on the Internet at http://www.childrenspartnership.org or for $8 by writing to : Parents Guide, 1460 4th Street, Suite 306, Santa Monica, CA 90401.

4. World Wide Web Sites

Families and teachers already online can have access to the latest, up-to-date information on content controls, acceptable use policies, and cyber-parenting techniques. The following is a sample of the myriad sites where help for parents is a mouse-click away.

- Barry and Ruth Cranmer's Safety on the Internet page with links to other resources http://www.voicenet.com/~cranmer/censorship.html

- Child Safety on the Information Superhighway, Produced by the Interactive Services Association and the National Centre for Missing and Exploited Children. http://www.isa.net/empower/child.html"

- Christian Science Monitor's Safeguarding the Children Page http://www.csmonitor.com/children/index.html

- Cyber-Savvy Parents Guide, by the Direct Marketing Association http://www.the-dma.org/pan/intro.html

- Disney's Family.com

- http://www.family.com

- The Family Education Network, sponsored by AT&T, Microsoft, and Nellie Mae. http://familyeducation.com

- The Guardian Angels' CyberAngels http://www.cyberangels.org

- Interesting Places for Parents http://www.crc.ricoh.com/people/steve/parents.html

- InternetAdvocate http://www.monroe.lib.in.us/~lchampel/netadv.html

- Internet Safety Tips from the University of Oklahoma's Department of Public

- Safety http://www.uoknor.edu/oupd/kidsafe/warn_kid.htm

- Interactive Services Association's Project OPEN http://www.isa.net/project-open

- Parent's Guide to Cyberspace from the American Library Association http://www.ala.org/parentspage/greatsites
- ParentSoup's Family and the Internet http://www.parentsoup.com/onlineguide/familyinternet/
- Platform for Internet Content Selection http://www.w3.org/pub/WWW/PICS
- SafeKids, produced by syndicated columnist Larry Magid http://www.safekids.com
- SafeSurf http://www.safesurf.com/index.html
- San Jose Mercury News, Family Guide to Cyberspace http://www.sjmercury.com/family

5. Internet Access Control Standards, Rating Systems, and Commercial Tools

The information technology marketplace, comprised of both suppliers and consumers, is acting decisively to solve the problems of appropriate access controls on the Internet and other online services. These solutions fall into three broad categories: standards and methods, rating systems and services, and commercial tools, including filters, blockers and proxy servers. A discussion of the options in each group follows. While this description of the marketplace is meant to be complete, it is by no means exhaustive. ITAA invites suppliers, sponsoring organisations and users of solutions not cited here to contact the Association. This document will be maintained on the ITAA home page (http://www.itaa.org) and updated as new information becomes available.

Before getting to specifics, a few observations may be useful. First, access control strategies are as diverse as the products and services themselves in this growing segment of the marketplace. For instance, many systems require proof of age before providing access to their content. This may or may not be a desirable feature. "Proof of age" systems require a judgement call on the part of those providing the content. This judgement call is made by someone who may have nothing in common with an individual's ideals as a parent or teacher. Other content providers are now requiring customers to have a registration on file that proves they are over 18 years of age. Some are using a credit card or an Internet FirstVirtual account number as proof of age.

Several online systems have proprietary environments which screen content for children. The parent requests that a child's account be placed into this environment. In this approach, the online service provider's performance depends on how efficiently and effectively this "safe space" operates. Other online services and commercial products set limits on the amount of time a child may spend on the service or the size of files that may be downloaded.

6. Standards and Methods

Standards and methods are generally pre-competitive technology and technical ideas provided to software publishers, online services and organisations to create ratings. PICs, discussed in the body of this report, is a leading example of a standard for rating system creation. Compliance with a standard such as PICs assures compatibility among rating systems, navigational products, Internet sites, and content providers.

Automated Collaborative Filtering (A proposal)
Alan Wexelblat *et al.*
Automated Collaborative Filtering

Automated Collaborative Filtering (ACF) is proposed as "a scaleable, community-based solution" to the problem of rating Web sites for content appropriateness. According to the authors, ACF helps like-minded people to communicate about items they like or dislike. Communities of people who share common views and attitudes can use the technology to help each other decide on appropriateness, "rather than relying on simpleminded keyword-blocking centralised censorship". Participants not only share ratings about items viewed, but the predictive nature of the software allows the system to make predictions about never-before-seen documents. Emphasis is placed on not only what to block out, but what - from millions of Internet sites and documents - to include for users too busy for extended exploration.

KidCode
First Virtual Holdings
25 Washington Avenue
Morristown, NJ 07960
201-540-8967

KidCode is a voluntary, open, non-proprietary naming convention which informs Web browsers if and when site content is inappropriate for children. The naming conventions are applied to the fixed address of the site, alerting the tool to the nature of the unsuitable material (an alternative approach applies the naming convention to the standard Web form mechanism). KidCode labels indicate the minimum age for viewing material and provides a set of textual descriptive category names, indicating the reason for restricting access. Adults decide how to configure browsers, based on these age and category criteria.

SafeSurf
16032 Sherman Way
Van Nuys, CA 91406
818-902-9390
SafeSurf

SafeSurf is a parents' organisation which has developed the SafeSurf Rating System. The SafeSurf plan creates what it calls a "cyber-playground" by providing sites that are appropriate for children with a child safe coding standard. Sites which do not adopt a code would become invisible to children surfing the Internet. Each child participating in the plan would receive a password from an Internet service provider; use of the password would act as a signal to third-party filtering software to accept only content from those sites marked "appropriate for children". Sites can be marked so as to identify information which is appropriate for children and not appropriate for children. Parents can specify varying levels of content to be blocked, based on the age of the child. The SafeSurf Rating Standard is not only used to rate sites, but also to identify and classify content.

7. Voluntary Internet Self-rating

Alex Stewart

A proposed rating system consisting of content labels placed with a document or other content on the Internet and a series of standard rating codes. Examples of the latter include: L (may contain language

unsuitable for some readers); M (May contain material unsuitable for some readers); S (May contain textual depictions of sexual acts); or D (May contain disturbing textual content).

8. Rating Systems and Services

Rating systems are actual ratings schema. Rating services involve the creation of one or more ratings systems to meet the diverse needs of a given constituency. Rating systems could be developed by a commercial company, political organisation, church group or other entity. Some firms combine an Internet browser, filter or other tools with a rating service to offer a complete business or consumer market solution. This type of multi-function product or service provider is discussed under Commercial Tools and Online Services.

The Interactive Digital Software Association

The Interactive Digital Software Association (IDSA), represents cartridge/CD-ROM game manufacturers such as Atari, Sega and Nintendo. The group's Entertainment Software Rating Board places products into five motion picture industry-like categories: early childhood (ages 3 and up); kids to adults (ages 6 and older); teens (ages 13 and older); mature (over 17); and adults only. Each category can have several descriptors.

Recreational Software Advisory Council
1718 M St., N.W.
Suite 139
Washington, D.C. 20036
202-293-3055

The Recreational Software Advisory Council (RSAC) is an independent, not-for-profit organisation which provides, promotes and administers a content-labelling rating system for recreational software and other media. The association seeks to provide parents and consumers information about the level of violence, sex and vulgar language within interactive media.

The RSAC method consists of polling software publishers on the existence of objectionable material (violence, nudity/sex, language) in their products. The RSAC questionnaire identifies and scores such content, employing what it calls "branching" logic. Based on a published algorithm, the method seeks to eliminate subjectivity. For instance, products receive a maximum violence rating (Level 4) if they contain gratuitous or extreme violence; they can receive no rating for violence if the action depicted meets the association's definitions for terms like "strategic aggression" or "sports violence". The rules-based approach taken to nudity/sex and language sections are similar.

An RSAC-rated computer game system can have four possible labels:

•"All" (no objectionable material and suitable for all audiences)
•The violence icon, a bomb, indicates a game contains violent scenes or action. The differences range from "creatures injured" at level one to torture and rape at level four.
•The nudity and sex icon shows an eye peeping through two split fingers. Levels ranging from "revealing attire; passionate kissing" to "provocative frontal nudity" and "explicit sexual activity; sex crimes".

•The language icon shows an exclamation point in a cartoon dialogue balloon. Variations are from “mild expletives” to “crude or explicit sexual references”.

The Web Rating Council
Decade Communications

The Web Rating Council seeks to establish a uniform rating system for Web pages and sites. A synopsis of this group’s ratings are as follows:

•Adult Users: Adult themes which may or may not have a sexual orientation.
•General Users: Suitable for most computer users.
•Graphic Violence: Content of a graphic violent nature, fiction or non-fiction.
•Mature Users: Suitable for those over 13 years of age. Parental guidance advised.
•Not Rated: Content not yet rated. May contain items of any type. Under 18 should not visit; parental controls strongly advised.
•Public Domain: Content without ownership rights; may be freely used for any purpose.
•Sexual Content: Contains content of a sexual nature.
•Explicit Sexual Situations: Highly explicit sexual nature. May be offensive to some users. Over 18 years old only.

9. Commercial Tools and Online Services

The following products and services are commercially available and are sold in total or in part to provide access control to Internet or other online services.

AOL Parental Controls
America Online
8619 Westwood Centre Dr.
Vienna, VA 22182-2285
800-827-6364; 703-448-8700

America Online (AOL) provides parental blocking in a proprietary interface. UseNet text downloads of more than 1 Kbyte require master screen name. Access can be blocked to chat rooms or discussion groups. Child access privileges can be limited to AOL’s “Kids Only” offerings. These include chat, message boards, Disney and DC Comics features, and an encyclopaedia. Parental Controls can be customised for teenagers as well. AOL provides telephone help, detailed instructions and advice for parents. A password must be used to disengage the blocking capability. The service is free. AOL also announced plans in July 1995 to add SurfWatch software tool capabilities as an extension of its Parental Controls to the Internet.

CyberPatrol
Microsystems Software
600 Worcester Rd.
Framingham, MA 01701-5342
800-489-2001; 508-879-9000
CyberPatrol

Cyber Patrol is an Internet access management utility. Product features allow parents to restrict access by time of day, total amount of time spent online per day, Internet resources and sites by content, and online service or client applications. Reports total use of Internet and other applications. Cyber Patrol provides

two levels of password authorisation: headquarters and deputy, allowing authority to be delegated. A separate CyberNOT Block List maintained by Microsystems rates sites for questionable material and divides content into categories. Access to content can be blocked at both the file directory and page level.

CYBERSitter TattleTale
Solid Oak Software, Inc.
Post Office Box 6826
Santa Barbara, CA 93160
Sales 1 800 388 2761
Fax 805 967 1614
EMail:info@solidoak.com
CYBERSitter TattleTale

Cybersitter blocks a child's access to adult-oriented material and pornography on the Internet and alerts the parent. Attempts by children to download or view an adult-oriented Web site, Internet Newsgroup or picture automatically abort and the system creates an alert for later parent viewing. Cybersitter also eliminates offensive and suggestive language from incoming and outgoing e-mail, newsgroups, Web sites, downloaded files and e-mail attachments. The product can block access to user-specified games, files and programmes.

InterGo
TeacherSoft Corp.
903 E. 18th St., 2nd Floor
Plano, TX 75074
214-424-7882
InterGo

InterGo is a tool which combines browsing, searching, e-mail, file transfer, Telnet, virus scanning, screening, news and extensive reference content. The product incorporates the company's KinderGuard security screen and the SafeSurf rating system. KinderGuard blocks a child's access to unsuitable material from Web and gopher sites, ftp archives, news groups and mailing lists. KinderGuard ratings are created by an in-house editorial review board, screening on sexual and violent content. A Web crawler searches for objectionable terminology. Rating codes have been adapted from the video game industry. The product also includes an automated customer feedback system.

Internet Filter
Turner Investigations, Research and Communication
Box 151, 3456 Dunbar St.
Vancouver, BC, Canada
V6S 2C2
Phone/Fax: (604) 733 5095
internet : bturner@direct.ca
Internet Filter

Internet Filter is a parental control programme for blocking or logging all data transfers, including World Wide Web pages, newsgroups, and IRC sessions.

Internet in a Box for Kids and KidNet
CompuServe/Spry Inc.
316 Occidental Ave., S, Ste. 200
Seattle, WA 98104
800-SPRY-NET; 206-447-0300
Internet in a Box for Kids and KidNet

CompuServe has a pair of projects in the access control area, KidNet and Internet in A Box For Kids. KidNet will be a "child-safe" online service featuring closely monitored interactive games, shopping, messaging, and chatting areas. Other chat areas can be blocked upon request. Family members share a single password, so no inappropriate activity can be hidden.

In March, 1995, CompuServe acquired Spry, Inc., maker of Internet in a Box. Internet in A Box For Kids will contain a programme called, “Crossing Guard” for access control to inappropriate sites on the Internet. Crossing Guard will also contain a travel log of a child’s site visits and a time-out feature to limit the duration of net visits. The product comes with pre-set location restrictions. In addition to these offerings, CompuServe offers its members aggressive patrolling of complaints, alerts online and through publications, including its monthly magazine.

Net Nanny
Trove Investment Corporation
Main Floor 525 Seymour Street
Vancouver, B.C. Canada, V6B 3H7
Email:netnanny@netnanny.com
Net Nanny

An Internet parental control tool with special features which prevent a user’s address, phone and credit card numbers from appearing on the Internet. The product can also be used to block other sensitive information from being transmitted on the Internet. Loading, downloading and use of unauthorised software or CD-ROMs can be stopped. PCs can be set to eliminate transmissions with specific words or phrases, transmissions to specific sites, or transmissions on specific subjects. Violations can result in monitoring, application shut down or complete system shut down.

NetSheperd
Internet Filtering Systems, Inc.
202 1212 31St Avenue, N.E.
Calgary, Alberta T2E7S8
403/258-5804
NetSheperd

Net Shepherd “democratically” rates and filters World Wide Web sites and selectively supervise access. Net Shepherd is a PICS-compliant rating and filtering solution. The product provides the ability to filter documents viewed by children selectively. Parents can choose from a variety of rating databases that represent the accumulated ratings from others who hold similar views and philosophies. Organisations that wish to create rating databases for their subscribers will also be able to use Net Shepherd.

Netscape Proxy Server
Netscape Communications
501 E. Middlefield Rd.
Mountain View, CA 94043
800-NETSITE; 415-528-2600
Netscape Proxy Server

Designed primarily for corporate environments, the Netscape Proxy Server is designed to increase a user's speed and security when accessing the Internet via firewall or low-bandwidth network link. The offering features basic access authorisation, requiring a username and password. Outbound access control allows companies and organisations to restrict employee visits on the Internet.

NewView
558 Brewster Ave.
Redwood City, CA 94063
415-299-9016
NewView

NewView is a comprehensive site-rating and access management solution. The product rates and indexes acceptable Internet site content according to a range of criteria. The company's software allows adults to make access decisions based on sex, violence or other issues. An Internet directory gateway provides children with 25 000 safe sites. Access to unrated sites is not allowed. Customer profile information, site ratings and usage records on a NetView server, making more storage space available on the client computer. The product can also be set to place time limits on Internet sessions.

NOV*IX for Internet
FireFox Inc.
2099 Gateway Plaza, 7th Fl.
San Jose, CA 95110
800-230-6090; 408-467-1100
NOV*IX for Internet

Geared for the business environment, NOV*IV is a Novell server which provides access to the Internet. This gateway product can be used by companies to specify available sites, thereby limiting their employees' visits to time-wasting or otherwise undesirable portions of the net (the software can also be used to allow access to any site except those specifically blocked). Site access can be blocked using domain name or IP address.

Prodigy and Prodigy Web Browser Junior
Prodigy Service Company
445 Hamilton Ave.
White Plains, NY 10601
800-PRODIGY; 914-448-8000
Prodigy and Prodigy Web Browser Junior

Prodigy is highly "kid-focused", both as a commercial online service and through its Classroom Prodigy (a service provided to schools). The company's "Just Kids" service features an interactive magazine from Nickelodeon, Sesame Street character Big Bird, Carmen San Diego games and an online Baby Sitters Club. Prodigy restricts its subscribers from posting inappropriate messages in public forums or in chat rooms. Parental permission is required to move on to the Internet. Prodigy provides parents with their children's site visit travel logs.

SurfWatch
SurfWatch Software
105 Fremont Avenue, Suite F
Los Altos, California 94022
Phone 415 948 9500
Fax 415 948 9577
SurfWatch

SurfWatch is a software product which blocks access to sexually explicit material on more than 1 500 sites on the Internet. The product screens for newsgroups likely to contain the same content. A separate subscription service updates the data base of blocked sites. Password protection can be used to allow or prevent site access.

Time's Up, Fresh Software Co.
2100 Salzedo Street, Suite 300
Coral Gables, FL 33134
305-444-7745

Times Up is a Windows-based software programme which creates time and access limits for a child's use of games, online services and other programmes. Adults define the limits, and these can vary for each user, programme or day of the week. "Block out" periods keep kids from playing games when they should be doing their homework or chores around the house. Special vacation schedules can give children more time online. The product generates family usage reports for parental review.

WebTrack
Webster Network Strategies
1100 5th Avenue South, Suite 308
Naples, FL 33940
E mail info@webster.com
(800) WNS 0066 or (813) 261 5503
Fax (813) 261 6549
WebTrack

WebTrack allows institutions to control Internet access of employees. Network administrators set restrictions on access to sites, classified into 15 categories: sex, games, gambling, lifestyles, job search information, drugs, criminal skills, alternative journals, hate speech, personal pages, worthless, online merchandising, sports, and humour. When access is denied, the product displays a corporate "acceptable use statement" on the screen. The system generates logs for instant replay of visited sites.

WinWatch Home
Crown Computer Products,
Plantation Road,
Burscough Industrial Estate,
Lancashire, L40 8JT
Phone 01704 895 815

WinWatch Home provides Internet filtering and is shipped with a database of objectionable sites. The software can be configured so that keywords or phrases trigger the shutting down of the Windows operating system. Other controls include time out, usage logs, and locking of other Windows applications on the personal computer.

Section II. Future Activities

A. Technology

A substantial effort is under way in the private sector in the United States that will improve the technological tools available to users of the World Wide Web for the purposes of filtering. This effort is being led by both industry, which seeks opportunities to offer new products and services to individual and business users of the Internet, and by universities and research institutions, which are developing the technological elements that will be needed for advanced filtering services. This effort has involved progress thus far in at least two areas that will help define future generations of content filtering tools.

First, the use of intelligent agents to examine, evaluate, and filter content. Intelligent agents, or sophisticated software that can be launched into a network environment and intelligently examine content with the purpose of evaluating or grading it, exist and operate today. The task being pursued today is to increase the intelligent capabilities of these agents by giving them independent abilities to evaluate and grade content based on more than basic syntax. This involves the recognition of context. A new and more sophisticated generation of such intelligent agents will emerge from this research over the next few years to address a variety of computer-based functions. One of them will enable Web users to inform their own intelligent agent(s) about what kind of content they do or do not want to access and for those agents to examine and evaluate content as it is encountered. Such tools will also permit the Web users' agents to learn from any mistakes made by incorporating the users' reactions into its own programmes. Second, the ability of filtering tools to examine and evaluate images in addition to text. Most automated filtering technology today relies on the evaluation of text. Images present a far more complex subject of evaluation since their variety and complexity is so great. But a substantial effort is under way at institutions like MIT, Columbia University, and elsewhere, to develop filtering tools that can discriminate based on fine differences among images. This will eventually lead to the development of tools that can help Web users automatically filter in or out the images that make sense to them.

B. The Environment

The next several years will see a significant growth in the availability of Web content rating and filtering tools and services and as a result the use of such tools. The industry's standard for content filtering, PICS, is just now emerging and although it will take a short while to become recognised and deployed, once it is it will enable a rich variety of services to emerge. Less than half of all Web browsers in use today are enabled for PICS, which means that for Web site operators, going through the effort to include a PICS-based content rating may be of questionable value. Similarly, less than half of all Web servers in use today are PICS-enabled, which means that for a Web surfer, relying entirely on a PICS-rating can be frustrating. Today, every major provider of Web server and Web browser technology is either offering PICS-enabled products or is committed to do so soon. As a result, over the next year or so, the proportion of both browsers and servers that are PICS-enabled will increase dramatically, most expect to over 90 per cent. As this happens, PICS-based content rating will be easy to implement and will become virtually ubiquitous. Perhaps more importantly, with the entire Web market PICS-enabled, prospective third-party Web rating services will have a much greater incentive to invest in the development of their rating services. These third-party rating services will help parents enormously in identifying content that they do or do not wish their children to access on the Web. As the PICS-based Web content rating environment strengthens, Web users will come more and more to rely on such tools to help them make sense out of a rapidly growing and complex medium.

Council of Europe

The Internet is commonly recognised as a new information network, which is rapidly developing and operates within the framework of existing national and international standards regulating content and conduct in speech or the traditional media. Since the Internet is part of the current and future services offered by means of digital information systems, content and conduct standards for the Internet should be compatible with those applicable to other digital services.

The issue of "content and conduct on the Internet" relates to a range of subjects, which have been or are currently being examined within the Council of Europe.

Freedom of expression and information

Article 10 of the European Convention on Human Rights guarantees the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Everyone within the jurisdiction of the Parties to the Convention enjoys this right. Article 25 of the Convention opens the possibility to any person, non-governmental organisation or group of individuals to file a petition with the European Commission of Human Rights against the violation of this right by a Party to the Convention. A possible subsequent decision of the European Court of Human Rights has to be complied with by the respective Party to the Convention.

Therefore, any regulation which limits freedom of expression via the Internet or other new communications technologies and is applied within the jurisdiction of the Convention, must be in conformity with Article 10 of the Convention.

The Committee of Ministers of the Council of Europe reiterated, in its Declaration on the Freedom of Expression and Information of 1982, the firm attachment by member states to the principles of freedom of expression and information as a basic element of democratic and pluralist society and declared, that in the field of information and mass media member states must seek to achieve "absence of censorship or any arbitrary controls or constraints on participants in the information process, on media content or on the transmission and dissemination of information".

The 5th European Ministerial Conference on Mass Media Policy [Thessaloniki, 11-12 December 1997, MCM (97)15] on "The Information Society: A Challenge for Europe" addressed the exercise of freedom of expression and information within the framework of new information services and put it in relation to other rights and interests possibly at stake by the use of these services. The Political Declaration, Resolutions and Statement adopted at the Conference are available at <http://www.dhdirhr.coe.fr/media/home.htm>. On the basis of the political decisions taken at the Ministerial Conference, the Steering Committee on the Mass Media and, in particular, its Group of Specialists on the Impact of New Communications Technologies on Human Rights and Democratic Values continues to examine the various issues raised in this respect with a view to formulating possible pan-European standards. Canada has requested to participate in this work as a non-member state.

Right to privacy

The interception of correspondence via the Internet, the sending of unsolicited information or the processing of personal data in connection with the use of the Internet are just some issues related to content (*i.e.* personal data) and conduct (*i.e.* breach of privacy). In this respect, the right to one's private and family

life, home and correspondence is guaranteed by Article 8 of the European Convention on Human Rights and safeguarded by the European Court and Commission of Human Rights.

In addition to this general norm, content and conduct on the Internet can fall under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 as well as Recommendation No. R(95)4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services.

The implications of the development of new information and communications technologies on privacy and data protection are currently being examined within the Council of Europe by Working Group No. 15 of the Project Group of Data Protection and the Group of Specialists on the Impact of New Communications Technologies on Human Rights and Democratic Values.

Harmful and objectionable content and conduct

Harmful and objectionable content can be disseminated by all types of media, not only by the Internet, although the possible number of authors and recipients, the speed of dissemination and the resources necessary for dissemination distinguish the impact of such content on the Internet from the traditional media. The standards for the evaluation of harmful and objectionable content should, however, be identical.

In this respect, Recommendation No. R(89)7 concerning principles on the distribution of videograms having a violent, brutal or pornographic content and Recommendation No. R(92)19 on video games with a racist content can serve as a guideline for Council of Europe member states. Two draft Recommendations on "the portrayal of violence in the electronic media" and on "hate speech", which have been prepared by the Steering Committee on the Mass Media and are currently before the Committee of Ministers with a view to their adoption, are also of relevance in this area.

Illegal content and conduct

National criminal laws seem to cover the Internet with respect to illegal content, *i.e.* content violating criminal laws, and illegal conduct, *i.e.* the violation of criminal laws by using the Internet. The inherently international or cross-border character of the Internet and new information technologies in general require, however, international rules on the applicability of national laws and the jurisdiction of national courts.

The European Committee on Crime Problems, therefore, elaborated Recommendation No. R(89)9 on computer-related crime and Recommendation No. R(95)13 on the problems of criminal procedural law connected with information technology. The European Committee on Crime Problems has established the Committee of Experts on Crime in Cyberspace, which has been mandated by the Committee of Ministers to examine the feasibility of drawing up a convention on this subject. The wider than pan-European character of cyberspace is reflected in the composition of the Committee, which comprises also the non-member states Canada, Japan and the United States. Council of Europe conventions can also be open for signature by non-member states.

Recommendation No. R(91)11 concerning sexual exploitation, pornography and prostitution of and trafficking in children and young adults, addresses issues of relevance to the current international discussion on the use of the Internet in this field.

Pluralism of content

The cultural challenges of new information technologies are currently being examined by the Project Group on New Technologies of the Culture Committee.

It should also be noted that the Second Summit of Heads of State and Government of the Council of Europe's member states (Strasbourg, 10-11 October 1997) will probably address new information technologies and provide the Council of Europe with further lines of action.

European Commission

Definition and description

The definition of the main concepts such as typology of functions or responsibilities is of fundamental importance. Other complementary work in the EU is currently dealing with these matters :

- Implementation of a study on liabilities has been planned.

- The Green Paper: during the consultation, a Europe-wide consensus emerged on a blueprint for the assignment of responsibility to the different operators involved in the communication chain. Liability is determined by degrees according to the operator's function(s) and the extent to which he has direct contact with the content.

The Bonn Ministerial Declaration also contains the following passage on responsibility:

41. Ministers underline the importance of clearly defining the relevant legal rules on responsibility for content of the various actors in the chain between creation and use. They recognise the need to make a clear distinction between the responsibility of those who produce and place content in circulation and that of intermediaries.

42. Ministers stress that the rules on responsibility for content should be based on a set of common principles so as to ensure a level playing field. Therefore, intermediaries like network operators and access providers should, in general, not be responsible for content. This principle should be applied in such a way that intermediaries like network operators and access providers are not subject to unreasonable, disproportionate or discriminatory rules. In any case, third-party content hosting services should not be expected to exercise prior control on content which they have no reason to believe is illegal. Due account should be taken of whether such intermediaries had reasonable grounds to know and reasonable possibility to control content.

43. Ministers consider that rules on responsibility should give effect to the principle of freedom of speech, respect public and private interests and not impose disproportionate burdens on actors.

The issue of responsibility is acknowledged to be one of the most important for governments to deal with and will be further explored by the work under way (draft recommendation, Action Plan) with the help of information collected, *inter alia*, by the DG XV study.

Regulation of content

The EU has been actively studying the issue of content in the new media, with particular reference to illegal and harmful content on the Internet and protection of minors and human dignity in new audiovisual and information services. In this perspective, two studies carried out by the European Commission may be relevant:

- Hydra Study, "The Protection of minors and human dignity in the Information Society".

- COMCRIME study on computer crime.

The work already achieved within the EU, based on the Commission's work within the Working Party and on the Green Paper, has led to broad agreement on the following concepts which bring together the diversity of member states' approaches:

- Illegal content must be distinguished from harmful content. The two categories require different measures to deal with them. The practical steps taken recently by individual member states in both areas are summarised in the second Working Party report.

- The protection of human dignity, a subset of illegal content, must be distinguished from the protection of minors, a subset of harmful content.

- The protection of human dignity refers to a type of restriction to prohibit certain kinds of material considered as intolerable both for the individual and the community at large and as going to the roots of society. Prohibitions on general categories of material detrimental to human dignity such as obscene, contrary to moral or indecent exist in most member states (child pornography, violent pornography, incitement to racial hatred or violence).

- The protection of minors is to ensure that minors do not normally have access to material which could damage their physical or mental development, while at the same time allowing adults access to such material (violence, sexually explicit content, etc.).

Illegal content

Illegal content must be dealt with at source by law enforcement agencies. The industry can help reduce circulation of illegal content through properly functioning systems of self-regulation (such as codes of conduct, establishment of hotlines) in compliance with and supported by the legal system.

Harmful content

In tackling harmful content, the priority actions should be:

- Enabling users to deal with harmful content through the development of actions to increase parental awareness and technological solutions (filtering) and content rating systems.

- Developing self-regulation which can provide an adequate framework, in particular for the protection of minors.

Protection of privacy and personal data

The European Community respects the fundamental rights and freedoms of citizens such as their right to privacy, including secrecy of communications, as well as freedom of expression and speech as laid down in international and European Human Rights Conventions, the constitutions and traditions of its member states. In the particular context of illegal and harmful content on the Internet, together with these fundamental texts, the European Data Protection Directive 95/49/EC lays down general principles for the processing of personal data. In addition, the draft directive on privacy in the telecommunications sector contains complementary requirements for the protection of privacy and the processing of personal data in the context of public telecommunication networks. These principles strike the necessary balance between different interests: the right of the individual to remain anonymous in the online world and limitations to that right only in so far as strictly necessary in a democratic society, for example to prevent, investigate and prosecute criminal offences. These legal requirements have also to be implemented by technical means, such as the provision of anonymous reading, browsing and e-mail facilities and in general the concept of privacy-enhancing technologies for access to, use of and payment of online services.

Non-regulatory initiatives

These issues have already been addressed by the Communication and the Green Paper will form a central part of future EU activity (draft recommendation, Action Plan).

- The Working party has recognised the importance of self-regulation and the Action Plan will investigate some of its aspects.

- The draft recommendation which will follow up on the Green Paper will provide for adequate safeguards within a flexible legal instrument in order to encourage the development of new services.

Illegal and harmful content on the Internet

Communication on illegal and harmful content on the Internet

The Communication[82] was adopted on 16 October 1996. It has been debated by the European Parliament and the Committee of the Regions, who have adopted reports. It sets out proposals from the Commission for immediate action to deal with harmful and illegal content.

Working party on illegal and harmful content on the Internet

The Telecommunications Council of 27 September 1996 agreed to extend the Working Party established previously to include representatives of the Ministers of Telecommunications as well as access and service providers, content industries and users. The Council requested the Working Party to present concrete proposals for possible measures to combat the illegal use of Internet or similar networks. The first report[83] was submitted to the Council on 28 November 1996. The report follows the proposals made in the Communication and elaborates on a number of issues such as self-regulation and liability.

A second report,[84] submitted to the Council on 27 June 1997, sets out the progress made in the member states on measures to deal with illegal and harmful content and summarises activities since then in the EU institutions.

Council Resolution on Illegal and Harmful Content on the Internet

This resolution[85] was adopted on 17 February 1997. The Council and representatives of member states welcomed the report of the Commission Working Party on illegal and harmful content on the Internet. They invited the member states to commence with the following measures:

- Encourage and facilitate self-regulatory systems including representative bodies for Internet service providers and users, effective codes of conduct and possibly hotline reporting mechanisms available to the public.

- Encourage the provision to users of filtering mechanisms and the setting up of rating systems for instance the PICS (Platform for Internet Content Selection) standard launched by the international World Wide Web consortium with EC support should be promoted.

- Participate actively in the International Ministerial Conference to be hosted by Germany and encourage attendance by representatives of the actors concerned.

They requested the Commission, as far as Community competencies are concerned, to:

- Ensure the follow-up and the coherence of work on the measures suggested in the above-mentioned report, taking into account other relevant work in this field and to reconvene the Working Party as necessary to monitor progress and take further initiatives if appropriate.

- Foster co-ordination at Community level of self-regulatory and representative bodies.

- Promote and facilitate the exchange of information on best practice in this area.

- Foster research into technical issues, in particular filtering, rating, tracing and privacy-enhancing technologies, taking into account Europe's cultural and linguistic diversity.

- Consider further the question of legal liability for Internet content.

They recommended that the Commission, in the framework of Community competencies, and member states take all necessary steps to enhance the effectiveness of the measures referred to in this Resolution through international co-operation, building on the results of the International Ministerial Conference and in discussions in other international forums.

European Parliament resolution on illegal and harmful content on the Internet.

On 24 April 1997, the European Parliament adopted a Resolution on the Commission Communication on illegal and harmful content on the Internet, based on a report[86] by M. Pierre Pradier. The Resolution contains a list of desiderata addressed to the Council, the Commission and the member states.

With respect to illegal content, the Resolution *inter alia* (1) calls on the member states to define a minimum number of common rules in their criminal law and to strengthen administrative co-operation on the basis of joint guidelines and (2) calls on the Commission to propose, after consulting the European Parliament, a common framework for self-regulation at EU level.

This framework should include: su

1. Objectives to be achieved in terms of the protection of minors and human dignity.

2. Principles governing the representation of the industries concerned at EU level and the decision-making procedures.

3. Measures to encourage the enterprises and industries involved in telematic networks to develop message protection and filtering software, which should be made available automatically to subscribers.

4. Appropriate arrangements for ensuring that all instances of child pornography uncovered on computer networks are reported to the police and shared with Europol and Interpol.

Furthermore, the Resolution stresses the need for international co-operation between the EU and its main external partners, on the basis of conventions or via the application of new international legal instruments and it calls upon the Commission to submit proposals for a common regulation of liability for Internet content. Finally, it urges the member states and the Commission to promote co-operation among Internet access providers, in order to encourage self-regulation.

With respect to harmful content the Resolution calls on the Commission and the member states to encourage the development of a common international rating system compatible with the PICS protocol, and sufficiently flexible to accommodate cultural differences, which will benefit both users and content publishers.

Action Plan on Illegal and Harmful Content on the Internet

The Rolling Action Plan on the Information Society adopted in December 1996 included a reference to an Internet action plan.

> "The Communication on illegal and harmful content ... indicates a number of policy options to combat this type of content on the Internet. The action plan ... will indicate the range of measures necessary to implement these policy options, the means to do this and the actors responsible. It will elaborate the measures necessary to ensure a coherent set of actions at the EU level and will especially address the question of liability for access and service providers."

The Internet Action Plan will be presented to the Council in December 1997.

Green Paper on the Protection of Minors

The *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*[87] [COM(96) 483 final] was adopted by the European Commission on 16 October 1996, together with the Communication on *Harmful and Illegal Internet*. The Green Paper has provided all those involved in the audiovisual and information sectors of Europe and beyond with a springboard for reflection and debate. Its scope is the much needed adaptation of regulatory frameworks and attitudes in the context of the emergence of new audiovisual and information services across the spectrum from television to the Internet with a specific focus on "the protection of minors and human dignity". The Communication, on the other hand, whilst concentrating on the Internet has a broader scope in terms of tackling "illegal and harmful content". The two instruments thus complement each other in that they address a number of issues

in different ways. In this context, the OECD questionnaire is welcome as it may contribute new insights into these issues.

Answering question II.9, it is likely that the anticipated analysis on existing legislation and practices will actually address "open information and communications networks". The study should therefore be restricted to the Internet and should not be extended to include cable, telecom and broadcasting as the latter services already fall within existing national and European legislative frameworks.

As regards the scope of the OECD study, the Commission, in writing the Green Paper, is fundamentally committed to the ethical dimension of "information content and online conduct" as it is an important element of new services which requires attention to increasing public awareness and greater responsibility on the part of the industry and the public as a whole. Therefore, an "attempt to incorporate an ethical dimension to this study" (see §9) is essential in continuing research into new services. It is not advisable to tackle these issues without first addressing the very concept of what is actually harmful in the new services.

The global nature of these information systems makes a concerted approach at the European level essential. As emphasised in the Green Paper and as outlined in the OECD questionnaire, free expression and exchange of ideas are not only a basic tenet of European citizenship, but also a cornerstone of the emerging communication culture. Europe has a role to play in facilitating progress in these issues on an international level.

Consultation on the Green Paper and Follow-up

The Green Paper is the first stage of a medium to long-term project in which a large number of public and private institutions and organisations are joining forces. The Commission called upon interested parties to voice their reactions to the Green Paper at two consultation meetings held in Brussels on the 4th and 27th of February 1997. Professionals and representatives of national governments extensively reviewed and discussed the issues which the Green Paper raised. Apart from these formal consultations, the Commission has received over 50 written submissions which are currently under analysis.

The Council of Ministers, on 16 December 1996, welcomed the Green Paper and requested the Commission to further its work and present its results at the forthcoming Audiovisual/Culture Council on 30 June 1997. The Green Paper is also currently being debated by the other Union institutions (the European Parliament, the Economic and Social Committee, the Committee of the Regions). The report drafted by M. Philip Whitehead was adopted by the Culture Committee on 19 June 1997.

When presenting the **results of the consultation**[88] on the Green Paper on 30 June 1997 to the Council which displayed a broad measure of agreement with the Commission's approach, Commissioner Oreja announced his intention to present a Communication and draft Council Recommendation in autumn 1997. This could include a co-ordination of national initiatives through the adoption of common principles for conduct, orientations and objectives for action by member states.

Activities in the Field of Justice and Home Affairs

The Dutch Presidency of the EU has launched, in the context of the structures of the Justice and Home Affairs Council, a reflection exercise on the Internet issue. It produced a working document, within the police co-operation working party, to allow for legal interception of Internet communications. A more general paper was also produced containing a number of further recommendations, still to be examined by the experts, with a view to developing practical co-operation among the law enforcement authorities

concerning Internet related activities. In the process of drafting a convention on mutual assistance, which concerns judicial co-operation in criminal matters, the question of possible need for a specific provision for Internet was raised. The working group considered that to be premature at this stage, since most member states have at present little or no experience of particular difficulties in the field of judicial co-operation in relation to offences perpetrated by the use of the Internet. Hence, work is being carried out with a view to investigating any measures which can be considered in the context of the "third pillar" comprising both the police and mutual judicial assistance in criminal matters involved in the use of the Internet.

The P8 Senior Level group on transnational organised crime (Lyon group) has started work to develop legal and technical mechanisms that allow for timely international law enforcement response to computer-related crimes *i.e.* to enhance abilities to locate, identify and prosecute criminals; co-operate with and assist one another in the collection of evidence; and commit resources to training law enforcement personnel to fight high-tech and computer related crime.

The COMCRIME study on legal aspects of computer-related crime in the information society, under the direction of Prof. Ulrich Sieber and Prof. Rik Kaspersen, will be reporting in autumn 1997. The report will cover:

> An in-depth analysis of the substantive law aspects describing the situation in the European Union, the United States, Canada and Japan. Not only specific penal sanctions for specific criminal acts, but the interrelation with civil and administrative law should be studied. The basis of the analysis will be the list in Recommendation 89 (9) of the Committee of Ministers of the Council of Europe as well as national laws, and the scope includes dissemination of illegal content on the Internet.
>
> The description of procedural law aspects: by its nature, computer crime is not strictly bound to a limited physical environment, but can be carried out world-wide very easily and at relatively "low cost"; therefore, it is a matter of international concern. Moreover, harmonising substantive law means creating a situation of "double incrimination", a formal condition for international co-operation in criminal matters. Expertise, search powers and mutual assistance in law enforcement are key questions in this field.

Its results will be feeding the on-going work on the implementation of the Action Plan to combat organised crime endorsed by the European Council in Amsterdam[89] and which includes a recommendation to combat the use of new technologies and means of communication, including the Internet, by organised criminals.

International Ministerial Conference, Bonn

The International Ministerial Conference entitled “Global Information Networks: Realising the Potential” was held in Bonn on 6-8 July 1997. The Conference was hosted by the Federal Republic of Germany and organised in co-operation with the European Commission. Ministers from 29 European countries took part (European Union, EFTA, Central and Eastern European countries and Cyprus), as did government representatives from the United States, Canada, Japan and Russia as guests, businesses which are global players (content providers, access and service providers, network providers, equipment manufacturers), representatives of users and as observers, representatives from European Union institutions or organs and from other European and International organisations.

Among themes dealt with were preventing and combating misuse of the Global Information Networks, the importance of industry self-regulation and the availability of technical solutions to provide user empowerment, and responsibility of the actors.

The Conference was concluded by three Declarations: by European Ministers, by industry and by users. These declarations and the Conference Theme Paper are available on the World Wide Web.[90]

Study on Liability

The European Commission, DG XV, has published a call for tenders for a study on legal liability systems in member states regarding Information Society services. The study will draw up an inventory of laws, regulations, administrative practices and forms of self-regulation which are in existence or in preparation in the member states, and which establish forms of legal liability applicable to operators and users of Information Society services, including copyright and neighbouring rights.

International activities

The issues at EU level have been addressed by the Communication and the Green Paper will form a central part of future EU activity (draft recommendation, Action Plan).

The Commission has identified areas and will promote them to establish a clear and predictable framework within which industry as well as users can realise the potential of the networks. Concrete measures where industry could take initiatives with support and encouragement from governments could include :

- An international network of hotlines (especially dealing with content affecting human dignity such as child pornography).

- Development of compatible rating systems, which take account of cultural and linguistic diversity.

- Exchange of experience between all those involved, in particular industry, self-regulation bodies and users.

ANNEX III: WORK CARRIED OUT BY A NUMBER OF INTERNATIONAL ORGANISATIONS FOR THE PROTECTION OF CHILDREN AGAINST SEXUAL EXPLOITATION

Background

Last January the Belgian Delegation to the OECD submitted a proposal for the deposit of a Convention to outlaw the sexual exploitation and abuse of children on the Internet.

In the follow-up to this proposal, the OECD Council of Ministers which met on 26-27 May 1997 strongly condemned the dissemination on the Internet of child pornography and information that promotes child abuse. Ministers urged that this abhorrent and unacceptable misuse of the Internet be addressed immediately, including in the appropriate international organisations (see the news release by the OECD Council of Minister).

Since June, a number of international organisations were contacted in order to obtain information on the nature and progress of their activities on the subject of child pornography and abuse and to draw their attention to the statement by the OECD Council of Ministers. The following information was obtained from these contacts.

United Nations Organisation

Commission on Human Rights

A draft optional protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography is being prepared by an open-ended inter-session Working Group of the Human Rights Commission. The Working Group's mandate is based on Resolution 1996/85 of the Human Rights Commission.

This Working Group held its third meeting, chaired by Mr. Ivàn Mora Godoy (Cuba), to examine this optional protocol on 3-14 February 1997. It emerged from the general discussion on the main object and scope of the optional protocol that all members of the Working Group considered that urgent action against the sexual exploitation of children was required.

Most of them thought that the future protocol should stress preventive measures, the classification of the acts concerned as offences under criminal law, and the rehabilitation of the victims. Many delegations also felt that the protocol should include the promotion of international co-operation in the administrative and legal fields. Lastly, some delegations considered that the protocol should have a special clause prohibiting the dissemination via electronic media such as the Internet of pornographic material involving children.

No agreement has been reached so far on the last proposal, or for that matter on the rest of the text.

A letter has been sent to the High Commissioner in order to draw his attention to the statement by the OECD Council of Ministers.

Working Group on Contemporary Forms of Slavery

This Group belongs to one of the Sub-commissions of the Commission on Human Rights: the Sub-commission on Prevention of Discrimination and Protection of Minorities. Its mandate is very wide (trafficking in human beings, protection of minorities).

The Group carries out investigations in various fields covered by its mandate and produces an annual report for the Sub-commission in which it proposes the adoption of resolutions, recommendations and guidelines.

With regard to the sexual exploitation of children and, in particular, problems arising from the use of the Internet, it does not seem that the work carried out by the Group will lead to any specific action being taken in this field.

Council of Europe

The Council of Europe recently set up a Committee of Experts on Crime in Cyber-Space which is to examine the following issues in particular:

- Cyber-space offences, in particular those committed with the use of telecommunication networks, such as those which violate human dignity and the protection of minors.

- Definitions, sanctions and responsibility of the parties concerned, including Internet service providers.

- The use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment (interception of telecommunications, electronic surveillance of information networks, etc.).

- Jurisdiction in relation to information technology offences (determination of the place where the offence was committed, resolution of jurisdiction conflicts, etc.).

- International co-operation in investigations.

This Committee held its first meeting on 14-16 April 1997.

Its first decision was to check whether any offences that might be committed in cyberspace were in a class by themselves (*sui generis*), or whether they were not covered well enough in certain cases by existing legal provisions. For the same reason the Committee decided to study the legal instruments previously adopted by the Council of Europe in similar fields with a view to adapting them to the case of cyberspace.

The Committee considered that its mandate was mainly concerned with the definition of responsibilities (of access providers in particular), sanctions and jurisdiction rules.

The Committee's next meeting will be held on 29-31 October 1997.

It is to be noted that Canada, Japan, the United States, Interpol and Unesco are taking part as observers in the activities concerned.

A letter has also been sent to the Chairman of the Committee of Experts on Crime in Cyberspace in order to draw his attention to the statement by the OECD Council of Ministers.

European Union

The international impact of the Dutroux case and the conclusions reached by the World Congress held in Stockholm in August 1996 calling for action against the commercial sexual exploitation of children have led to joint actions by the European Union against the abuse and sexual exploitation of children.

The first joint action was adopted in November 1996. Under a programme known as "STOP" (Sexual Trafficking of Persons), which was also adopted by the Council (Justice et Affaires Intérieures) in November 1996, this action is being implemented under the supervision of the "STOP Committee".

The second joint action was adopted on 24 February 1997 by the Council on the basis of Article K.3 of the Treaty on European Union. It is aimed at stepping up action to combat trafficking in human beings and sexual exploitation of children (97/154/JIA -- Official Journal of the European Communities, 4.3.97, No.L63/2).

Under this second joint action, each member state undertakes to review its relevant national laws in order to classify as criminal offences the sexual exploitation or abuse of children and trafficking in children with a view to their sexual exploitation or abuse. However, the possession of pornographic material involving minors has been excluded from the range of sanctions enforced by the joint action, the aim being to reconcile the varying opinions within the European Union.

Member states also undertake to provide for extraterritorial jurisdiction with regard to the sexual exploitation of children when the offences are committed abroad by their nationals or habitual residents, although the possession of pornographic material involving minors is excluded from this provision.

Moreover, member states must also take the measures necessary to ensure the appropriate protection for witnesses and appropriate assistance for victims and their families, and grant each other the widest possible judicial co-operation to combat the sexual exploitation of children as well as trafficking in human beings.

Lastly, a third joint action was adopted at the Dublin European Council meeting of 13-14 December 1996, which extended the mandate of the Europol Drug Unit to include trafficking in human beings, as well as trafficking in children with a view to their sexual exploitation.

UNESCO

UNESCO is preparing an international legal instrument to establish a legal framework for cyberspace. One important area in this draft instrument is the protection of minors against sexual exploitation.

A draft resolution on this subject will be submitted to UNESCO member states at their next general conference in October or November 1997.

NOTES

1. 1 July 1997, <http://www.iitf.nist.gov/eleccomm/ecomm.htm>.

2. 6-8 July 1997, <http://www2.echo.lu/bonn./conference.htm>.

3. 18 September 1997, <http://www.ispo.cec.be/infosoc/promo/speech/venice.html>.

4. The IETF is the major standards actor for everything other than HTML and special applications. The IAB deals generally with Internet technical standards and allocating resources (such as addressing). IANA and similar organisations are the recognised authorities on addressing (e.g. on assigning IP numbers to machines). The W3C deals only with the World Wide Web and with the HTTP display and special purpose applications.

5. A “local area network” or “LAN” is usually comprised of computers which are physically located at one site, such as at one company or organisation location, while a “wide area network” or “WAN” has geographically dispersed computers which can be connected to the network via dedicated telecommunications lines.

6. The closed and open network distinction is unclear in the case of proprietary networks (such as America Online or CompuServe), bulletin boards or other kinds of connected networks which can operate as closed systems but with a “gateway” connection to the Internet that may or may not be fixed.

7. Basically, the Internet Protocol (IP) manages addressing, and the Transmission Control Protocol (TCP) manages the packets.

8. For more information on domain names, see Internet Domain Names: Allocations Policies [DSTI/ICCP/TISP(97)2]. In addition, see Management of Internet Names and Addresses (5 June 1998) a Statement of Policy released by the US Department of Commerce, National Telecommunications and Information Administration, available at http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm

9. E-mail is similar to sending a letter through the post. It can be used to transmit messages or any kind of data file directly to one individual or to many individuals on a distribution list. Even where e-mail can be used to distribute messages from one-to-several, it is generally distinct from the one-to-many distribution of other kinds of transmissions because e-mail requires some direct involvement of the sender to select recipients of the message -- it is not fully automatic.

10. Listserv is one kind of automatic mailing list service that operates when a number of users subscribe to a list and any message transmitted to the list is forwarded by e-mail to all the members of the list, either automatically or through a human moderator.

11. Usenet newsgroups are similar to mailing lists in that they allow distribution of messages from one-to-many, but unlike a mailing list it is not necessary to subscribe to Usenet newsgroups in advance. Instead of receiving messages by e-mail as with the mailing list, users can access the newsgroup database of messages at any time. Newsgroups can be moderated or unmoderated.

12. These types of transmissions allow real-time communications, for example as text or audio, via the Internet.

13. Telnet allows a user to access and use a remote computer via a local connection to the Internet.

14. The ftp protocol can be used to transfer files from a remote computer to a local computer; gopher is a mechanism for navigating the files on a remote computer that provides hierarchical menus describing files.

15. The World Wide Web allows a combination of many of the services listed above via a user-friendly, interactive, graphical interface.

16. Hypertext links provide an address or "URL" based on the domain name for the computer which hosts the referenced Web page. The URL acts like a telephone number to direct the browser to the referenced Web page.

17. "Webcasting" sometimes known as netcasting, is the term applied to an emerging group of services that use the Internet to deliver content to users in ways that take on many of the characteristics of other traditional communications services (e.g. print media, audio-visual, telecommunication services). For more information on webcasting, see Webcasting and Convergence: Policy Implications [OCDE/GD(97)221].

18. See the section of this report on existing approaches for more information on countries that have hotlines in place for reporting illegal content.

19. <http://www.dca.gov.au/policy/fwork_4_online_svces/framework.htm>.

20. <http://www.dca.gov.au/aba/invest.htm>.

21. See Annex of Supplementary Information to National Submissions for statute citations to specific federal laws which are being applied in Austria, in terms of obscenity/sexually explicit materials, hate propaganda/hate speech, national security issues, communication of erroneous information, protection of personal information/privacy (in particular direct marketing regulations), and other.

22. The hotline can be reached at <INTERPOL@abacus.at>.

23. The text of the Austrian Telecom Act is available from the Website of the Austrian Ministry of Science and Transport <http://www.telekom.gv.at/telekom/TKG3e/tele0.htm>.

24. For information on specific laws, see Annex of Written Submissions.

25. <http://strategis.ic.gc.ca/nme>.

26. <http://www.iid.de> or <http://www.bmbf.de>

27. Directive 96/46EC.

28. Law No. 675 of 31/12/96.

29. Law No. 676 of 31/12/96.

30. Law No. 269 of 3/8/98.

31. The full text of the new articles appears in the Annex of Written Submissions.

32. For a list of laws applicable to the Internet, see the Annex of Written Submissions.

33. <http://www.mpt.go.jp/>.

34. <http://www.miti.go.jp/>.

35. <http://www.nmda.or.jp/enc/index-english.html>.

36. See "Operation of the first PICS compliant label service bureau in Japan" <http://www.nmda.or.jp/enc/ratingop-english.html>. MITI granted ¥200 million to ENC to develop the filtering system.

37. See <http://www.nmda.or.jp/enc/rating/index.html>.

38. See <http://www.nmda.or.jp/enc/guideline.html> and <http://www.nmda.or.jp/enc/etiquette.html>.

39. <http://www.isocnz.org.nz/isocnz/theispco.html>

40. See <http://childhouse.uio.no/redd_barna/>.

41. "A New Medium: New Legal Issues", Report of an Interdepartmental Working Party on penal, data protection and copyright aspects of the Internet. Document available at <http://www.admin.ch/bakom/>.

42. See Annex of Written Submission for more on US position in relation to the development of the Internet. See also the Clinton Administration's "Framework for Global Electronic Commerce", 1 July 1997.

43. At the Federal level, agencies such as the Federal Trade Commission, the Food and Drug Administration, the Bureau of Alcohol, Tobacco and Firearms, the Federal Communications Commission, and the Department of Transportation have oversight authority to regulate advertising.

44. <http://www.w3.org/PICS/Activity>.

45. <http://www.w3c.org>.

46. <http://www.rsac.org/>.

47. See Annex of Written Submissions for more detailed information on PICS.

48. For a list of rating systems see the Annex of Written Submissions or <http://www.itaa.org>.

49. See Annex of Written Submissions for more detailed information on RSAC rating.

50. See Annex of Written Submissions for more detailed information on the available filtering software.

51. <http://www.solidoak.com/cysitter.htm>.

52. <http://www.surfwatch.com>

53. See the Annex of Written Submissions for more detailed information on specific industry codes of conduct.

54. <http://www.missingkids.com/cybertip/>.

55. Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions [COM(96) 487] <http://www.echo.lu/legal/en/internet/communic.html>.

56. <http://www.echo.lu/legal/en/internet/wpen.html>.

57. Interim report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet <http://www.echo.lu/legal/en/internet/wp2en-toc.html>.

58. Resolution of the Council of the European Union and the Representatives of the Member States meeting within the Council [OJ C70 6.3.97 p 1] <http://www.echo.lu/legal/en/internet/resol.html>.

59. <http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.htm>.

60. [COM(96) 483] <http://europa.eu.int/en/record/green/gp9610/protec.htm>.

61. <http://europa.eu.int/en/comm/dg10/avpolicy/new_srv/comlv-en.htm>.

62. European Treaty Series, No. 108. Opened for signature 28 January 1981.

63. Recommendation No. R(95)4, adopted by the Committee of Ministers of the Council of Europe on 7 February 1995.

64. Recommendation No. R(89) 9 adopted by the Committee of Ministers of the Council of Europe on 13 September 1989.

65. Recommendation No. R(95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995.

66. <http://www2.echo.lu/bonn/conference.html>.

67. INCORE is a consortium of organisations representing Internet service providers, users and content providers at the European level, established in 1997 to address issues related to content on the Internet.

68. ChildNet International is a UK-based charity devoted to promoting the interests of children in international communications <http://www.childnet-int.org>.

69. <http://ue.eu.int/amsterdam/en/conclusions/freedom/main.htm>.

70. < http://www.dca.gov.au/aba/unesco.htm>.

71. Sections of this submission were used in creating the Australian entry in the main part of the Inventory. For ease of reference, and to improve comprehensibility, the full submission is presented here even though this involves some duplication.

72. See <http://www.dca.gov.au/policy/fwork_4_online_svces/framework.htm>.

73. The National Classification Code set out in the Schedule to the Classification (Publications, Films and Computer Games) Act 1995 (Cth) provides for films, publications and computer games to be classified RC that:

(a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or

(b) depict in a way that is likely to cause offence to a reasonable adult, a minor who is, or who appears to be under 16 (whether the minor is engaged in sexual activity or not); or

(c) promote, incite or instruct in matters of crime or violence.

Computer games that are unsuitable for a minor to see or play may also be classified RC.

74. The National Classification Code provides for films (except RC films) that:

(a) explicitly depict sexual activity between adults, where there is no sexual violence, coercion or non consent of any kind, in a way that is likely to cause offence to a reasonable adult; and

(b) are unsuitable for a minor to see; to be classified X.

Note. The Government proposes that the X classification be abolished and a new classification of NVE (non-violent erotica) be created.

The Code provides for films (except RC films and X films) that are unsuitable for a minor to see to be classified R

75. See <http://www.dca.gov.au/aba/invest.htm>.

76. Drafts of some of these codes are available at the following Internet addresses:

CAUDIT, at <http://www.anu.edu.au/people/Roger.Clarke/CAUDIT/Code.html>.

INTIAA, at <http://www.intiaa.asn.au/codeintro.htm>.

SAIA, at <http://www.saia.asn.au/Documents/cofcv1_0.html>.

WAIA, at <http://www.waia.asn.au/Documents/CodeOfConduct.html>.

77. The report is available on-line at <http//www.dca.gov.au/aba/invest.htm>.

78. For ease of reference, and to improve comprehension, some of the sections of this submission that were used to create the Canadian entry in the main part of the Inventory are repeated here.

79. The National Classification Code set out in the Schedule to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) provides for films, publications and computer games to be classified RC that:

(a) depict, express or otherwise deal with matters of sex, durg misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or

(b) depict in a way that is likely to cause offence to a reasonable adult, a minor who is, or who appears to be under 16 (whether the minor is engaged in sexual activity or not); or

(c) promote, incite or instruct in matters of crime or violence.

Computer games that are unsuitable for a minor to see or play may also be classified RC.

80. At the Federal level, agencies such as the Federal Trade Commission, the Food and Drug Administration, the Bureau of Alcohol, Tobacco and Firearms, the Federal Communications Commission, and the Department of Transportation have oversight authority to regulate advertising..

81. <http://www.iitf.nist.gov/ipc/privacy.htm>.

82. Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(96) 487 <http://www.echo.lu/legal/en/internet/communic.html>

83. <http://www.echo.lu/legal/en/internet/wpen.html>

84. Interim report on Initiatives in EU member states with respect to combating illegal and harmful content on the internet <http://www.echo.lu/legal/en/internet/wp2en-toc.html>.

85. Resolution of the Council of the European Union and the Representatives of the Member States meeting within the Council OJ C70 6.3.97 p 1 <http://www.echo.lu/legal/en/internet/resol.html>

86. <http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.htm>

87. COM(96) 483, <http://europa.eu.int/en/record/green/gp9610/protec.htm>

88. <http://www2.echo.lu/legal/en/internet/gpconsult.html>

89. <http://ue.eu.int/amsterdam/en/conclusions/freedom/main.htm>

90. <http://www2.echo.lu/bonn/conference.html>