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

OLIS : 09-Dec-1998
Dist. : 14-Dec-1998

Or. Eng.

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

DSTI/ICCP(98)18/FINAL
Unclassified

PROCEEDINGS OF THE OECD/BIAC FORUM ON INTERNET CONTENT SELF-REGULATION

Paris, 25 March 1998

72759

Or. Eng.

ACKNOWLEDGEMENT

The Business and Industry Advisory Committee to the OECD (BIAC), which co-sponsored the Forum on Internet Content Self-Regulation together with the OECD, would like to thank the ***IBM Corporation*** (which kindly hosted the meeting at its facilities), the ***AT&T Corporation, Groupe Bull***, and the ***Oracle Corporation*** for their contributions that made this sponsorship possible.

TABLE OF CONTENTS

OVERVIEW

The Forum on Internet Content Self-Regulation was held on Wednesday 25 March 1998 at the IBM building at Tour Descartes, Paris-La Défense, France. It was organised by a steering committee comprised of national delegation representatives -- led by the United States and Canada[1] -- and was sponsored under the joint auspices of BIAC and the OECD.

More than 150 participants from government, business, public and private sector international organisations, and advocacy groups attended. Panellists were mainly from industry, with representatives (including several legal experts) from Internet Service Provider (ISP) industry associations and firms, filtering software firms, content providers, and advertisers. Consumer and freedom of speech advocacy groups and one law enforcement agency active in this area were also represented.

The Forum examined various issues in the area of Internet content self-regulation:

- identifying the pressures for self-regulation and their source;
- identifying key industry codes of conduct and corporate practices and why they work;
- identifying user empowerment technology and why it works; and
- government and private sector roles in self-regulation: identifying the conditions for successful self-regulation.

Perhaps the most important theme addressed was the need for ongoing education: of users, parents, teachers, and children about using and taking responsibility for their use of technology; of policy makers; of the business community; and, finally, of law enforcers.

The Forum also identified the need for a partnership between businesses, government and users, particularly in the area of law enforcement. It was stated that users should be included in the development of self-regulation.

Some ISPs expressed concern about their role in co-operating with law enforcement authorities. Many agreed that questions of liability, particularly for content provided by third parties based abroad, needed careful consideration and clarification. Several specifically expressed apprehension about being put in a position of substituting for law enforcement authorities.

A number of areas for self-regulation by the Internet provider industry were identified: with respect to content, the focus was on offensive and illegal content, protection of personal information, censorship, spamming and copyright; in other areas, consumer protection and anonymity were identified.

Self-regulation is being used in a variety of areas where laws of general application are applied to online content. Self-regulation is also responding to market pressures, as in the case of offensive content, where user empowerment technologies are proving to be very valuable. A number of self-

1. The Steering Group which organised the Forum was comprised of representatives from Belgium, Canada, Finland, France, Japan, Hungary, United Kingdom, United States, and the Business and Industry Advisory Committee (BIAC) to the OECD.

regulatory strategies were discussed -- codes of conduct, corporate policies, awareness programmes, hotlines, labelling and filtering software.

Some panellists expressed the view that "soft law" such as codes of conduct should complement "hard law", or that self-regulation needed a legal framework in order to operate usefully and successfully.

Panellists expressed interest in participating in further international dialogues involving the Internet industry, content providers, users and public sector representatives to further promote international collaboration and exchange of experience with respect to self-regulation.

AGENDA

Introductory Remarks by Forum Co-Chairs

Dr. Etienne Gorog, Chair, ICCP/BIAC and Richard Beaird, Chair, ICCP/OECD

Panel No. 1: What are the pressures for self-regulation and where do they come from?

Moderator: Roger Cochetti, IBM (USA)

Panellists:

- Manuel Kohnstamm, Time Warner Europe
- Lisa Balaban, Sympatico/MediaLinx Interactive, L.P. (Canada)

Panel No. 2: What are key industry codes of conduct and corporate practices and why do they work?

Moderator: Yves LeRoux, Digital Equipment Corporation (France)

Panellists:

- Stefano Lamborghini, Associazione Italiana Internet Providers (AIIP) (Italy)
- Walter J. O'Brien, National Advertising Review Council, Inc. (USA)
- Kazuko Otani, Telecom Services Association (TELESA) (Japan)
- Margo Langford, Canadian Association of Internet Providers (Canada)
- Professor Michel Vivant, Université de Montpellier (France)

Panel No. 3: User empowerment technologies and why do they work?

Moderator: Claude Boulle, Groupe Bull (France)

Panellists:

- Marilyn S. Cade, AT&T (USA)
- Akio Kokubu, Electronic Network Consortium (ENC) (Japan)
- Don S. Sandford, NetShepherd, Inc. (Canada)
- Gordon Ross, NetNanny, Ltd. (USA)
- Susan J. Getgood, The Learning Company, Inc. (USA)

Panel No. 4: Government and private sector roles in self-regulation: what are the conditions for successful self-regulation?

Moderator: Peter Upton, Australian Information Industry Association (Australia)

Panellists:

- Markku Ropponen, Internet Service Providers Association (Finland)
- Dr. A. Eisner, Association of Dutch Internet Service Providers (NLIP) (Netherlands)
- Dr. James R. Savary, Consumers' Association of Canada (Canada)
- Christophe Sapet, Association des Fournisseurs d'Accès (AFA) (France)
- Guy Verbeeren, Child Pornography Internet Contact Point / Police Judiciaire (Belgium)

Panel No. 5: General discussion

Moderator: Maria Livanos Cattaui, International Chamber of Commerce (ICC)

Panellists:

- Dr. Michael Baker, Electronic Frontiers (Australia)
- David Kerr, Internet Watch Foundation (UK)
- David W. Phillips, AOL Bertelsmann Online (Europe)

Closing remarks by Forum co-chairs

SUMMARY RECORD

The Forum was co-chaired by **Dr. Etienne GOROG**, Chairman of the BIAC Committee on Information, Computer and Communications Policy, and **Richard C. BEAIRD**, Chairman of the Information, Computer and Communications Policy Committee of the OECD. The Forum was organised to consider self-regulation for Internet content by looking at initiatives and technologies which can be used to address issues related to harmful and illegal content on the Internet. Dr. Gorog emphasised the importance of technological solutions, and urged the private sector to make a range of technological tools available to Internet users to enable them to exercise choice about the content they view on the Internet.

Mr. Beaird highlighted the benefits to be gained from a dialogue between industry and government in approaching Internet content issues. He recognised the established relationship of the OECD Information, Computer and Communications Policy (ICCP) Committee and the Business and Industry Advisory Committee to the OECD (BIAC), which forms a basis for the efforts of the OECD in this and other areas that require active private sector input. He noted that both the business user community and the information technology industry were well represented at the Forum, providing a good opportunity for Member governments to interact with key players in this developing field.

PANEL 1: What Are the Pressures for Self-Regulation and Where Do They Come From?

The first panel was chaired by **Roger J. COCHETTI** of IBM, who launched the panel by describing the pressure for industry self-regulation stemming from recent publicity about children accessing illegal and harmful content on the Internet. The public attention and government interest in these issues, together with the rapid growth of the Internet, present a challenge for the private sector. The use of technological tools is the most powerful and effective way to address public concerns about illegal and harmful content, and technological developments are offering solutions. Mr. Cochetti highlighted in particular the Platform for Internet Content Selection (PICS) standard, which is currently the most important technological tool for controlling access to content on the Internet. He recognised the government concern that the PICS standard has not been widely used, and described how this situation is changing. Mr. Cochetti explained that PICS is most useful when embedded in the Internet browser software, and noted that now both Microsoft and Netscape will incorporate PICS in their browser programmes, making PICS almost universally available.

Manuel KOHNSTAMM of Time Warner Europe began by describing Time Warner's position as one of the largest Internet content providers, operating five of today's most popular Web sites (CNN, Warner Brothers, Time, Fortune and Money). He noted that Time Warner is also active in providing Internet access to schools and communities. In that context, the Time Warner experience offers a useful perspective on the Internet industry. Mr. Kohnstamm looked at the emerging need for self-regulation in this new industry, and outlined some of the benefits and limitations of regulation and self-regulation. He described the implications of the editorial powers which content providers exercise in their daily decisions about what to "print" -- whether via traditional media or via online technologies -- underlining their responsibility to provide uncensored material while at the same time recognising the need to empower

users to choose the content they view. He emphasised the importance of protecting freedom of speech, including speech on the Internet.

Mr. Kohnstamm said that Time Warner supports the view that voluntary rating systems are one option for addressing content issues on the Internet, but they should be developed in a competitive environment which offers a variety of rating mechanisms, and they should not be required as a default setting. There are many different filtering tools available and PICS is just one of those tools. It is also important to have a range of rating systems available to accommodate the needs of different countries and cultures. He noted, however, that rating systems should not be a substitute for parental responsibility to monitor children's behaviour on the Internet. He suggested that strong "brand" recognition is one way to give guidance to parents. Parents are often not as computer literate as children, therefore the industry needs to help to educate, and thus empower, parents. As information providers, the industry should provide users with sensible material. Companies like Time Warner have a particular incentive to provide "child friendly" content so as to keep customers faithful to their brand name. The media industry has experience in judging the right balance between content control and freedom of expression, and there is no reason why that should not also be applied on the Internet. *(Speaker's materials: slides.)*

Lisa BALABAN of Sympatico began her presentation by explaining how she had a quick education in the area of Internet law and self-regulation, when her company, one of Canada's major Internet service providers (ISPs), was launched last year within a period of six weeks in both French and English. She described how the inherently international nature of the Internet can make it difficult to determine which rules apply to online content and she argued that, in the current evolving environment, it is policy issues, not law, which are most important when putting together a business approach to providing content on the Internet.

In looking at the question of whether a body of "cyberlaw" exists, Ms. Balaban described the situation in Canada where there is no specific cyberlaw, but the Canadian government (Industry Canada) is monitoring developments in the industry. Liability for Internet content is among the many legal issues encountered by ISPs and other players in the online industry. If ISPs create content, then they must assume responsibility for it. On the other hand, how can an ISP assume responsibility for content it does not control? Other key legal issues in the online environment are related to intellectual property, privacy and electronic commerce. More broadly, policy issues involve establishing a secure Internet environment to foster consumer confidence; empowering users (i.e. allowing the individual user to protect himself from unwanted content), making the Internet as accessible as possible to users; and establishing co-operation between government, industry and consumer organisations.

Ms. Balaban described how Sympatico is addressing these key issues. Sympatico uses clauses in service contracts with individual users and Websites, and visitors to Sympatico sites are presented with online "Terms and Conditions". Sympatico has taken the stance that as a Canadian content provider, the laws of Canada apply to the content on its Website, users are notified of this policy by the posting of national flags on Websites (a practice borrowed from Admiralty Law). Sympatico believes that liability for content should be allocated to the party with control over the content. The company itself does not censor content, but it responds to complaints for breaches of the law and will shut down sites containing illegal material. In conclusion, Ms. Balaban emphasised the need for ISPs to work together and with the public and government, in order to educate users of the networks and to develop policies that correspond to all parties' expectations. *(Speaker's materials: slides, including Sympatico Website Terms and Conditions and Recommendations.)*

PANEL 2: What Are Key Industry Codes of Conduct and Corporate Practices and Why Do They Work?

The second panel was chaired by **Yves LE ROUX** of Digital Equipment Corporation. He pointed out that since the panellists were all subject to different regulatory environments, they could provide an account of what is happening around the world on these issues.

The first panellist, **Stefano LAMBORGHINI** of the Associazione Italiana Internet Providers (AIIP) described the development by AIIP of a code of conduct for Internet Service Providers in Italy. In drafting the code, the AIIP looked at other efforts in Europe and elsewhere. In May 1997, the code was submitted for approval to the Italian Ministry of Communications and following constructive debate on the provisions involving telecom operators and consumer groups, it was adopted by the AIIP members at the beginning of 1998. The next important step involves monitoring how the code works in practice.

The principal aim of the code is to provide an environment for the Internet which is conducive to cultural development and education, as well as commerce. Mr. Lamborghini emphasised the need to establish a positive environment on the Internet and to promote user trust. In addition to establishing general principles and obligations for ISPs, the code addresses three main points related to the self-regulation of ISP activities: liability, identification and anonymity. With respect to liability on the Internet, the code places responsibility on the one who makes content available on the Internet, whether on a commercial site or a personal site. It also calls for the ability to trace content providers and verify their identity in order to establish liability for content. However, at the same time the code identifies the importance of protecting anonymity to safeguard the diffusion of information and data and to protect the privacy of individuals, taking into account the balance between preserving anonymity and providing law enforcement officials with the means to identify subscribers who engage in illegal activities online. The code also highlights the need to safeguard human dignity and children. Mr. Lamborghini noted that while the code favours the use of filtering, blocking and rating mechanisms, some human rights advocates argue that this may amount to a form of censorship. Finally, the code covers intellectual property issues.

In terms of the management and implementation of the AIIP code of conduct, the code envisages two kinds of self-regulatory bodies: the first would deal with the initial problems of implementing the code, including reviewing it in the light of new developments; and the second would be a dispute settlement body to enforce the terms of the code by dealing with infractions and issuing sanctions. Additionally, the AIIP hopes to create an online arbitration system in conjunction with the Italian Supreme Court and the Milan Chamber of Commerce. The AIIP is also co-operating on various projects with EuroISPA and other European and American ISP associations, in order to keep a global perspective on developments and foster harmonisation of self-regulatory rules. *(Speaker's materials: speech notes.)*

Walter J. O'BRIEN of the National Advertising Review Council (NARC) focused his presentation on Internet content in the form of children's advertising. He described the role of the National Advertising Review Council in self-regulation for advertising in the United States. Advertising self-regulation has worked well in the US for 20 years based on the premise that there is a role for government as well as a role for self-governance by advertisers. The Children's Advertising Review Unit (CARU) is one of three component parts of the Council. CARU is funded by the children's advertising industry and it administers Guidelines for advertising aimed at children younger than 12 years old which ensure that this advertising is truthful, accurate and sensitive to the particular nature of its audience. CARU implements the Guidelines through the voluntary co-operation of advertisers.

Mr. O'Brien expressed concern about the new electronic interactive media and the unique questions they raise for the advertising industry, as well as the impact of the Internet on existing self-regulatory systems. This concern is compounded by the complexity of the emerging online environment for children. Mr. O'Brien described how, with a mouse and a keyboard, choices about the content viewed

by children are only "a click away", making parental mediation more difficult to exercise. The principal challenge for online advertising content is the potential blurring of the distinction between advertising and editorial content or entertainment. He argued that advertising content must be clearly labelled, for example by using child-friendly cartoon characters such as the CARU "Ad Bugs", to alert children to advertising online. Examples of Websites employing these kinds of labels are Galoob Toys and the Kelloggs site.

Another significant issue affecting the online industry is the collection of data from children online. The NARC considers that protecting children's privacy involves providing parents with notice and choice, by making parents aware of how data is collected and what is subsequently done with that information. The Guidelines call for the industry to exercise "reasonable efforts" to obtain a parent's consent before collecting information about children. It is hoped that setting goals without prescribing the means to achieve them will give the advertiser the freedom and responsibility to decide how best to educate and empower parents. Kidscom, Kelloggs, Disney, and Microsoft Kids are some of the corporations abiding by these Guidelines.

Mr. O'Brien concluded his presentation by describing an innovative new initiative in self-regulation: BBBOnline, a certification tool developed by the Council of Better Business Bureaus, which promotes ethical business practices based on six standards. To date, more than 1000 companies have signed up. The BBBOnline Seal is proof that a company is respecting certain online business practices and a user can verify the seal's authenticity by clicking on an icon. There are plans to establish a similar scheme focusing on privacy. Mr. O'Brien argued that it is the role and responsibility of the private sector to provide guidelines for advertisers; to develop tools for consumers to protect themselves; to introduce "seals of approval" to help parents protect children; and, to provide enforcement consequences to ensure effective self-regulation. He offered the view that self-regulation is the solution, and he urged industry to take action to protect children's privacy in order to avoid government regulation. (*Speaker's materials: speech notes.)*

Kazuko OTANI represented the Telecom Service Association of Japan (TELESA), a group comprising 18 per cent of Japanese Internet Service Providers, and introduced the TELESA Guidelines for Codes of Practice for Internet Service Providers. The guidelines were developed against the backdrop of an explosive increase in the number of ISPs in Japan, increases in the diffusion of harmful content and other criminal activity on the Internet, as well as an increased number of disputes about online activities, including disputes about copyright infringement, defamatory statements and liability. The Guidelines aim to protect users and to provide the industry with a framework for self-regulation.

Ms. Otani summarised the main parts of the guidelines, highlighting in particular the following basic principles:

- freedom of expression of the content provider should be respected;
- the content provider should have responsibility for the content;
- the secrecy of communications and personal data should be protected; and
- consideration should be given to the protection of minors: ISPs should use systems which enable parents or guardians to take measures to protect children.

Ms. Otani outlined those parts of the guidelines dealing with implementation and enforcement. ISPs are encouraged to include certain clauses in agreements established with users. For example, ISPs should specify in the conditions of the agreement that users are expected to behave appropriately with regard to the content they distribute via the ISP, and set out the measures that the ISP can take when they become aware of users' violations. Another chapter of the guidelines is devoted to complaints procedures and appropriate responses by the ISP to official investigations and other inquiries about users. Finally, the

guidelines promote international co-operation with other ISP organisations, in view of the global nature of the Internet. TELESA is now in the process of encouraging members and other ISPs to comply with these guidelines. *(Speaker's materials: slides.)*

Margo LANGFORD of the Canadian Association of Internet Providers (CAIP) described the creation of the CAIP code of conduct, which represents a first step toward implementing self-regulatory initiatives in this area. She outlined a number of potential liabilities faced by ISPs, including defamation, obscenity, child protection, consumer protection, content quotas, privacy, data protection and intellectual property. All ISPs and content providers should think carefully about the wide variety of issues that affect their online business; however, while large companies can put resources into addressing these issues, many of the smaller companies do not have the financial resources to deal with them and are uncertain as to how to handle them effectively. This is where ISP industry organisations, such as CAIP, can play an important role.

In considering the question of the potential liabilities faced by ISPs and Web owners, Ms. Langford highlighted the importance of determining who has "control" over the technology. There is a need for the law to address Internet actors according to their functions. ISPs have a number of means available to manage their liability risks, including blocking IP addresses, refusing to host or distribute illegal content, contractual allocation of liability, and specifying jurisdiction and venue for redress. Users, for their part, can employ content control and privacy protection technologies, encourage rating systems, and use complaint-registering processes. Unfortunately, not enough people know about the existence of the CAIP code, and the media continues to project a negative image of the Internet. Furthermore, very few complaints are actually made, and responses are not consistent.

Ms. Langford described a case study example of how the threat of legal action with economic sanctions was used to pressure an ISP to remove illegal content posted to a Website by a local user (in this case a pirated audio recording). An unresolved legal issue, which arose in this case, is whether an ISP's release of customer contact details constitutes a violation of the user's privacy. Ms. Langford also pointed out that, although this example resulted in removal of the illegal material, where small Websites around the world may be guilty of distributing illegal material, it may not always be a worthwhile exercise to pursue them.

Information and education for all actors, specifically ISPs, user groups and content creators, is key to resolving these issues and ensuring the development of effective self-regulatory mechanisms -- technology tools alone are not effective. One idea for establishing accountability for online content is establishing a Website "yellow pages" directory listing site owners and addresses. Ms. Langford argued that education must extend world-wide. User groups should be educated about infringement, creators of content need to be informed about enforcement, and ISPs should be encouraged to improve their responsiveness using procedures and tools. *(Speaker's materials: slides.)*

The last speaker on the panel, **Michel VIVANT,** spoke about the recent initiatives in the area of Internet content in France. He described the 1997 French proposal to draft an Internet Charter, an ambitious document designed to promote harmonious development of the Internet by laying down rules for its actors and establishing a self-regulatory body, or "Internet Council". When this proposal failed to gain broad acceptance, a legal committee, chaired by Professor Vivant, drafted a "Manifesto" incorporating the major principles on which Net users should agree. Professor Vivant described professional codes of conduct for ISPs which were developed by the *Groupement des Fournisseurs d'Information en Ligne* (GFII -- the online information suppliers' group) and the *Association des fournisseurs d'acces* (AFA -- association of access providers). Finally, he noted a Government Commission which is currently conducting an in-depth study of these issues to look at how Internet regulation might be adapted to the specific nature of the network environment.

Professor Vivant described how "soft law" that is more flexible, realistic, and adapted to the Internet could complement "hard law". Legal liability standards based on a determination of the "reasonable person" offer one example of where conventional laws need to be supplemented in order to be appropriately applied to the Internet, because it is not clear what "reasonable" behaviour is on the Internet. Another example where soft law could augment hard law is international conventions on jurisdiction that may not provide the same guidance in the online world as they do in the off-line world, because of the Internet's trans-frontier nature.

Professor Vivant concluded by reiterating the point already made by others, that self-regulation requires education of Internet actors, users and the authorities. To that end, in France some initial steps toward achieving a flexible approach which is adapted to the reality of the Internet would include the creation and management of a hotline to provide advice on a case-by-case basis, and the organisation of an authority to act in an advisory role and to provide a facility for mediation. *(Speaker's materials: speech notes.)*

PANEL 3: User Empowerment Technologies and Why Do They Work?

The third panel was chaired by **Claude BOULLE,** of Groupe Bull in France. He noted that a variety of user empowerment tools were available in the market, and that only a few of them would be described by the contributors to the panel.

Opening the session, **Marilyn S. CADE** of AT&T Corporation emphasised the need to promote user empowerment on the Internet and to develop globally accepted solutions. The Internet offers a variety of positive contributions to society which will also benefit children, notably as an important tool for education and entertainment, but a collaborative approach is needed to ensure its success. During the past two years, AT&T has worked to bring together all players -- including child advocacy groups, industry representatives, law enforcement authorities and government policy-makers -- to develop effective user empowerment tools that address online content issues and allow the media to develop as a safe environment for children.

Ms. Cade compared the Internet to a city under construction where there are safe places, as well as other places which are uncertain or still being developed. In such an environment, it is important that parents and teachers have tools to help make the Internet a safe place for children. AT&T is concerned about protecting children, but it is also concerned that government regulations might be unnecessary or inappropriate. For example, the US Communications Decency Act (CDA) would have forced Internet service providers to take on a law enforcement role that would have been difficult and onerous to implement. Ms. Cade expressed the view that proposals to make the implementation of filtering or blocking software compulsory would slow innovation and impede progress on the Internet. When considering what action to take regarding harmful and illegal content, she advised the use of a combination of technology tools, enforcement of existing laws, and education, especially to promote parental involvement and empowerment.

Ms. Cade highlighted four key private sector commitments agreed upon at a White House summit in late 1997. ISPs should implement a "zero tolerance" policy towards harmful and illegal content; engage in awareness and training sessions for users, including law enforcement officers; promote a "Cyber-Tipline," (funded by Congress and industry) where inquiries and complaints could be submitted; and, create a thorough inventory of existing technology tools. In her conclusion, Ms. Cade recognised there may be a need to establish rules, but urged governments to exercise flexibility and patience while work on user empowerment technologies and education continues.

Akio KOKUBU introduced the Electronic Network Consortium (ENC), a trade organisation for online service providers in Japan dedicated to solving the various problems that ISPs encounter in doing

business. Mr. Kokubu outlined the current ENC activities related to self-regulation, which include the development of ethical guidelines for running online services, setting out "online etiquette" for users, and the establishment of the first PICS-compliant label bureau in Japan.

Mr. Kokubu spoke about approaches to illegal and harmful content on the Internet under Japanese law, looking at the principle of secrecy of communications, the need to avoid censorship, the question of responsibility for inappropriate content, and the issue of human rights protection. As an illustration of the difficulties of policing the Internet, Mr. Kokubu related a recent criminal case in Japan which involved a minor whose identity and privacy were protected by the Japanese Juvenile Act. Photos of the suspect were published on the Internet and a public outcry resulted. Eventually most Japanese Web publishers deleted the photo of the boy, however overseas sites did not obey Japanese laws. Japanese police have encountered difficulties in enforcing Japanese laws against this and other kinds of illegal content held on foreign Web sites. In particular, Japan is concerned about controlling illegal pornography, in particular child pornography, on the Internet.

Mr. Kokubu elaborated on self-regulation activities in this area in Japan, describing in particular the efforts to develop and implement the ENC guidelines for service providers and users. He explained that for the ENC guidelines to be as effective as possible, they must be backed by the provision and dissemination of filtering capabilities such as PICS. To date, more than 20 000 Japanese users have downloaded PICS compliant filtering software. In addition to promoting third-party rating and self-rating, ENC has called on teachers and parents to assist in rating and the use of filtering software. There are limits to technological approaches which can be supplemented by user participation. Mr. Kokubu described the Japanese label bureau system which will promote the rating of Japanese Web pages for use with filtering technologies. He concluded by outlining future ENC work, including the "one-hundred-school networking project" to connect schools to the Internet, the development of a multiple rating systems and label bureaus, and co-operation with international standardisation work. *(Speaker's materials: slides.)*

Net Shepherd's **Don SANDFORD** described how his company is providing tools and services that empower users to self-regulate Internet use. Mr. Sandford presented ten basic principles, which are followed by Net Shepherd, that companies should consider when designing Internet filtering products and services. The user should be given total control with simple and accessible filtering products and services that enable the user to set the degree of filtering, with "no filtering" set as the default. Since choice creates an alternative to censorship, users should be given freedom of choice with a range of filtering options, including first, second and third-party ratings. Government should encourage industry to develop as many diverse filtering solutions as possible. Human intelligence should be involved in the rating process to allow for contextual information and to reflect local community standards in ways that machine indexing and key word blocking cannot. Internet users should receive positive guidance so that technologies that enable filtering can act both as a screen for unwanted content and a lens for focusing on desired content. Companies must clearly and visibly disclose information so users can make informed decisions regarding use of the services (e.g. regarding rating criteria and processes). To protect personal privacy, users must be made aware of the collection and use of their personal data. Placing the user in control, using third-party ratings and rating Internet content will all impact the potential liability of various parties. The Internet industry should understand the laws pertaining to illegal content on the Internet and should co-operate with law enforcement agencies within the context of the law. Standards are required to advance the use, economic development and adoption of Internet technology.

Mr. Sandford went on to describe how Net Shepherd has used the ten principles to create a competitive advantage. Since December 1997, over 500 000 sites have been rated using a third-party virtual community, making this the world's largest Internet opinion-based ratings database. These ratings form the foundation of the Net Shepherd World Opinion's Service and are the means through which Net

Shepherd is now, in partnership with the AltaVista Search Group, providing "Intelligent Filtered Searches" of the Internet. An initiative which has been nominated for a Computerworld Smithsonian Award. *(Speaker's materials: speech notes).*

Speaking on behalf of Net Nanny Ltd., **Gordon ROSS** discussed the different options for filtering content on the Internet. Filtering is important to protect children, but it is also imperative to preserve freedom of speech and allow individual users and organisations to control content according to their own unique set of values. He urged the Forum to consider whether there should be unrestricted access to Internet content or whether there should be monitoring of content and the persons accessing it. Mr. Ross explained how different filtering methods work, including the Platform for Internet Content Selection (PICS) standard (which both Net Nanny and Safe Surf use), self-rating systems, Website address lists, and "words and phrases" filtering.

Mr. Ross looked at the differences between filtering at the ISP level or at the PC level and outlined some of the consequences resulting from each method. Where ISPs control filtering, they become liable for illegal or unwanted content that gets through, while the user is not fully empowered and must rely on others to make decisions about content. If filtering is done at the PC level, then the user has personal control over the content filtered, and liability for content remains with the content "owner". Mr. Ross highlighted some of the advantages in the latest blocking and filtering mechanisms, including flexibility and the opportunity to carry out custom controls and audit trails. Blocking and filtering today can be done at the terminal or server level, can be run by the operating system or application, and can be applied to incoming or outgoing data.

Turning to the current concerns over the Internet, Mr. Ross emphasised what a remarkable resource the Internet is and suggested that in terms of solutions, education is key: policy makers, parents and educators must learn about the Internet through effective educational programmes that focus on positive as well as negative aspects of the Internet. There should also be properly funded and trained law enforcement personnel. He also described how access controls, identification mechanisms, and audit trails can encourage responsible Internet use. Mr. Ross was optimistic that there are a variety of technology solutions available today which can help address Internet content issues. *(Speaker's materials: slides)*

Susan J. GETGOOD described the popularity of Cyber Patrol, the Internet filtering technology tool developed by The Learning Company. Cyber Patrol is based on a foundation of choice and user empowerment. In the US Supreme Court's decision on the Communications Decency Act (CDA), Cyber Patrol was cited by the Court as a way of protecting children that did not infringe on Americans' right to free speech.

Cyber Patrol empowers parents and teachers to tailor Internet access to each individual child according to age and maturity. The software filters Internet content based on a proprietary list of sites which are constantly updated: a blacklist of more than 60 000 sites have been deemed inappropriate for a number of reasons including violence, intolerance, depiction of nudity and drugs (the "CyberNOT" list), and a whitelist of recommended children's sites (the "CyberYES" list). Cyber Patrol can also help parents control how long their child spends on line, and can protect the child from inadvertently divulging personal information to strangers online.

Ms. Getgood highlighted the unique benefit offered by Cyber Patrol that allows filtering to be tailored to meet the needs of different communities. This is helping Cyber Patrol to be used internationally, and the Learning Company is introducing localised versions of the software in a number of countries in Europe and elsewhere. The software is available in multiple languages and can be downloaded over the Internet from anywhere in the world. Cyber Patrol is now available in French and

German to European subscribers accessing the Internet over CompuServe, and is offered by a growing number of telecommunications companies providing Internet access. *(Speaker's materials: speech notes.)*

PANEL 4: Government and Private Sector Roles in Self-Regulation - What are the Conditions for Successful Self-Regulation?

Peter UPTON, of the Australian Information Industry Association (AIIA) chaired the fourth session, which comprised representatives from Internet service provider and consumer groups, as well as a law enforcement officer specialised in Internet issues.

Markku ROPPONEN spoke on behalf of the Finnish Internet Service Providers' Association (ISPA Finland), a trade association launched in December 1997 to promote co-operation among Finnish ISPs with regard to legal issues and industry self-regulation. In considering the allocation of liability among the various Internet actors, the views of ISPA Finland follow from the results of a recent project organised by the Finnish Ministry of Transport and Communications which aimed to identify and define the actors in the "information chain" between the provider and the end user, as well as their rights and responsibilities for the content published online. For purposes of regulation for public network communications, ISPA Finland proposes a distinction be made between content from "public personal communication" (e.g. news services), and "content distribution" (such as video-on-demand). Under Finnish law, liability for content is based on the actor's actual knowledge of the content. Therefore, responsibility for content varies according to the actor's role in the information chain; users in public personal communication, for example, are liable for the content of their communications, while technical carriers who have neither created the content nor decided on its delivery or publication are not liable.

Mr. Ropponen argued that the division between self-regulation and regulation for Internet content needs rethinking, and he noted some of the technical and legal issues related to industry self-regulation in this area. He expressed his view that a legal framework is necessary to support the Internet industry if it is expected to restrict the distribution of harmful and criminal materials within the network. Some actors do not have the technical ability or legal authority to block content. In order to work effectively, self-regulation must take account of the different roles of each actor, and be based on a mandate from the authorities. ISPs should work to define acceptable and unacceptable content, educate parents about the positive and negative sides of the Internet, promote international co-operation to find solutions, and support the activities of law enforcement authorities such as hotlines. *(Speaker's materials: speech notes.)*

Fred EISNER, representing the Association of Dutch Internet Service Providers, looked at the necessary conditions for successful self-regulation of Internet content, and related the Dutch experience in this area. He noted the important distinction between the information industry that deals in content, and the ISP industry which has the major responsibility to expedite and maintain an orderly flow of Internet traffic. At present in the Netherlands, ISPs are not liable for third-party content. This is due to the importance of freedom of speech and expression in a country where *ex ante* censorship is forbidden. It is also because it is technically impossible, or not proportional to the goal, for ISPs to monitor "every bit and byte" passing through networks, and such a responsibility would slow Internet growth and impede further technological development. One exception where an ISP can be held liable for content is when the ISP has knowledge of illegal content actually residing on its system. Law enforcement officers are responsible for tracking down and prosecuting law-violators, and ISPs are obliged to assist when requested to do so. Notwithstanding the legal situation, Dr. Eisner pointed out that ISPs in the Netherlands feel that they have a weighty social and moral responsibility to do all within their means to minimise the diffusion of illegal and harmful content and to protect minors and human dignity. However,

even while co-operating with law enforcement authorities ISPs must remain within the law; for instance, they cannot provide names and addresses without a Court order.

As an example of a self-regulation initiative that is operating successfully, Dr. Eisner described the hotline in the Netherlands created in response to public concern over child pornography distributed on the Internet. ISPs, concerned citizens and police officers working together decided that a neutral reporting authority should be organised to receive reports about illegal content on the Internet. The hotline was established through a public/private sector partnership, which is a structure well adapted to Dutch culture and follows similar procedures used in other sectors. The various parties involved have learned to work well together, sharing knowledge and contributing to the development of an effective and efficient hotline system. Nevertheless, there are still some areas that need to be clarified, including the financing of the hotline, prosecution of offenders (i.e. there is little experience, no trained personnel, and no clearly stated priorities), and guidance as to how cases should be handled at both the national level and international level. Dr. Eisner stressed his belief that this kind of self-regulation through a public/private sector partnership is the best solution to address content issues, but he noted that in implementing it, all parties have to make concessions. *(Speaker's materials: speech notes.)*

James R. SAVARY of the Consumers' Association of Canada described the consumer perspective on self-regulation based on the Canadian experience. He argued that the nature of the content issue makes it appropriate for self-regulation, and offered the development of the Canadian national privacy standard as an example of successful consensus-building based on a self-regulatory approach. The priority issues for Internet consumers right now relate to gaining confidence in electronic transactions, and online privacy and security concerns. Illegal or offensive content is a lower priority because there is less unanimity on the issue, with a tension between those who favour free speech and those who believe users, especially children, should be protected from harmful content. Nevertheless, the development of the Canadian national privacy standard offers a model for self-regulation that is developed by stakeholders, adopted as a national standard, and provides a basis for international co-operation.

Mr. Savary outlined several important principles that should govern self-regulation initiatives. It is essential to build consensus based on compromise with all interested parties, including the government, involved in the discussion. Mr. Savary pointed out that unlike privacy, there should be no "market failure" with content self-regulation, i.e. users usually know when they see illegal content, whereas they do not always know when their privacy rights are being violated. This kind of self-regulatory approach can significantly reduce the need for government intervention, however, it also confers responsibility on the users to adhere to the spirit as well as the letter of the standard. In order to make such a code work, it is necessary for all actors to participate. It is also necessary to make the adoption of codes mandatory and to impose sanctions for non-compliance, but it is not clear what the sanctions should be. He pointed out that the market will help monitor compliance, as content is an emotional, and therefore complaint-driven, issue. User-controlled filtering software which gives the consumer choice offers a useful complement to standards and codes of conduct. Mr. Savary concluded that self-regulatory codes following international standards together with technology tools for users are the ideal solution, ensuring maximum flexibility for industry and protection and empowerment for consumers. *(Speaker's materials: slides.)*

Christophe SAPET spoke on behalf of the French *Association des fournisseurs d'accès à des services en ligne et à Internet* (AFA) (Association of access providers to online services and Internet). Mr. Sapat began by pointing out that the roles of government and the private sector have not changed just because of the Internet; the Internet is merely a new space which the public and private sectors must learn to manage together. The Internet represents an innovative means of communication that is global and interactive, and allows anyone to distribute content, thereby raising new challenges for addressing content issues. He argued that a number of misconceptions have arisen around the meaning of "self-regulation" as applied to the Internet. For the AFA, self-regulation does not imply that the competence of the regulatory

and judicial authorities is compromised, but rather it establishes the role of the private sector to manage the space in which it carries out its activities. The AFA will participate as a part of the process by playing a consultative and informative role to assist the government in establishing norms that will be applied by the private sector.

Mr. Sapet highlighted three unique aspects of the Internet which raise issues for regulation and policy-making: the distribution of data is instantaneous, the Internet is constantly developing, and the Internet is global. The AFA advocates the creation of hotlines to address the distribution of harmful content with quick and flexible response mechanisms. Representative consultative bodies specialised in the Internet could assist in the law-making process by advising legislators on the fast-paced changes and future trends in Internet technologies. Finally, co-ordination at the international level will facilitate the resolution of difficult issues implicit in the nature of the Internet network. In conclusion, Mr. Sapet stated that the AFA intends to continue to play a significant role in addressing these issues by bringing together Internet actors and co-ordinating with the government, and working to implement the hotline and advisory initiatives. *(Speaker's materials: speech notes.)*

The final contributor to the panel, **Guy VERBEEREN** of the Belgian *Police Judiciaire* (Criminal Investigation Department), spoke about the efforts in Belgium to combat child pornography on the Internet. Tragic events in Belgium in 1996 led to the creation of the Child Pornography Internet Contact Point, an official "child pornography" contact service which is administered by the Belgian National Computer Crime Unit (NCCU). The NCCU also carries out searches on the Internet for child pornography and, at the request of other criminal investigation units, supplies technical assistance for identifying and tracing those responsible. The contact site allows members of the public to report information about child pornography to the police.

Under Belgian law, distribution of pornography via any medium is a punishable offence. The law was extended to specifically cover the distribution or possession of child pornography, and it was written without imposing conditions as to the type of media or technology used so that it would apply to computer networks, hard disks, or any other electronic or optical format -- in particular the Internet and digital technologies. In practical terms, distribution of child pornography via any Internet application, including e-mail, news groups, Internet Relay Chat (IRC) or the World Wide Web, can be punished in Belgium under current legislation.

Through the central email address of the Criminal Investigation Department, it is possible for the public to contact, in their own language, the National Computer Crime Unit to report child pornography for investigation. In 1997, approximately 2000 messages or notices were received, but only five led to investigations or arrests, either abroad or in Belgium. So far, in 1998, two investigations have begun. If a message is received containing relevant and valuable information concerning illegal content in a foreign country, the message is sent to the competent authority in that country. Occasionally, the service also receives messages about other offences, such as "spamming" or pyramid games, in which case the matter is also forwarded to the competent authority. Mr. Verbeeren noted that in undertaking this effort, the Belgian police have experienced good co-operation with the ISPs involved.

Mr. Verbeeren closed the session by summarising his views on how to help resolve these problems in a satisfactory manner. The authorities must provide Internet actors with a clear legal framework and service providers must collaborate to create a safe medium. The protection of children is a responsibility that should be shared by law enforcement officials, ISPs and those responsible for children on a much more personal level, such as teachers and parents. For example, parents must take steps to use filtering technologies and passwords to protect children from illegal and harmful content on the Internet. Taking this into consideration, it is also important that children's access to the valuable educational resources offered by the Internet is not completely restricted. *(Speaker's materials: speech notes.)*

PANEL 5: General Discussion

In her introduction of the final session, **Maria LIVANOS CATTAUI** of the International Chamber of Commerce (ICC), noted the timeliness of the Forum in light of developments in network technology and electronic commerce. She noted the OECD conference "Dismantling the Barriers to Global Electronic Commerce," held in November 1997 in Turku, Finland, and the forthcoming Ministerial meeting on Electronic Commerce "A Borderless World: Realising the Potential of Global Electronic Commerce," to be held in Ottawa, Canada on 7-9 October 1998. She highlighted the importance of education to promote the use of network technologies and to increase the awareness about the benefits offered by the Internet.

Michael BAKER spoke on behalf of Electronic Frontiers Australia (EFA), which is a member of the Global Internet Liberty Campaign (GILC). He began by reminding the Forum that the Internet is an amazing new communications tool: it is not just an industry, it is not just about developing electronic commerce, and not all of the content available on the Internet is commercial. Content regulation at this point in time refers to the regulation of non-commercial content, therefore policy-makers must use caution to avoid infringing upon the rights of individuals. There is a concern that the kind of "self-regulation" currently being promoted would force ISPs into an enforcement role to control their users. He highlighted the importance of involving all end-users in the process of developing self-regulatory mechanisms. He voiced his concern that discussions about Internet content issues should consider both freedom of speech and the welfare of children on the Internet. Dr. Baker warned against creating false expectations about filtering and blocking technologies as some of these tools may not fulfil all the promises being made. He questioned the existing incentives for content providers to self-rate, and suggested that promoting self-rating mechanisms as a way of solving problems could provide a false sense of security that the content problem is in hand. He argued for parental empowerment and education as an alternative solution.

Dr. Baker described some of the recent thinking in this area in Australia. For example, in light of the inherently international nature of the Internet, it might be useful to review the criteria for determining what is considered "legal" and "illegal" Internet content. It has been proposed that the only content which should be banned is that which is banned in all countries, and the term "Internet illegal" has been proposed to indicate something that should be considered illegal all over the world. Child pornography is currently the only item in that category. As for other content, Dr. Baker expressed the view that it would be useless to establish controls because the restricted content would only become available somewhere else. Dr. Baker urged that the dialogue on these issues should continue at the international level, and he suggested that specific discussions should be organised in the year ahead involving more ISPs, activists and users.

David KERR of the Internet Watch Foundation (IWF) described how the IWF was founded 18 months ago when United Kingdom law enforcement officials sought to prosecute ISPs for distributing harmful and illegal content. After considerable discussion, a compromise was reached to introduce self-regulation for Internet content issues, and a co-operative relationship was launched between UK law enforcement authorities, the UK ISP industry, and user representatives. The IWF represents a form of self-regulation whereby industry abides by a set of standards which have been developed through consultation among all actors, including ISPs and police authorities. In response to some of the earlier observations regarding self-rating mechanisms, Mr. Kerr expressed his opinion that the incentive to self-rate a Website exists if there is a desire to have the Website approved by parents and thus accessed by children. He noted the conclusions of the IWF Advisory Board on content rating systems which are available from the IWF Web site (http://www.iwf.org/uk).

The IWF supports the development of partnerships at the international level, and it plans to extend it's activities to the European level. In its initiatives, the European Union has also adopted a

consultative approach involving both the public and private sectors. Self-regulatory initiatives, such as hotlines, will be funded jointly by the European Union and industry. Mr. Kerr recognised the important role of the OECD as a forum for addressing content issues at the international level, and he urged that focused discussions of this type should be encouraged in the future. *(Speaker's materials: speech notes).*

David W. PHILLIPS of AOL Bertelsmann Online, Europe, began by outlining what he sees as the key attributes of the Internet and the important ways that it differs from traditional media: the global network is interactive, interdependent, and open. The interactive nature is seen in the fact that Internet content is generally selected by users, it is "pulled" not "pushed", and a wide range of content can be provided by anyone at a variety of levels. This allows an opportunity for both user empowerment technologies and third party "information brokers" to play an important role in managing content on the Internet. The essence of the World Wide Web is the links between different sites offering data that can be physically located anywhere; this global nature makes the network interdependent, limiting governments' ability to regulate. Finally, the ubiquity and openness of the Internet set it apart from more traditional telephone and broadcast media, so that the existing regulatory regimes of telecommunications and broadcast industries cannot be applied to the Internet.

Bearing in mind these attributes of the Internet, different regulatory models should be considered. Among the current options are the market model, self-regulation and government regulation. Mr. Phillips argued that the market model, based on the premise that consumer confidence is needed to maintain the customer relationship, does not always work. With the free flow of information, consumers have more choice in a competitive environment and thus greater bargaining power. Looking to the government regulation model, at this early stage in the development of the Internet it would be premature to impose rigid government regulations, as they might hamper technological development. Another disadvantage of this model is the inadequacy of government resources to address enforcement or compliance issues. Furthermore, there is the potential for national laws to overlap and conflict with one another. Mr. Phillips maintained that the government regulation model should only be used when the market has broken down and when there is no meaningful self-regulation. He pointed out that self-regulation is not just about codes of conduct, and it has three important aspects: legislative, adjudicative and regulatory. An important advantage of self-regulation is that it employs industry expertise and takes into account the rapid developments in the field.

Mr. Phillips concluded that the best approach to addressing Internet content issues would be a mixture of all three models. He urged policy-makers to promote competition and transparency in developing their approaches. They should look at where the market has broken down and where self-regulation might be inadequate. Laws should be narrowly focused and specifically tailored to address the issue they are aimed at, and they should not, if possible, raise more problems than they solve. He illustrated this point by offering the US Communications Decency Act and the German Multimedia Law as two examples of government regulatory initiatives which failed because they were too broad and gave no meaningful guidance regarding the application of the law.

Closing Remarks by Co-Chairs

The Chairs thanked the organisers of the meeting, and concluded that the OECD and BIAC had succeeded in providing a useful forum where the main industry actors could meet with government representatives to exchange opinions and experiences of self-regulation in the field of illegal and harmful content on the Internet. They noted with interest that many common viewpoints had been expressed in the presentations and discussions. They were encouraged to see that a partnership between governments and the private sector is emerging, with the private sector taking the lead.

RESOURCES: RELEVANT WWW SITES AND DOCUMENTS

The Steering Group which organised the Forum recognised that the work being done at the OECD on approaches to content on the Internet is only one effort among a large variety of initiatives on these issues currently underway all over the world in both the public and private sectors. The following list was compiled to provide information about relevant Websites and documents offering further resources on related issues for participants at the Forum and other interested parties.

The Steering Group also highlighted the importance of putting the issues under discussion at the Forum into a positive context by recognising the enormous economic and social benefits offered by the developing Internet. To that end, the list below also includes references to sites and documents which illustrate current facts and statistics regarding Internet growth and development. The list is not intended to be exhaustive, but it provides a starting point for gathering further information in this area.

Note: *While every effort has been made to ensure that the references and URLs provided in this list are correct at the time of publication, URLs may be subject to change from time to time.*

WORLD WIDE WEB SITES

Technological-based solutions

Blocking / Filtering Software Sites

- CYBERsitter (Solid Oak Software)
  http://www.solidoak.com
- Filtering Software download site (Japanese)
  http://www.nmda.or.jp/enc/rating/index.html
- NetNanny
  http://www.netnanny.com
- Recreational Software Advisory Council
  http://www.rsac.org/homepage.asp
- Surfwatch
  http://www.surfwatch.com
- Net Shepherd
  http://www.netshepherd.com

Information on Internet Access Control Standards, Rating Systems, and Commercial Tools

- Information Technology Association America (ITAA)
  http://www.itaa.org
- 'Technology Inventory' by Lorrie Faith Cranor and Paul Resnick
  http://www.research.att.com/~lorrie/pubs/tech4kids/
- Peacefire
  http://www.peacefire.org/

Codes of Conduct and Private Sector Policies

Codes of Conduct

- Codes of Practice and Guidelines for UK Academic WWW Sites
  http://cspmserver.gold.ac.uk/guidance.html
- Canadian Association of Internet Providers' "Code of Conduct"
  http://www.screen.com/mnet/eng/indus/internet/Caipcode.htm
- EuroISPA Aims and Objectives
  http://www.euroispa.org/aims.html
- Georgetown University
  http://www.georgetown.edu/student-affairs/stconduc/compuse1.htm
- General Ethical Guidelines for Running Online Services (Electronic Network Consortium, ENC, Japan)
  http://www.enc.or.jp/enc/guideline.html
- Guideline for Codes of Practice for Internet Service Providers (Telecom Services Association, TELESA, Japan) *http://www.telesa.or.jp/e_guide/e_guide01.html*
- Internet Conduct: Basic Reference Manual
  http://info.isoc.org/policy/conduct/conduct.html
- ISPA (Internet Service Provider Association) UK Code of Practice
  http://www.ispa.org.uk
- South Australian Internet Association's Code of Conduct V2.1- General Ethics and Conduct rules agreed to by the South Australian Internet Association ("SAIA")
  http://www.saia.asn.au/Documents/coc_v2-1.html

Netiquette

- Florida Atlantic University Guide, "The Net: User Guidelines and Netiquette," by Arlene Rinaldi
  http://www.fau.edu/rinaldi/net/index.htm
- Recommended Etiquette for Online Service Users (Electronic Network Consortium, (ENC) Japan)
  http://www.enc.or.jp/enc/etiquette.html

Educational resources

- American Association of School Administrators
  http://www.aasa.org/
- Barry and Ruth Cranmer's Child Safety on the Internet
  http://www.voicenet.com/~cranmer/censorship.html
- Center for Children and Technology
  http://www.edc.org/CCT/ccthome/
- Center for Media Education
  http://www.cme.org/cme/
- Center for Democracy and Technology
  http://www.cdt.org/
- Childnet International's Launchsite
  http://www.launchsite.org/
- Child Safety on the Information Superhighway, Produced by the Interactive Services Association and the National Center for Missing and Exploited Children (1994)
  http://ericps.ed.uiuc.edu/npin/respar/texts/preteen/safety.html
- Cyber-Savvy Parents Guide, by the Direct Marketing Association
  http://www.cybersavvy.org/
- Disney's Family.com
  http://www.family.disney.com/
- Electronic Frontier Foundation
  http://www.eff.org/
- Interesting Places to Browse on the Web for Parents and for Kids
  http://www.starport.com/places/
- InternetAdvocate
  http://www.monroe.lib.in.us/~lchampel/netadv.html
- Internet On-line Summit focus on Children (December 1-3 1997, Washington, US)
  http://www.kidsonline.org/
- Interactive Services Association's Project OPEN (Online Public Education Network)
  http://www.isa.net/project-open/
- Media Awareness Network "User empowerment and education and awareness building"
  http://www.screen.com/mnet/
- National Centre for Educational Technology
  http://www.ncet.org.uk/index.html
- National School Boards Association's Institute for the Transfer of Technology to Education
  http://www.nsba.org/itte/
- National Urban League
  http://www.nul.org/

- NCH Action for Children
  http://www.nchafc.org.uk/
- 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/PICS
- SafeKids, produced by syndicated columnist Larry Magid
  http://www.safekids.com/
- SafeSurf, Making the Net Safe
  http://www.safesurf.com/index.html
- The Family Education Network, sponsored by AT&T, Microsoft, and Nellie Mae
  http://familyeducation.com/
- The Guardian Angels' CyberAngels Internet Safety Organization
  http://www.cyberangels.org/
- "The Parents Guide to the Information Superhighway", America's Children and the Information Superhighway The Childrens Partnership, 1996
  http://www.childrenspartnership.org

Children's Issues (including hotlines)

- Childnet International, a UK-based charity devoted to promoting the interests of children in international communications (includes links to European initiatives under the auspices of the "inhope forum" (Internet Hotline Providers in Europe)
  http://www.childnet-int.org/index.html
- Internet Watch Foundation
  http://*www.iwf.org.uk/*
- Movement Against Paedophilia on the Internet
  http://www.info.fundp.ac.be/~mapi/mapi-eng.html
- Redd Barna (Save the Children Norway)
  http://www.childhouse.uio.no/redd_barna/
- Regulation of Child Pornography on the Internet
  http://www.leeds.ac.uk/law/pgs/yaman/child.htm
- US Government Report Child Pornography
  http://www.customs.ustreas.gov/enforce/childprn.htm
- US Cyber-tipline
  http://www.missingkids.com/cybertip
- Child Pornography Hotline in the Netherlands
  http://www.meldpunt.org/meldpunt-eng.htm

Anti-Censorship

- Citizens Internet Empowerment Coalition
  http://www.ciec.org/
- Families Against Internet Censorship
  http://shell.rmi.net/~fagin/faic/
- Peacefire
  http://www.peacefire.org/
- XENU Censorship Web-page
  http://www.xemu.demon.co.uk/censor/index.html

Civil Liberties

- American Civil Liberties Union
  http://www.aclu.org/
- Center for Democracy and Technology
  http://www.cdt.org/
- Computer Professionals for Social Responsibility
  http://www.cpsr.org/home.html
- Cyber-Rights and Cyber Liberties (UK)
  http://www.leeds.ac.uk./law/pgs/yaman/yaman.htm
- Electronic Frontier Foundation
  http://www.eff.org/
- Paul F Burton Web-page (links and resources)
  http://www.dis.strath.ac.uk/control/

OECD Member Government Initiatives

Australia

- Australian Federal (Commonwealth) Government online services initiatives: Innovate Australia
  http://www.dca.gov.au/policy/natstrat.htm
- Investigation into the content of on-line services, Australian Broadcasting Authority, June 1996
  http://www.dca.gov.au/aba/invest.htm

Canada

- Cyberspace is not a “No Law Land”, Information Highway Advisory Council Report, March 1997
  http://www.ic.gc.ca/nme

- Internet Service Providers in Canada: An Economic Analysis by Industry Canada and Statistics Canada (ISP industry survey results that include Canadian ISP's practices in dealing with offensive content)
  http://www.strategis.ic.gc.ca/networks

Germany

- The German Federal Government's Information and Communication Services Bill ("IuKDG" or "Multimedia Law"), 1 August 1997
  http://www.iid.de or *http://www.bmbf.de*

Japan

- Guidelines for ISPs' codes of practice for Internet Service Providers, Telecom Service Association, Japan, 16 Feb 1998
  http://www.telesa.or.jp/e_guide/e_guid01.html
- The Rules for the Flow of Information on the Internet, Study Group of Ministry of Posts and Telecommunications, 25 Dec 1997 (Outline)
  http://www.mpt.go.jp/policyreports/english/group/telecommunications/rules_outline_e.html
- Electronic Network Consortium Guidelines, Ministry of International Trade and Industry (MITI)
  http://www.nmda.or.jp/enc/guidelines.htm

New Zealand

- Internet Service Providers Code of Practice
  http://www.isocnz.org.nz/isocnz/theispco.html

Switzerland

- Swiss study on penal, data protection and copyright aspects of the Internet, Interdepartmental working party of the Federal Office of Justice, May 1996
  http://www.admin.ch/bakom/

United Kingdom

- Internet Watch Foundation
  http://www.iwf.org.uk/

United States

- Clinton Administration Framework for Global Electronic Commerce, 1 July 1997
  http://www.iitf.nist.gov/eleccomm/ecomm.htm

- National Information Task Force (NIST) Options for Promoting Privacy on the National Information Infrastructure, Draft, April 1997
  http://www.iitf.nist.gov/ipc/privacy.htm

Standards Development

- The World Wide Web Consortium (W3C)
  http://www.w3c.org
- Platform for Internet Content Selection (PICS)
  http://www.w3.org/PICS/Activity
- Operation of the first PICS compliant label service bureau in Japan
  http://www.nmda.or.jp/enc/ratingop-english.html

European Union

- Action Plan on promoting safe use of the Internet
  http://www2.echo.lu/legal/en/internet/actplan.html
- Communication on Illegal and Harmful Content on the Internet, October 1996
  http://www.echo.lu/legal/en/internet/communic.html
- Global Information Networks Declarations
  http://www2.echo.lu/bonn/conference.html
- Commissioner Bangemann on the Policy of Response to Globalisation, 9 Sept 1997
  http://www.ispo.cec.be/infosoc/promo/
- Legal Advisory Board Regulation of Internet Content
  http://www.echo.lu/legal/en/internet/content.content.html
- Report by Mr. Pierre Pradier
  http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.htm
- The Council Resolution on illegal and harmful content on the Internet
  http://www.echo.lu/legal/en/internet/resol.html
- The Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services, 16 October 1996
  http://europa.eu.int/en/record/green/gp9610/protec.htm
- Working Party on Illegal and Harmful Content on the Internet interim report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet, July 1997
  http://www.echo.lu/legal/en/internet/wp2en-toc.html

Other International Initiatives

- Global Information Networks: Realising the Potential, International Ministerial Conference, Bonn, 6-8 July 1997
  http://www2.echo.lu/bonn/conference.html

- European Council in Amsterdam - Action Plan to combat organised crime
  http://ue.eu.int/amsterdam/en/conclusions/freedom/main.htm

Internet Growth and Development: Facts and Statistics

Growth of Internet Hosts

- Matthew Gray, Massachusetts Institute of Technology, Web Page on Internet Growth
  http://www.mit.edu/people/mkgray/net/
- Network Wizards "Internet Domain Survey January 1998"
  http://www.nw.com/zone/WWW/report.html
- Network Wizards Survey methods
  http://www.nw.com/zone/WWW/new-survey.html
- CANARIE Inc.
  http://www.canarie.ca
- Matrix Information and Directory Services, Inc. (MIDS)
  http://www.mids.org
- Next Generation Internet: Trends
  http://www.ngi.org/trends.htm

Growth of number of Internet Users

- ICONOCAST by Michael Tchong
  http://www.iconocast.com/
- CommerceNet and Nielsen Media Research
  http://www.commerce.net
- The Economist - the special Electronic Commerce Survey (May 10, 1997)
  http://www.economist.com/

Internet Usage Statistics

- The 7th Georgia Tech Graphic, Visualization, & Usability Center's (GVU) WWW User Survey conducted April 10 through May 10 1997
  http://www.gvu.gatech.edu/user_surveys/survey-1997-04/
- Keynote Business 40 Internet Performance Index
  http://www.keynote.com/measure/business/business40.html
- New Media Watch (Media Metrix)
  http://www.pcmeter.com/
- Internet Statistics and Demographics: A Library of Congress Internet Resource Page
  http://lcWeb.loc.gov/global/internet/inet-stats.html

- eMarketer
  http://www.e-land.com/e-stat_pages.htm

Statistics relevant to Internet Usage in some OECD areas

- NUA Internet Surveys
  http://www.nua.ie/surveys/
- ACNIELSEN: The Canadian Website
  http://acnielsen.ca/

Research Firms

- Jupiter
  http://www.jupiter.com/
- Forrester
  http://www.forrester.com/
- Hambrecht & Quist
  http://www.hambrecht.com/
- Cyberatlas
  http://www.cyberatlas.com/

OECD

- Reference paper "Measuring Electronic Commerce"
  http://www.oecd.org/dsti/sti/it/ec/prod/e_97-185.htm

European Commission

- Evolution of Internet and WWW In Europe, Trans-European Telecommunications Networks Study, DG XIII, October 1997
  http://www2.echo.lu/tentelecom/en/evol-summary.htm

RELEVANT DOCUMENTS

OECD Member Country Initiatives

Canada

- Building the Information Society: Moving Canada into the 21st Century, Government of Canada, May 1996.
- Connection, Community Content: The Challenge of the Information Highway, Final Report of the Information Highway Advisory Council, September 1995.

- Illegal and Offensive Content on the Information Highway, a background paper prepared by Gareth Sansom, DPP, spectrum, Information Technologies and Telecommunications Sector, SITT, Industry Canada, June 1995.
- Preparing Canada for a Digital World, Information Highway Advisory Council, Phase II Conclusions and Recommendations, Information Highway Advisory Council, April 1997.
- The Cyberspace is not a "No Law Land", a study of the issues of liability for content circulating on the Internet prepared for Industry Canada by Michael Racicot, Mark S. Hayes, Alec R. Szibbo and Pierre Trudel, February 1997.
- Undue Exploitation of Violence, a consultation paper released by the Department of Justice, March 1996.
- The Canadian Association of Internet Providers (CAIP) "Code of Conduct".
- Summary of the CSA Standard "Model Code for the Protection of Personal Information".
- Inventory of Voluntary Codes Currently in Operation by Government of Canada, Industry Canada's Office of Consumer Affairs, 1997 (hard copy only).
- Voluntary Codes: A guide for their development and use by Government of Canada, Industry Canada's Office of Consumer Affairs, 1997 (hard copy only).

United States

- A Framework for Global Electronic Commerce, Clinton Administration, July 1997.
- Cryptography's Role in Securing the Information Society, Kenneth Dam and Herbert Lin, 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: Issues Affecting Development, General Accounting Office (GAO/RCED-94-285) September 1994.
- Information Superhighway: An Overview of Technology Challenges, General Accounting Office (GAO/AIMD-95-23) January 1995.
- Intellectual Property and the NII. Information Infrastructure Task Force, Bruce A. Lehman, September 1995.
- Online Law, Thomas J. Smedlinghoff, Software Publishers Association, 1996.
- Options for Promoting Privacy on the National Information Infrastructure, Draft for Public Comment, Information Policy Committee, National Information Task Force, April 1997. *http://www.iitf.nist.gov/ipc/privacy.htm*
- The NTIA Infrastructure Report: Telecommunications in the Age of Information, NTIA, DOC, October 1991.

Books

- Child Safety on the Internet, Gregory Giagnocavo (Editor), 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, Lindac. Joseph. 1995.

SPEAKERS' BIOGRAPHIES

Co-Chairmen

Mr. Richard C. BEAIRD

Mr. BEAIRD is Senior Deputy US Co-ordinator and Deputy Director of the International Communications and Information Policy, United States Department of State. He has extensive experience in international telecommunication policy matters involving multilateral and bilateral fora. In his current position, he manages State Department activities across a broad range of international telecommunications and information policy issues, including those arising in the International Telecommunication Union (ITU), the OECD and APEC. He is the Chairman of the Working Group on Telecommunications within the APEC process. He is also Chairman of the OECD Committee for Information, Computer and Communications Policy.

Dr. Etienne GOROG

Dr. GOROG as well as serving as Chairman of the BIAC Committee on Information, Computer and Communications Policies, is Vice President of IBM Consulting Group and General Manager, IT Solutions Consulting, IBM Middle East and Africa (*http://www.ibm.com).* He has been a pioneer in telecommunications technology and networking. He perfected the theory of communications error protection coding and designed the first digital modem. He also defined the concept of "networking" which became the basis for IBM's highly successful Systems Network Architecture (allowing any terminal to access any application in any computer). Currently, his responsibilities include managing IBM's participation in the European Community's programme for Research in Advanced Communications Technologies in Europe, aiming at the implementation of Integrated Broadband Communications (IBC) across Europe.

Moderators and Panellists

Dr. Michael BAKER

Dr. BAKER is a Board Member of Electronic Frontiers Australia (EFA) (*http://www.efa.org.au)* which he founded four years ago. He has served as Chairman of the Board and now is EFA's international liaison. Dr. Baker has also been an active contributor to the activities of the Global Internet Liberty Campaign (GILC) (*www.gilc.org).* He edited the GILC member statements on Human Rights and the Internet for a briefing of Members of the European Parliament and prepared the GILC response to W3C's request for comments on PICS rules. Dr. Baker is a Senior Software Engineer working for Adacel Technologies Limited (*www.adacel.com.au),* an Australian software house, and is also a member of the ISOC.

Ms. Lisa BALABAN

Ms. BALABAN as Senior Vice President for Business Affairs and General Counsel at Sympatico/Medialinx Interactive, L.P. (*http://www.sympatico.ca* and *http://www.medialinx.ca),* is responsible for negotiating and structuring MediaLinx partnerships and business arrangements for the

acquisition and development of multimedia content, applications and services. She works with each of the twelve Sympatico Service Providers in Canada addressing policy and legal issues such as security, privacy, copyright, and other intellectual property rights. Ms. Balaban is also a member of the Barreau du Québec, the Canadian Bar Association, and sits as a director on the Board of Invention Media, a new media company.

Mr. Claude BOULLE

Mr. BOULLE is Director of European Affairs in the Corporate Strategic Technologies and Partnerships Department of Groupe Bull, (*http://www.bull.com)*, and has spent more than 20 years in information technology research and development. His experience covers a wide spectrum of technologies and applications with a strong focus on communication and distributed systems. He was responsible for the definition and the design of Groupe Bull DCM -- Distributed Computing Model -- a coherent framework to implement the smooth integration of mainframes, open systems and PCs or workstations. He is a member of the HLSG -- High level Strategy Group for ICT -- which brings together at European Union level representatives from the different industry sectors involved in the implementation of the Information Society, with a view to defining the main orientations of standardisation activities. Mr. Boulle is leading the HLSG Electronic Commerce Project.

Ms. Marilyn S. CADE

Ms. CADE is Director of Technology and Infrastructure Advocacy for AT&T Corporation, in the United States (*http://www.att.com*). She is responsible for issues relating to the Internet, online services and electronic commerce for AT&T. Ms. Cade's career has included lobbying, sales, business management and organisational development positions within state government, non-profit organisations, and the private sector. Since joining AT&T, she has held a variety of positions in sales, marketing, and business management. Ms. Cade is active in a variety of professional organisations and consortiums which deal with the Internet and related public policy issues, including: high performance computing and communications and the research agenda; Internet and online privacy; intellectual property protection for copyright and trademarks.

Ms. Maria LIVANOS CATTAUI

Ms. CATTAUI assumed the office of Secretary General of the International Chamber of Commerce (ICC) (*http://www.iccwbo.org)* in July 1996. Her immediate task was to raise the public profile of the ICC as the world's business organisation and make it a more vigorous advocate of business in dealings with international organisations and governments. Prior to assuming her duties at the ICC, Ms. Cattaui was with the World Economic Forum in Geneva. During her tenure at the World Economic Forum, she was instrumental in increasing membership from 80 companies to more than 1 000 major world firms in over 60 countries. Her role was crucial in the development of the foundation as a unique partnership of leaders. She was particularly responsible for the well-known annual meeting in Davos.

Mr. Roger J. COCHETTI

Mr. COCHETTI as Program Director for Policy & Business Planning at the IBM Internet Division (*http://www.ibm.com*), is responsible for the co-ordination of IBM's efforts to ensure that government policies and regulations world-wide are supportive of electronic business and the Internet. Named by Wired Magazine in 1998 as one of "Washington's Most Wired" people, Mr. Cochetti serves on the boards of a variety of Internet related organisations, including the Internet Law & Policy Forum; the Recreational Software Advisory Council-Internet; the US Internet Council; TRUSTe; the Internet State Coalition; the Internet Education Foundation (which sponsors programs of the Congressional Internet Caucus). He is a consultant on Internet matters to the United Nations World Intellectual Property Organisation (WIPO).

Dr. A. EISNER

Dr. EISNER is Chairman and Chief Executive Officer of the Association of Dutch Internet Service Providers (NLIP) (*http://www.nlip.nl*), and member of the board of the Dutch Hotline against Child Pornography. He handles all issues affecting national and international public affairs for Dutch Internet Service Providers and regularly advises the Dutch government on key issues which affect the nature of the ISP business. NLIP covers approximately 85 per cent of the business-market and 65 per cent of the consumer market. Mr. Eisner has held several management and advisory positions in public service, education, health-care, and most recently in the ICT Industry.

Ms. Susan J. GETGOOD

Ms. GETGOOD is Director, Corporate Communications, The Learning Company, Inc. (United States) (*http://www.learningco.com),* a leading publisher of consumer and educational software. Previously, she was Director of Marketing at Microsystems Software, the Internet software company that developed the Cyber Patrol Internet filtering software and which was acquired by The Learning Company in 1997. She has been involved in Internet children's issues for over three years, starting with the successful challenge to the Communications Decency Act of 1996. She has testified before the FTC on Internet safety and privacy, and in December 1997, joined a panel at the White House Summit on Children's Safety that discussed Internet filtering issues. Most recently, she has been working on issues surrounding positive digital content for children and the development of quality educational content for home and school.

Mr. David KERR

Mr. KERR is Chief Executive of the Internet Watch Foundation (United Kingdom) (*http://www.iwf.org.uk).* He developed the organisation from the original agreement between the UK Internet industry, government and police. One of his main responsibilities at the IWF is to implement agreements established in 1996 between the DTI, the Home Office, police authorities and Internet service provider associations. He has extensive experience of policy review and management consultancy in local government where he worked to develop partnerships between public and private sector organisations to address issues such as race relations and rural services.

Mr. Akio KOKUBU

Mr. KOKUBU as Senior Executive Director for the Electronic Network Consortium (ENC) of Japan (http://www.enc.or.jp), is responsible for issues such as intellectual property rights, content self-regulation and privacy protection in services on the Internet. For over 20 years, Mr. Kokubu has worked on the architecture of computer systems at the Electrotechnical Laboratory of the Agency of Industrial Science and Technology. In 1990, he left the Laboratory and became Director of the New Media Development Association where he has worked on the development of online multimedia services and the use of smart cards in public and private regional systems.

Mr. Manuel KOHNSTAMM

Mr. KOHNSTAMM is Vice-President of Public Affairs at Time Warner Europe (http://www.pathfinder.com/corp/). He is responsible for legal and regulatory policy issues for Time Warner operating divisions in Europe, as well as shaping Time Warner corporate policy regarding European regulation in a range of new media and communication technologies. These activities serve the European operations of Time Warner Publishing, Time Warner Cable, Home Box Office, Turner Broadcasting and Warner Brothers. Mr. Kohnstamm previously worked for the EU Commission in Brussels in DG XIII and for the consultancy firm European Research Associates.

Mr. Stefano LAMBORGHINI

Mr. LAMBORGHINI as Secretary-General of the Associazione Italiana Internet Providers (AIIP), (http://www.aiip.it) is responsible for a number of ISP-related issues including illegal and harmful content, domain names, copyright, electronic commerce, and network development. He also has extensive knowledge and experience in dealing with issues in the area of multimedia and electronic publishing such as copyright, anti-piracy, privacy, on-line publishing and fair competition. Mr. Lamborghini is a Member of the Board of the European Internet Services Providers Association (EuroISPA) and active in a number of committees and workshops throughout Europe including some organised by the European Commission.

Ms. Margo LANGFORD

Ms. LANGFORD as Chair of the Canadian Association of Internet Providers (CAIP) (http://www.caip.ca), has worked in an advocacy role to protect the interests of both content creators and Internet providers. She brings a "convergence" background garnered from working in the broadcasting industry and as a telecommunications and entertainment lawyer. Having worked for a Canadian Federal Cabinet Minister and more notably as senior legal advisor to the UK-based International Federation of the Phonographic Industry (IFPI), she has extensive knowledge and insight into both international and domestic regulation, law and treaty making processes, as well as how NGOs and multi-lateral institutions contribute to these activities.

Mr. Yves LE ROUX

Mr. LE ROUX is responsible for Techno-Policy Issues at the Corporate Security Program office of Digital Equipment Corporation (http://www.digital.com) and chairs the Security Working Group of the European Association of Manufacturers of Business Machines and Information Technology Industry (EUROBIT). He is actively involved with the Business and Industry Advisory Committee (BIAC) to the OECD and has participated in the drafting of the OECD Cryptography Policy Guidelines. He also participates in the OPEN GROUP Security Program Group, studying proposed technical solutions for enforcing security in the open networked environment, including "video-on-demand" and the WWW. Mr. Le Roux is also the chairman of the P3P Transport and Protocol Working Group of the W3C.

Mr. Walter J. O'BRIEN

Mr. O'BRIEN is President of the National Advertising Review Council, Inc. (http://www.bbb.org/advertising/index.html) and Vice President of the Council of Better Business Bureaus, Inc. He oversees the day-to-day application of policies developed by the National Advertising Division (NAD), Children's Advertising Review Unit (CARU) and the National Advertising Review Board (NARB). Through these organisations, Mr. O'Brien works to create a "level playing field" for advertisers, minimise government intrusion into the creation process, and encourage trust in advertising among consumers.

Ms. Kazuko OTANI

Ms. OTANI is General Manager of the Legal Affairs Department of the Japan Research Institute Ltd., and also works with the Telecom Services Association of Japan (TELESA) (http://www.telesa.or.jp), an association of Internet service providers and other telecommunications providers in Japan. She participated in the development of TELESA's Guidelines for Codes of Practices for Internet Service Providers, which were finalised on 16 February 1998.

Mr. David W. PHILLIPS

Mr. PHILLIPS as Vice President & General Counsel for Europe, AOL Bertelsmann Online Europe, is responsible for developing and managing legal and public policy strategies for the AOL and CompuServe European brands. His particular area of expertise relates to legal and policy issues arising from the

provision of Internet and other online services in Europe. He has also handled numerous liability issues related to online content and communications issues (e.g. privacy, copyright, defamation, online crimes) and drafted and negotiated content, commerce and technology deals.

Mr. Markku ROPPONEN

Mr. ROPPONEN is the Director of the Finnish Internet Service Providers' Association, and an attorney with Scandinavian Law, Attorneys-at-Law, in Finland. He has extensive consulting experience in Telecommunications and Internet policy, more specifically with expertise in the areas of contract law, intellectual property law and communications law. He has also been instrumental in the development of international solutions to legal problems in the field of electronic trade. Mr. Ropponen regularly lectures on Internet and electronic commerce related areas, and has produced three official reports to the Finnish Ministry of Transport and Communications. Mr. Ropponen is also an active member of the Council of EuroISPA and the Chairman of the Board of Directors of CommerceNet Finland Oy.

Mr. Gordon ROSS

Mr. ROSS as Chief Executive Officer and President of Net Nanny Ltd. (http://www.netnanny.com) (a subsidiary of Net Nanny Software International Inc.), has steered Net Nanny Software International through various technology acquisitions and product developments. Under his leadership, Net Nanny continues to be the leading developer of tools that allow individuals, schools and corporations to protect their digital data according to their own values. As the driving force behind Net Nanny's conceptual design and functionality, he is dedicated to preserving free speech while allowing the protection of children, organisations and computer data.

Mr. Don SANDFORD

Mr. SANDFORD is President & Chief Executive Officer of Net Shepherd Inc. (http://www.netshepherd.com). He joined Net Shepherd in October of 1996 to transform the company into an online information service and commercialise its technology. His strong international business management experience with ICI plc. and other organisations brought to Net Shepherd a remarkable track record in marketing and business development, a quality essential to success during this time of emerging commerce on the Internet.

Mr. Christophe SAPET

Mr. SAPET is President of the Association des fournisseurs d'accès à des services en ligne et à Internet (AFA), and also the President and Founder of Infonie (http://www.infonie.fr), the first francophone multimedia network, launched in October 1995. Providing basic access, this online service provides users with information, education and entertainment resources, a virtual shop and many other communication tools for everyone in the family, according to their age group and specific interests.

Dr. James R. SAVARY

Dr. SAVARY represents the Consumers' Association of Canada and is an Associate Professor and Chair of the Department of Economics at Glendon College at York University (http://www.glendon.york.ca/). He specialises in consumer economics and information systems and technology economics. He serves as the Vice-Chair of the Canadian Standards Association Technical Committee on Privacy and is the Chair of the Canadian Payments Association Stakeholders Advisory Council. Mr. Savary is also involved in the work of the OECD Project Team on Consumer Issues in Electronic Commerce.

Mr. Peter UPTON

Mr. UPTON is the Executive Director of the Australian Information Industry Association (AIIA) (http://www.aiia.com.au/) and has held this post since November 1992. He has day-to-day responsibility for the management of the Secretariat to ensure its efficient carriage of Board policy and decisions, and to

represent agreed industry views to governments, the media, other groups and the general public. Before joining AIIA, Mr. Upton was Chief Executive Officer and Managing Director of the Australian and New Zealand operations of Burson-Marsteller Pty Ltd, the international public affairs and marketing agency. Prior to that he held a number of positions in Commonwealth Government central agencies.

Mr. Guy VERBEEREN

Mr. VERBEEREN is the Chief of the National Computer Crime Unit (NCCU), a branch of the National Brigade of the Judicial Police in Belgium. He has been a member of the Judicial Police since 1977 when he was assigned to the Financial and Computer Crime Division of the Courtrai and Brugges Judicial Police Brigade. The NCCU, which was created in September 1997, manages the Child Pornography Internet Contact Point programme of the Judicial Police which was set up to act swiftly on leads and information in this area (www.gpj.be).

Professor Michel VIVANT

Professor VIVANT is a Professor at the *Université de Montpellier*, (*http://www.sc.univ-montp1.fr)* in France. He is a specialist in intellectual property rights in general, and new technologies in particular, renowned both within and outside Europe. He is a member of the French High Council of Industrial Property and of the EU Commission DGXII's Legal Advisory Board (Intellectual Property Rights Task Force). Professor Vivant has published extensively on the following themes: patents, trademarks, copyright, computer law, communication and networks. He is frequently called upon to act as a national and international arbitrator and also regularly serves as a consultant for law firms and industry (e.g. EDF, Elf, IBM, Sligos). He also acts in the capacity of expert for several international organisations (in particular the Council of Europe's Committee of experts on Crime in Cyberspace) as well as the French Government.

LIST OF PARTICIPANTS

Steering Committee

Mr. Pierre LEDUC	Steering Committee Co-Chair Senior Officer Industry Canada CANADA
Ms. Suzanne Radell SETTLE	Steering Committee Co-Chair Senior Policy Advisor, NTIA/DIA Department of Commerce UNITED STATES
Mr. Joseph ALHADEFF	United States Council for International Business (USCIB) Business and Industry Advisory Committee (BIAC) to the OECD UNITED STATES
M. Didier BUREAU	Directeur Adjoint, Ministère de l'Economie, des Finances et de l'Industrie, Direction Générale des stratégies industrielles FRANCE
Mr. Deniz EROCAL	Business and Industry Advisory Committee (BIAC) to the OECD
Mr. Neil FEINSON	Head, International Communications Policy Section Department of Trade and Industry UNITED KINGDOM
Mr. Peter HANAK	National Committee for Technological Development HUNGARY
Mr. Masaaki KOBASHI	Ministry of International Trade and Industry (MITI) JAPAN
Mr. Yves LE ROUX	Corporate Security Program Office Digital Equipment Corporation FRANCE

Ms. Kate McGEE	Vice President, Corporate Affairs Oracle UNITED STATES
Mr. Kazutaka NAKAMIZO	Telecommunications Consumer Affairs Office Ministry of Posts and Telecommunications (MPT) JAPAN
Ms. Teresa PETERS	Information, Computer and Communications Policy (ICCP) Division Organisation for Economic Co-operation and Development (OECD)
Ms. Kristiina PIETIKAINEN	Senior Adviser Ministry of Transport and Communications FINLAND
Mr. Guido POUILLON	Advisor Institut Belge de Poste et Télécommunication (IBPT) BELGIUM
Mr. Luc RIFFLET	Permanent Delgation of Belgium to the OECD BELGIUM
Mr. Richard SIMPSON	Director General Electronic Commerce Task Force Industry Canada CANADA

Co-Chairmen

Mr. Richard C. BEAIRD	Chairman of the OECD Committee on Information, Computer and Communications Policy Senior Deputy Coordinator International Communications and Information Policy Department of State UNITED STATES
Dr. Etienne GOROG	Chairman of the BIAC Committee on Information, Computer and Communications Policy General Manager IT Solution Consulting – EMEA IBM Consulting Group, IBM Eurocoordination FRANCE

Moderators and speakers

Dr. Michael BAKER	Board Member, Electronic Frontiers Australia AUSTRALIA
Ms. Lisa BALABAN	Senior Vice President Business Affairs and General Counsel Sympatico/Medialinx Interactive, L.P. CANADA
Mr. Claude BOULLE	European Affairs, Groupe Bull FRANCE
Ms. Marilyn S. CADE	Director, AT&T UNITED STATES
Ms. Maria Livanos CATTAUI	Secretary General International Chamber of Commerce (ICC) FRANCE
Mr. Roger J. COCHETTI	Program Director, Policy & Business Planning IBM Internet Division UNITED STATES
Dr. A. EISNER	Chairman and Chief Executive Officer Association of Dutch Internet Service Providers (NLIP) NETHERLANDS
Ms. Susan J. GETGOOD	Director, Corporate Communications The Learning Company, Inc. UNITED STATES
Mr. David KERR	Chief Executive, Internet Watch Foundation UNITED KINGDOM
Mr. Manuel KOHNSTAMM	Vice President, Public Affairs Time Warner Europe BELGIUM
Mr. Akio KOKUBU	Senior Executive Director Electronic Network Consortium (ENC) JAPAN
Mr. Stefano LAMBORGHINI	Segretario Generale Associazione Italiana Internet Providers (AIIP) ITALY

Ms. Margo LANGFORD	Canadian Association of Internet Providers CANADA
Mr. Yves LE ROUX	Corporate Security Program Office Digital Equipment Corporation FRANCE
Mr. Walter J. O'BRIEN	President, National Advertising Review Council, Inc. UNITED STATES
Ms. Kazuko OTANI	General Manager, Legal Affairs Department Telecom Services Association of Japan (TELESA) The Japan Research Institute, Ltd. JAPAN
Mr. David W. PHILLIPS	Vice President and General Counsel for Europe AOL Bertelsmann Online (Europe) UNITED KINGDOM
Mr. Markku ROPPONEN	Director, Finnish Internet Service Providers' Association Scandinavian Law Offices, Attorneys-at-Law FINLAND
Mr. Gordon ROSS	Chief Executive Officer and President, Net Nanny, Ltd. UNITED STATES
Mr. Don SANDFORD	President and Chief Executive Officer, Net Shepherd, Inc. CANADA
Mr. Christophe SAPET	Président, Association des Fournisseurs d'Accès à des services en ligne et à Internet (AFA) President, Infonie FRANCE
Dr. James R. SAVARY	Consumers' Association of Canada CANADA
Mr. Peter UPTON	Executive Director Australian Information Industry Association (AIIA) AUSTRALIA
Mr. Guy VERBEEREN	Commissaire Judiciaire, Police Judiciaire Brigade Nationale National Computer Crime Unit Child Pornography Internet Contact Point BELGIUM

Mr. Michel VIVANT	Professeur Université de Montpellier FRANCE

Other Participants

Mr. Yaman AKDENIZ	Cyber-Rights and Cyber-Liberties UNITED KINGDOM
Mr. Joël d'ANGIO	DGCCRF FRANCE
Mr. Rogelio ARELLANO	Permanent Delegation of Mexico to the OECD
Ms. Rebecca ARBOGAST	Senior Counsel for International Law Federal Communications Commission UNITED STATES
Mr. Shoichiro ASANO	Professor, National Center for Science Information Systems (NACSIS) JAPAN
Ms. Véronique BARRY	Direction des Postes et Télécommunications FRANCE
Mr. Antoine BEAUSSANT	Président de GESTE FRANCE
Ms. Michel BEJOT	Avocat, SCP Bernard Hertz Béjot FRANCE
Mr. Rolf BENDER	Federal Ministry of Education, Science, Research and Technology GERMANY
Ms. François BLOCH	Attorney, Compuserve and UUNet FRANCE
Mr. Vilmos BOGNAR	Project Manager National Committee for Technological Development HUNGARY
Mr. Maurizio BONANNI	Ingegnere Elettronico Ministero Comunicazioni Italia ITALY

Mr. Sandor BOTTKA	Vice President National Committee for Technological Development HUNGARY
Mr. Wray CANDILIS	Director, Information Services Division International Trade Administration U.S. Department of Commerce UNITED STATES
Dr. Seung-Hee CHOI	Senior Researcher, Electronics and Telecommunications Research Institute KOREA
Mr. Tom DALE	Assistant Secretary, Regulatory Policy Branch Telecommunications Industry Division Department of Communications and the Arts AUSTRALIA
Mr. Jacques DELORME	Conseiller économique et commercial Représentation Permanente de la France près l'OCDE
Mr. Christine DEMARTINI	Service juridique et technique de l'information (SJTI) FRANCE
Mr. Daniel DOLAN	Permanent Delegation of the United States to the OECD
Mr. Rüdiger DOSSOW	Administrator, Media Section Directorate of Human Rights, Council of Europe
Mr. André DUBOIS	Industry Canada CANADA
Mr. Paige EASTMAN-SUBUH	Government Relations, IBM UNITED STATES
Ms. Marja EROLA	Programme Manager, TEKES FINLAND
Mr. Olivier ESPER	Autorité de Régulation des Télécommunications (ART) FRANCE
Mr. Didier ETIENNE	Service juridique et technique de l'information, SJTI FRANCE

Ms. Isabelle FALQUE-PIERROTIN	Conseil d'Etat FRANCE
Mr. David FARES	Manager, International Telecommunications and Information Policy US Council for International Business UNITED STATES
Mr. Pierre FIORINI	Ministère de l' Industrie, DGSI FRANCE
Mr. Paul FLORENSON	Ministry of Culture and Communication FRANCE
Mr. Alessandro FOGLIATI	Permanent Delgation of Italy to the OECD
Mr. Chantal FOURNIER	Service juridique et technique de l'information, SJTI FRANCE
Ms. Joëlle FREUNDLICH	Direction de la Réglementation et des Relations Extérieures FRANCE
Mr. René FRIES	Superior Counsellor, Ministry for Science and Transport AUSTRIA
Dr. Teresa FUENTES	Legal Officer, UNESCO FRANCE
Mr. Nobuhiro FUKUOKA	Deputy Director, International Policy Division Ministry of Posts and Telecommunications JAPAN
Mr. Gérard GABELLA	SPA Europe BELGIUM
Mr. Olivier GAINON	Chargé de Mission, CNPF FRANCE
Mr. Luigi GAMBARDELLA	Direzione Affari Generali e Regolamentari, Olivetti ITALY
Ms. Julie GARCIA	Senior Counsel, America Online, Inc. UNITED STATES

Yvonne GÄRTNER	European Affairs Associate Law & Corporate Affairs, Europe S.A. Microsoft N.V. BELGIUM
Ms. Marie GEORGES	CNIL FRANCE
Dr. Haluk GERAY	Consultant, Institute for Information Technologies and electronic Research TURKEY
Ms. Susan J. GETGOOD	Director, Corporate Communications The Learning Company, Inc. UNITED STATES
Mr. Yonca GÜNDÜZ-ÖZÇERI	Permanent Delegation of Turkey to the OECD
Ms. Kim HAALAND	Industry Canada CANADA
Mr. Jostein HÅØY	Deputy Director General Ministry of Trade and Industry NORWAY
Ms. Hora HARING	Permament Delegation of Germany to the OECD
Ms. Heidi HIJIKATA	Director, Software Division International Trade Administration U.S. Department of Commerce UNITED STATES
Mr. Zoltan HORVATH	First Secretary Permanent Delegation of Hungary to the OECD
Mr. Axelle HOVINE	Service juridique et technique de l'information -SJTI FRANCE
Mr. Tomoya ICHIMURA	Deputy Director, Office of International Co-operation for Information Infrastructure Machinery and Information Industries Bureau Ministry of International Trade and Industry JAPAN
Mr. Francesco IMPARATO	Lawyer ITALY

Mr. Takaya ISHIDA	Senior Chief Researcher, Mitsubishi Electric Corporation Corporate Research & Development JAPAN
Mr. Klaus-Dietmar JACOBY	Permament Delegation of Germany to the OECD
Mr. Eivind JAHREN	Deputy Director General Ministry of Trade and Industry NORWAY
Mr. Brian KAHIN	Senior Policy Analyst, Information Infrastructure Office of Science and Technology Policy Executive Office of the President UNITED STATES
Mr. Daniel KAHN	Avocat à la Cour, Cabinet Kahn & associés FRANCE
Mr. Zoltan KATONA	
Mr. Keiichi KAWAKAMI	First Secretary Permanent Delegation of Japan to the OECD
Mr. David KERR	Chief Executive, Internet Watch Foundation UNITED KINGDOM
Ms. Margaret A. KESHISHIAN	Permanent Delegation of the United States to the OECD
Mr. Reinhard KNORRECK	Permanent Delegation of Austria to the OECD
Ms. S. KRAEMER	DG XIII, European Commission
Ms. Nathalie LABOURDETTE	Administrator, European Commission
Mr. Claude LAFONTAINE	Broadcasting Policy Branch Department of Canadian Heritage CANADA
Ms. Isabelle LA FONTAINE	Direction des Postes et Télécommunications, Secrétariat d'Etat auprès du Ministre de l'Economie, des Finances et de l'Industrie, Chargé de l'Industrie FRANCE
Mr. Edgar DE LANGE	Ministry of Transport, Public Works and Water Management NETHERLANDS

Mr. Laure de LATAILLADE	Directeur de GESTE FRANCE
Mr. Michele LEDGER	Consultant, INTUG BELGIUM
Mr. Eric LEE	Public Policy Director, Commercial Exchange UNITED STATES
Mr. Jae Woong LEE	Deputy Director, International Economic Bureau Ministry of Foreign Affairs and Trade KOREA
Dr. Kyung Koo LEE	Senior Member of Technical Staff Korea Information Security Association KOREA
Ms. Marie-Françoise LE TALLEC	Service juridique et technique de l'information (SJTI) FRANCE
Mr. Jean-Christophe LE TOQUIN	Service and Internet Access Providers Association FRANCE
Mrs. Irène LEVI-MUSTRI	FRANCE
Ms. Kelly LEVY	Deputy Associate Administrator National Telecommunications & Information Administration, U.S. Department of Commerce UNITED STATES
Mr. Ros De LOCHOUNOFF	Directeur juridique, GESTE FRANCE
Ms. Mette LUNDBERG	Head of Section, Telecoms Policy Division Ministry of Research and Information Technology DENMARK
Mr. John LYNN	Telecommunications Counsel, EDS Corporation UNITED STATES
Ms. Annie MARI	Direction des Affaires Economiques et Financières Ministère des Affaires Etrangères FRANCE
Ms. Maria MARTIN-PRAT	Administrator, European Commission DG XV – Internal Market and Financial Services

Mr. Hubert MARTY-VRAYANCE	Service Central de la Sécurité des Systèmes d'information FRANCE
Mr. Michael McCABE	International Communications and Information Policy Bureau of Economic Affairs US Department of State UNITED STATES
Ms. Alicia MIGNONE	Permanent Delegation of Italy to the OECD
Ms. Hélène de MONTLUC	Ministry of Culture & Communication FRANCE
Mr. Minoru MORISHITA	Deputy Director Telecommunications Consumer Affairs Office Ministry of Post and Telecommunications, JAPAN JAPAN
Ms. Barbara MOTZNEY	Senior Policy Analyst, Broadcasting Policy Branch Department of Canadian Heritage CANADA
Mr. Robert MOURIK	Ministry of Transport, Public Works and Water Management NETHERLANDS
Mr. Jean-Pierre NORDMAN	TLC/Edusoft FRANCE
Mr. Jun OKAYAMA	Director, Trade Policy Office International Affairs Department Ministry of Post and Telecommunications JAPAN
Mr. Michel PACHE	Chef du Service International des Media Département fédéral des Affaires étrangères SWITZERLAND
Mr. Bruno DE PADIRAC	Senior Management Officer, UNESCO FRANCE
Ms. Marie PANCZEL	Permanent Delegation of Hungary to the OECD
Mr. Paul PIERLOT	Industry Canada CANADA
Mr. Ilmari PIETARINEN	Counsellor, Ministry of Finance FINLAND

Ms. Charlotte-Marie PITRAT	Secrétariat général du Gouvernement FRANCE
Mr. Dallis RADAMAKER	Vice President, European Public Policy Software Publishers Association NETHERLANDS
Mr. Bong Ha RHA	First Secretary Permanent Delegation of Korea to the OECD
Mr. Jonghyuk RO	Deputy Director, International Co-operation Bureau Ministry of Information and Communication KOREA
Mr. Luc ROCHARD	DGCCRF FRANCE
Mr. Nicolas ROS DE LOCHOUNOF	Transiciel FRANCE
Mr. Joseph ROYEN	Conseiller-adjoint Ministère des Affaires Economiques Administration de la Politique commerciale FRANCE
Mr. Pascale de SAINTE-AGATHE	Ministère de l' Industrie, DGSI FRANCE
Mr. Martin SALAMON	Special Advisor Telecoms Policy Division Ministry of Research and Information Technology DENMARK
Mr. Christophe SASSERANT	Senior Consultant, SV&GM FRANCE
Mr. Phil SAUNDERS	Vice President, Commercial Relations Nortel CANADA
Ms. Florence SCHMIDT-PARISET	Ministry of Justice, SAEI FRANCE
Mr. Vidal SERFATY	Ministry of Culture & Communication FRANCE

Mr. Michael SCHNEIDER	Council Member, Director Regulation and Self-Regulation European Internet Service Provider's Association (EuroISPA) GERMANY
Ms. Diana SHARPE	Barrister & Solicitor of The High Court of Australia Special Advisor, Communications & Technology CHAIR-INTUG AUSTRALIA
Mr. Ted SHAPIRO	Deputy Legal Counsel, Motion Picture Association BELGIUM
Ms. Catherine SOUBEYRAND	Ingénieur, CNET FRANCE
Mr. Len St-AUBIN	Industry Canada CANADA
Mr. Alfred STRATTL	Director, Ministry for Science and Transport AUSTRIA
Mr. Fredrik SYVERSEN	Consultant, Norwegian Association of Business Machine Vendors The Norwegian Internet Society NORWAY
Mr. Richard SWETENHAM	Principal Administrator DG XIII, European Commission
Mr. Andras SZIGETI	Deputy Director General, Prime Minister's Office HUNGARY
Ms. Jennifer TALLARICO	Electronic Commerce Policy Advisor International Trade Administration U.S. Department of Commerce UNITED STATES
Mr. Michael TIGER	Industry Canada CANADA
Mr. Pierre TRUDEL	Professor, Centre for Research in Public Law Université de Montréal CANADA

Mr. Christiaan VAN DER VALK	Policy Manager, Electronic Business Coordinator, Policy Commissions International Chamber of Commerce (ICC) FRANCE
Mr. Daniel J. WEITZNER	Deputy Director, Center for Democracy and Technology UNITED STATES
Mr. Nigel WILLIAMS	Director, Childnet International UNITED KINGDOM
Mr. Mabito YOSHIDA	First Secretary Permanent Delegation of Japan to the OECD
Mr. Didier ZMIRO	Ministère de l' Industrie, DGSI FRANCE
Mr. Haluk ZONTUL	Project Manager, Institute for Information Technology and Electronic Research TURKEY

OECD Secretariat

Mr. John DRYDEN	Head of Division Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Mr. Jeremy BEALE	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Ms. Laurie LABUDA	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Ms. Marta MONTESINOS	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Mr. Sam PALTRIDGE	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry

Ms. Kyoko SATO	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Mr. Jürgen SPAANDERMAN	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Mr. Shigeyoshi WAKAYABASHI	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Ms. Lisa WATSON-COOK	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry
Mr. Dimitri YPSILANTI	Information, Computer and Communications Policy (ICCP) Division Directorate for Science, Technology and Industry

SPEAKERS' PRESENTATION MATERIALS

Panel No. 1: What are the pressures for self-regulation and where do they come from?

Manuel Kohnstamm
Time Warner Europe

Internet Self-regulation

Slide One
Time Warner

- New Opportunities On The Web
- Great Potential For Kids
- cnn.com, warnerbros.com
- time.com, fortune.com, money.com
- 120+ Websites, 200+ million visitors a week

Slide Two
"Content Industries"

- More Than Its Name Would Suggest
- Covers Many Individual And Collective Expressions
- Artistic Freedom
- Editorial Independence

Slide Three
Editorial Independence

- The Heart Of Content Industries
- Creative vs. Commercial Interests
- Voluntary Rating Is An Option
- No Substitute For Parental Responsibility

Slide Four
Media Experience

- News and Information Edits
- Decades Of Experience in Content Selection
- CNN Does Not Show Everything It Has
- Protecting Media Brand Value

Slide Five
Educational Exercises

- Public Education And Awareness
- Digital Toolbox
- Responsible Industry Behaviour
- Empowerment Of Parents /Educators

Slide Six

Self-regulating Content

- Active Co-operation For Different Audiences
- Brands Provide Strong Customer Guarantee
- Protect Free Flow Of Information
- Promotion Of Self-regulation By EU

Slide Seven

Conclusions

- Cautious With Rating Expectations
- Sensitivity For Sex Is Temporal
- Individual Facilitating Tool
- Rating An Option, Not A Default Setting

Panel No. 1: What are the pressures for self-regulation and where do they come from?

Lisa Balaban
Sympatico/MediaLinx Interactive

CYBER LAW 101 – AN INTERNET PRIMER

Index

- Cyber Law 101
- Terms and Conditions/Modalités et conditions (see attachment below)
- Important Advisories/Recommandations importantes (see attachment below)

Road Map

- Cyberlaw 101 – Overview
- Key Legal Issues
- Site Visits and General Discussion

Cyber Law 101: The Internet

- A network of networks (>100K servers)
- Spanning multiple jurisdictions and cultural norms (> 80 nations)
- Used for personal and commercial activities by millions (>100M users)
- With no central control or management
- Providing near instant access to volumes of content from multiple sources

What are the Rules?

Legislation

- No specific "cyberlaw" in Canada
- Industry Canada currently reviewing issues in consultation with ISPs and industry experts
- *Criminal Code*, *Copyright Act*, *Trade-Marks Act*, *CCQ*, privacy and consumer protection legislation, common law ……
- Laws of general application

Regulation

- Other than tariffed services, no regulation
- CRTC has acknowledged that it has no authority to regulate the Internet but it may try to regulate access providers

Who Are Some of the Players?

- Backbone Providers
- ISP: Internet Service Providers
- OSP: On-Line Service Provider
- Intranet: Internal networks

Key Legal Issues

Liability of service providers:

- Content
- Access
- Employees

Intellectual Property Issues:

- Copyright and trade-mark infringement
- Domain names registration and protection

Privacy issues:

- Service members' and visitors' privacy
- Related services

Electronic commerce:

- Credit clearance and fraud
- Security

Liability of Service Providers

Who is responsible?

- Still unsure
- A number of service providers (primarily BBSs) have been charged and requested to restrict access to certain sites:
  - *R. v Hurtubise* - B.C. BBS convicted of distributing porn
  - CompuServe suspended access to newsgroups in response to German government request
- Most examples involve copyright infringement
- US courts have found online service providers liable regardless of their knowledge of or consent to the infringing material:
  - *Playboy v Frena* (photos)
  - *Sega v Maphia* (games)
  - *Religious Technology Center v. Netcom* (written works)
- In Canada, the Copyright Subcommittee to IHAC is in agreement with the US trend

What is content?

Content:

- computer code
- graphics
- text
- video and audio

- Primary media focus has been on "obscene" content

- Current Canadian criminal law criminalizes obscenity and child porn (creating, distributing and making available for distribution)
- The creation and distribution of general pornography is not illegal in Canada
- Recent prosecutions and investigations have been against the individuals posting or downloading, not the ISPs

Content and Control

"Content"

- Self created
- Member and Commercial User Content
- Newsgroups
- The Internet (none of the above)

Control

- Access
- Servers
- Self created content

Self Created Content:

- Creation and control are in ISP's hands
- Agreements with employees, subcontractors, partners are needed to ensure compliance with laws and policies

Member and Commercial Users:

- Creation and control are in the hands of the individual members or commercial users
- Agreements, such as the end user agreement for the access/online service, are required to ensure compliance with laws and policies

Internet Content:

- Creation and control are beyond ISP's reach
- No ISP can monitor or otherwise control content on the Internet at large
- According to Microsystems, creator of CyberPatrol screening software, only 1 to 2 per cent of all content on the Internet contains "generally unacceptable" material

Content in newsgroups:

- Newsgroups:
  - collection of messages with related theme
  - divided into categories which try to define broad groups: bit.listserv, biz, comp, misc (doesn't fit elsewhere), news, rec (hobbies, games and recreation), sci, soc (Social groups, ethnic groups), talk, alt (controversial or unusual topics)
  - names start with broad hierarchy, followed by more specifics on the topic of discussion
  - creation is largely beyond ISP's reach however control may be in part within its grasp
  - ISPs can't control content but do "control" which newsgroups to carry
  - according to Microsystems, most of the unacceptable and illegal material is located in newsgroups (bestiality, child pornography, pirated software)

Control in the Hands of Members:

- Software Tools
  - Members can use filtering (access control and lists NetSheppard, CyberPatrol, NetNanny) software to restrict access to potentially illegal or unsuitable material
- Rating System
  - ISPs can participate in industry initiatives to develop standard rating and blocking guidelines

Content Control Increases Risk

- "Publisher"(Producer): Stratton Oakmont v Prodigy
- "Distributor"(Carrier): Cubby v CompuServe
- US caselaw suggests that if ISP exerts editorial control over content the risk of being held responsible increases
- Due to nature of Internet - "clean" "family" service is impossible
- Attempts to control or censor content will by its nature demonstrate an increased sense of responsibility, which may translate into an increase in liability for the ISP

OSP as Publisher (Libel and Defamation)

- *Stratton Oakmont v Prodigy* - Prodigy found to be "publisher" of libelous statements made by subscriber on one of its online bulletin boards
- Prodigy's editorial role key to liability
- Discourages service providers from screening material

OSP as Distributor (Libel and Defamation)

- *Cubby v CompuServe* - OSP not liable for defamatory statements posted to its bulletin boards
- Liability only if the OSP "knew or had reason to know" of the posting and took no action
- Cubby not viewed as an "editor" or "publisher" but as a "distributor" (library or newsstand)
- Encourages service providers to take a minimal role in censoring or controlling content

<u>Access</u>

- Telecommunications companies provide communication lines for other ISPs and OSPs (common carrier)
- Telecommunications company servers may store content for customers and corporate clients (control)
- Telecommunications company newsservers are used by other ISPs (control)

<u>Employees and Consultants</u>

As employer, ISP may be found liable to third parties for the activities of its employees for:

- Damages caused or arising in the performance of his/her duties (downloading and/or posting), misuse of e-mail
- Modifications to Bell Websites or customer Websites

As employer, ISP may be at risk from the activities of its employees:

- Misappropriation of trade secrets maintenance of confidentiality in general
- Privacy (interception of private communications) and e-mail problems (internal) theft of time

Risks can be reduced by adoption of E-mail and Internet Use Policies that:

- Prohibit personal use and illegal conduct (service agreement similar to that required by end-users)
- Control access
- Inform employees and consultants of the risks and procedures and update them regularly
- Provide for occasional monitoring
- Address network security (firewalls, passwords and encryption policies)

Intellectual Property Issues

Copyright Infringement

- No Canadian caselaw
- US courts have found parties liable for indirect infringement - regardless of their knowledge or approval of what was uploaded:
  - *Playboy* v *Frena* (photos)
  - *Sega* v *Maphia* (games)
  - *Religious Technology Center v Netcom* (written works)

Copyright

Common Carriers

- Suggestion in the Copyright Subcommittee Report of the Advisory Council on the Information Highway to add ISPs as common carriers
- S. 3 of the *Copyright Act* relieves common carriers from liability

The Copyright Subcommittee to IHAC recommended that BBSs be liable for copyright infringement on their service (constructive knowledge)

Types of Issues:

- Identifying “owner” or “author”
- Copying and downloading (reproduction, communication, performance)
- Morphing
- Framing
  - *Westminster.com*
- Hyperlinking
  - Shetland Times Ltd. v The Shetland News
  - totalnews.com
- Jurisdiction

Trade-marks

Types of Issues:

- In Canada, Common law and *Trade-marks Act* apply
- Domain names
  - Non-governmental bodies manage the Internet address systems (NSI and others)
  - Conflicting legitimate uses
- Icons and linking
- Passing off
- Jurisdiction

Privacy

Legislation:

- Quebec (individual)
- Other provinces and federal (public)

Other:

- IHAC
- CSA *Model Code for the Protection of Personal Information* and *STENTOR CODE*
- Uniform Law Conference of Canada draft *Private Sector Protection of Personal Information Act*
- Proposed Canadian legislation on privacy and cryptography

Members and Visitors

- "Private" communications via e-mail
- Tracking profiles and preferences
- Direct "mail"
- Security of servers
- Sharing of information with other ISPs, partners and/or third parties

Related Services

- Directories
  - Unlisted numbers/addresses "accidentally" published
  - Mapping services without published numbers (worldpages.com)
- E-tailing
  - consumer buying habits
  - equipment
  - credit and other financial information
  - security

Electronic Commerce: E-tailing

ISPs Role:

- Offering e-tailing infrastructure for merchants
- Providing servers for infrastructure of third parties
- Hosts, within its own sites, the e-tailing services of others
- Selling its own products and services

E-tailing

- Credit card clearance
- Fraud
  - consumer
  - "merchants"
- Security
  - Servers
  - Site Verification and Certification

Conclusion: What do we know?

- If ISP takes an active role in "controlling" content it may be held liable for all content on its networks, be forced to attempt to screen all content before it is allowed on its servers (news or otherwise)
- Certain ISPs (those by major corporations and PTTs) appear to be held to a higher standard than other ISPs by the general public
- If ISP doesn't take some role, public opinion may be negative

What are we doing?

Clauses in employment and service agreements for ownership and compliance with laws
Service Agreements

- Disclaimers
- Allocation of risk to parties with control such as Members/commercial customers
- Provide for termination of service

Terms and Conditions on Sites

- Admiralty Law Approach: Canadian laws apply
- Trade-mark and copyright notices
- Disclaimers on content and Members' Forums
- Assumption of responsibility for content within our "control"
- Allocation of risk to visitors with control
- New Members' Section including Guidelines for safe surfing with children
- Constantly updating the Site with Frequently Asked Questions

Most Canadian ISPs do not routinely "censor" content , but:

- will respond to complaints and terminate access or service if required
- Personal Webpages of Members which contain potentially illegal material are occasionally removed as a result of commercial reasons for their removal
- will work together and separately educating the public and government

STENTOR and the SOCs have indicated their support of CAIP Guidelines

Sympatico Ad hoc Team made recommendation for Personal Webpages and is working with SOCs to develop policy on newsgroups

Sympatico Members are provided with information on industry trends and developments - on site

Sympatico Members provide feedback through e-mail and forums

Meet regularly to discuss specific Internet related policy and legal issues

Monitor relevant developments in case law and legislation on Internet issues - nationally and internationally

Participate in business meetings on Internet issues, as well in associations such as the Canadian Association of Internet Providers and OECD

Attachment to Lisa Balaban's Presentation Materials
(extracts from Sympatico Website, *www.sympatico.ca*)

Terms and Conditions

MediaLinx Interactive Inc. ("MediaLinx") provides the Sympatico Home Page and other Sympatico content (collectively, the "Sympatico Site") subject to your compliance with the terms and conditions below. PLEASE READ THIS BEFORE ACCESSING THE SYMPATICO SITE. BY ACCESSING THE SYMPATICO SITE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS BELOW. IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS AND CONDITIONS, YOU MAY NOT ACCESS OR USE THE SYMPATICO SITE.
By accessing the Sympatico Site you agree to be bound by the terms and conditions listed below:

1. Rules.

While visiting the Sympatico Site, you may not: post, transmit or otherwise distribute information constituting or encouraging conduct that would constitute a criminal offense or give rise to civil liability, or otherwise use the Sympatico Site in a manner which is contrary to law or would serve to restrict or inhibit any other user from using or enjoying the Sympatico Site or the Internet; post or transmit any information or software which contains a virus, cancelbot, trojan horse, worm or other harmful or disruptive component; upload, post, publish, transmit, reproduce, or distribute in any way, information, software or other material obtained through the Sympatico Site which is protected by copyright, or other intellectual property right, or derivative works with respect thereto, without obtaining permission of the copyright owner or rightholder.

2. Monitoring.

MediaLinx has no obligation to monitor the Sympatico Site. However, you agree that MediaLinx has the right to monitor the Sympatico Site electronically from time to time and to disclose any information as necessary to satisfy any law, regulation or other governmental request, to operate the Sympatico Site properly, or to protect itself or its subscribers. MediaLinx will not intentionally monitor or disclose any private electronic-mail message unless required by law. MediaLinx reserves right to refuse to post or to remove any information or materials, in whole or in part, that, in its sole discretion, are unacceptable, undesirable, or in violation of this Agreement.

3. Privacy.

MediaLinx cannot insure or guarantee privacy for Sympatico users. It is therefore recommended that this service not be used for the transmission of confidential information. Any such use shall be at the sole risk of the user, and MediaLinx and its affiliate and related companies shall be relieved of all liability in connection therewith.

4. Buying over the Internet.

When making purchases or other transactions through the Sympatico Site or the Internet, you may be asked by the merchant or information or service provider to supply certain information, including credit card or other payment mechanisms. You agree that all information you provide any merchant or information or service provider through the Sympatico Site will be accurate and complete. You agree to pay all charges incurred by you or other users of your account and credit card or other payment mechanisms at the prices in effect when such charges are incurred. You also will be responsible for paying all applicable taxes, if any, relating to purchases on the Sympatico Site. MediaLinx is in no way responsible for paying all applicable taxes, if any, relating to purchases on the Sympatico Site. MediaLinx is in no way responsible for any charges you or any user of your account incurs when making purchases or other transactions in this manner.

5. Limitation of Liability.

MediaLinx takes no responsibility for the accuracy or validity of any claims or statements contained in the documents and related graphics on the Sympatico Site. Further, MediaLinx makes no representations about the suitability of any of the information contained in the documents and related graphics on the Sympatico Site for any purpose. All such documents and related graphics are provided without warranty of any kind. In no event shall MediaLinx be liable for any damages whatsoever, including special, indirect or consequential damages, arising out of or in connection with the use or performance of information available from the service.

6. Recourse.

If you are dissatisfied with the Sympatico Site or with any terms, conditions, rules, policies, guidelines, or practices of MediaLinx in operating the Sympatico Site, your sole and exclusive remedy is to discontinue using the Sympatico Site.

7. Confidential Information.

You authorize MediaLinx to collect from any party and to retain all relevant information relating to your use of the Sympatico Site, and you hereby authorize any party to provide us with such information. You understand and agree that unless you notify MediaLinx to the contrary by e-mailing us, you further authorize MediaLinx to disclose, on a confidential basis, to any party with whom MediaLinx has business relations all relevant information relating to your dealings with us and the Sympatico Site. We will open and maintain a file in your name, which file will be kept at our head office. You may access your file or such credit reports free-of-charge upon 24 hours' prior written request to our credit department at our head office. If any of the information contained in your file or in such reports is inaccurate, you may make a written request for rectification, specifying the information to be rectified and explaining the inaccuracy, to our credit department at our head office.

8. Indemnity. You agree to defend, indemnify and hold MediaLinx and its and its affiliate and related companies harmless from any and all liabilities, costs and expenses, including reasonable attorneys' fees, related to any violation of this Agreement by you or users of your account, or in connection with the use of the Sympatico Site or the Internet or the placement or transmission of any message, information, software or other materials on the Sympatico Site or on the Internet by you or users of your account.

9. Trademarks.

SympaticoTM and other names, logos and icons identifying Sympatico and MediaLinx products and services referenced herein are trademarks or registered trademarks of MediaLinx. All other product and/or brand or company names mentioned herein are the trademarks of their respective owners.

10. Territory.

The Sympatico Site originates in Canada.

11. Miscellaneous.

This Agreement, including any and all documents referenced herein constitutes the entire agreement between MediaLinx and you pertaining to the subject matter hereof. MediaLinx's failure to insist upon or enforce strict performance of any provision of this Agreement shall not be construed as a waiver of any provisions or right. If any of the provisions contained in this Agreement be determined to be void, invalid or otherwise unenforceable by a court of competent jurisdiction, such determination shall not affect the remaining provisions contained herein. This Agreement shall be governed by and construed in accordance with the laws of the province of Ontario and the federal laws of Canada applicable therein. The parties have required that this agreement and all documents relating thereto be drawn up in English. Les parties ont demandé que cette convention ainsi que tous les documents que s'y rattachent soient rédigés en anglais.

Recommendations

The Internet is a vast and uncontrolled source of information. The Sympatico service gives its members full access to the Internet and all it has to offer. If you have concerns about security, legalities, viruses or objectionable material, please read the advisories below.

What is the content policy of the Sympatico service?

- Content policy of the Sympatico service

The Internet consists of a global collection of networks and computers with no one organization responsible for its supervision or operation. Due to its dynamic nature, providers of Internet service, including Bell Global Solutions (BGS), are unable to monitor or control the worldwide mass of content available on the Internet. As such, BGS is unable to provide assurances that all material accessible through the Sympatico Internet service will be free of illegal or otherwise unsuitable content.

In response to growing concerns over particular content available on newsgroups and Personal Web pages, BGS has the following policy regarding content available through the Sympatico Internet service:

- As a provider of Internet service and member of the Canadian Association of Internet Providers (CAIP), BGS will not knowingly host on its equipment, newsgroups and Personal Web pages containing content which would likely constitute a violation of Canadian law.
- BGS will investigate and respond, where appropriate, to legitimate concerns and complaints related to content available on newsgroups and Personal Web pages, hosted on BGS equipment in an effort to minimize content which BGS reasonably believes is in violation of Canadian law.
- Newsgroups bearing titles which suggest that their respective content may contain visual representations that BGS believes may be contrary to Canadian law, such as child pornography, bestiality, necrophilia, paedophilia, as

well as pirated software, will not be directly accessible to Sympatico Internet service members in the BGS territory through its news server equipment.

- BGS encourages the responsible use of newsgroups, Personal Web pages and the Internet by all members. To assist our members in accessing content which is suitable to their needs, we provide online help, reviews of software that serve to filter Internet content, education on using the Internet, and password management to limit access to the Internet from a member's account. We also encourage parents to explore the wonders of the Internet together with their children. To this end, we offer an area designed especially for children and teens.

Restricting children's use of the Internet

- Can I restrict my children's use of the Internet?

The long and the short of it is "Yes, you can, but no, we cannot." Let us explain. You have probably heard about the controversy surrounding the uncensored and uncontrolled nature of the Internet. The Internet is not owned or controlled by any organization or country, and it knows no geographic boundaries. There are those who wish to control and censor it, and those who don't; and those who say it can't be done in any case. Due to the uncensored nature of the Internet, some material (a very small proportion of the total) is certainly inappropriate for a young audience and, some would say, even for adults. If you look for it, sexually explicit material, hate propaganda and other objectionable material can be found.

What we offer through the Sympatico service is full uncensored access to the Internet, in all its glory and with all its warts. The question is: how to get the value out of the Internet while avoiding its warts? We offer the following suggestions:

1. Within the Sympatico Web site, we provide an area for children and teens called "Definitely Not For Adults" (DNA). Our intention with this area is to provide hundreds of links to sites on the Internet (selected from many thousands) which we feel are appropriate for a younger audience. We recommend that you encourage your children to surf within this area. Sites have been selected that are interesting, educational, fun, or just plain silly, but do not knowingly contain any material of an objectionable nature (and if you do not agree with one of our selections, we would like to hear from you!).

A note of caution: While we have made every effort to review the contents of the sites we have selected for children, it should be recognized that we do not have control over these sites, which have been created by third parties. Furthermore, Internet sites that are one or more links removed from "DNA" may not fit our selection criteria. And lastly, unsupervised, your children can purposely or accidentally access other sites directly on the Internet that would not be appropriate for them.

2. There are now a few commercially available software products that you can purchase and install on your computer to "block out" objectionable material on the Internet. These products act something like "virus checkers", but they scan for objectionable material on the Internet rather than viruses on your computer. These products attempt to block out any known material that would be unsuitable for a young person before it comes to your computer. Information on these products (such as SurfWatch, Net Nanny, CYBERSitter, Internet Lifeguard) can be found on the Internet (select SEARCH on the Sympatico toolbar) and at your local computer store; or you can see our Review of censoring software. If searching on the Internet, try using search words such as screening; parental; control; blocking software.

A note of caution: While these products can be highly effective, they are not guaranteed foolproof. See our reviews of censoring software.

3. You can password-protect your Sympatico account. This means that each time someone connects to the Sympatico service from your computer, they will be asked for a password. If you are the only one who knows the password, your children can't access the Internet if you are not around. Read our instructions on how to password-protect your Sympatico account.

4. Since the Sympatico service does not (and cannot) restrict your use or your child's use of the Internet, the only guaranteed safe way for your child to surf is with you! Discover together.

- Review of Censoring Software
- Can my computer get a virus from the Internet?
- Can I restrict use of my Sympatico account with a password?
- Basic tips on surfing securely
- What to know about shopping online

- Is it safe to use my credit card on the Internet?
- Terms and Conditions for using the Sympatico Web site

If you have a concern not listed here, you can search by keyword for it within Sympatico Help (see Search box below), or click on Contact Us on the Sympatico toolbar at the bottom of this page to send a message to Sympatico Member Services.

Panel No. 2: What are key industry codes of conduct and corporate practices and why do they work?

Stefano Lamborghini
Associazione Italiana Internet Providers (AIIP)

CODE OF CONDUCT FOR INTERNET SERVICE PROVIDERS IN ITALY

In 1997 the Italian Association of Internet Service Providers (AIIP) with the support of other Italian organisations drafted a document aimed at creating a Code of Conduct for Internet Service Providers. The working group for the Code of Conduct started its activity by selecting and analysing main codes of conduct for Internet Service Providers, national laws on telematic services and other regulatory and self-regulatory projects existing at the time in EU countries, Canada, Australia and Japan.

In May 1997 a final draft text of the Code was submitted to a forum for discussion at the Italian Ministry of Communications, composed by representatives of the Ministry of Communications, Telecom operators and consumers associations. After some months of debate, the definitive text was approved and adopted as the official Italian Internet Service Providers Self-Regulation Conduct.

The fundamental aim of the Italian ISPs' Code of Conduct is the creation of a proper cultural, economical and technical environment for the development of the Internet Market. This will deeply influence the other main aspects of the Internet such as E-Commerce, Education, Information and Telework. The creation of some basic rules concerning the contents and the liability on the Internet is considered essential in order to achieve the mentioned aim of the Code. Therefore, besides other important general principles and obligations, the code concerns three main points of reference for the self-regulation of ISPs activity:

- First of all, the concept of liability on the Internet: who is liable for what? The fundamental idea is that every player (commercial operator or simple user) can make content available to the public on the Internet. Therefore, when someone publishes some content on the Internet (commercial sites or personal Web pages), he/she will provide content to the public. Moreover, the definition of roles played by commercial operators or by end users is not important in order to establish the liability for the contents: focus must be pointed on the single activities of the Internet players and it is, also, necessary to make a clear distinction between the simple services (access, hosting, etc.) and the activities of general provision of content to the public. It must be considered that the ISPs cannot devote time and money to monitor the content made available to the public by other players. So, according to this Code of Conduct, when offering a simple service of access or hosting, ISPs should not be considered liable, but for the content they make available to the public.

- On the other hand, in order to establish the liability of players who make content available to the public on the Internet, it is necessary to have the possibility to trace them on the Internet and to ensure their identification.

- Thirdly, anonymity must be defended. Anonymity safeguard is essential for the development of the Internet, for the diffusion of information and data, for the individual's privacy.

The Code of Conduct takes into consideration other important principles and obligations concerning the respect of human life, the refusal of every kind of discrimination, the protection of children against sexual

exploitation and the respect of minors sensitivity. In order to prevent every action against minors, the Code favours the adoption of filtering, blocking and rating standard systems by the ISPs and the possibility to inform and assist the end users in the implementation of such systems.

The principles of the Code also address the safeguards of Privacy and the treatment of personal information and data through Internet, starting from the constitutional principle of secrecy of correspondence to the recent Italian regulations on Privacy.

Another very important matter considered by the Italian Code is the protection of Intellectual Property Rights. Intellectual Property, and Copyright in particular, is extremely important in order to safeguard protected works and also to ensure the creation of a market for the information and the development of the Internet as an instrument for education, training and for the diffusion of the culture. In this light, the Code takes in account the fulfilment of all the requirements of Italian author rights, EU directives and WIPO treaties.

Another important part of the Code of Conduct concerns the mechanism of management and implementation of the Code. This part starts from the point that a simple declaration of principle is not sufficient to implement the rules effectively. The Code of Conduct, to this aim, considers a two phase period for the creation of competent bodies for the management and implementation of the Code. A first phase will see the birth of a self-regulatory body (*IARI - Instituto per l'AutoRegolamentazione di Internet*) that will follow the first steps of the implementation of the Code and will prepare the ground for the second phase. In the second phase, the self-regulatory body will change in a regulatory committee (*Comitato di Attuazione del Codice*) and will appoint the members of a dispute settlement body (*Giurì di autotutela*).

The main tasks of the regulatory committee will be:
- to follow the development of the Code of Conduct and to make changes in self-regulation according the technological and marketing evolution of the Internet;
- to inform and support ISPs in implementing the Code;
- to support the activities of the disputes settlement body;
- to develop contacts and relationships with similar self-regulatory bodies from other countries, organizations and governmental bodies;
- to conduct research and studies on the regulation of the Internet environment.

The tasks of the disputes settlement body will be:
- to enforce the respect of the Code obligations by the ISPs;
- to receive information about violations of Code obligations;
- to sanction the misuse of the Internet.

The dispute settlement body of the Italian Code of Conduct could soon have some important developments, because AIIP is dealing with the Chamber of Commerce of Milan regarding the proposal for the creation of an online arbitration and conciliation system ("Virtual Chamber") that has many common points with the Giurì of the Code. A co-operation at European, but also at the worldwide level, is strongly favoured by the Code of Conduct in order to adopt self-regulatory common rules and to harmonize national legislation. AIIP is a founding member of EuroISPA, the European ISPs Association, and its main goal is the creation of common rules for Internet operators in Europe. AIIP is also in contact with the OECD and the European Commission in order to promote proposals and to co-operate with important projects concerning content regulation and Internet development.

Panel No. 2: What are key industry codes of conduct and corporate practices and why do they work?

Mr. Walter J. O'Brien
National Advertising Review Council, Inc

CHILDREN, CONTENT AND COMMERCE ON THE INTERNET

Good Morning. I'm delighted to be here with you. Including us is a sign that you are exploring all areas to develop a cogent, fair and cohesive approach to content on the Internet.

Today, the core of what I cover will be content on the Internet as it relates to children's advertising. Before doing so, however, let me put into perspective what we do as the only voluntary self-regulatory system for national advertising in the USA. A part of that perspective is the dynamic which makes the system effective.

Twenty-six years ago, the advertising industry and the Council of Better Business Bureaus forged a strategic alliance to protect the consumer, aid advertisers and maintain a competitive marketplace. It was named the National Advertising Review Council. The National Advertising Review Council is a guardian of, and a catalyst for, trust in national advertising through voluntary self-regulation.

The system has three component parts. They are:

National Advertising Division (NAD)	its role is to foster truth and accuracy in national advertising aimed at consumers 12 years of age and older.
Children's Advertising Review Unit (CARU)	its role is to move beyond truth and accuracy to ensure adherence to its guidelines for advertising targeted at children, younger than 12 years old.
National Advertising Review Board (NARB)	its role is that of an "appellate court", should an advertiser/challenger disagree with a NAD or CARU decision.

The entire process is voluntary. The National Advertising Review Council and its action units have no sanction; however, advertisers who do not abide by NAD/CARU/NARB decisions are reported to the Federal Trade Commission, which has endorsed this process as "the most effective in American business." Fewer than 5 per cent of NAD cases are referred to government; or put in a more positive way, 95 per cent of national advertisers comply with our decisions.

Now, let's concentrate on the "Children's' Advertising Review Unit".

CARU, which is funded by the children's advertising industry, was established in 1974 to promote responsible children's advertising and respond to public concerns. When children's advertising is found to be inaccurate, misleading or otherwise inconsistent with CARU Guidelines, CARU seeks changes through the voluntary co-operation of advertisers. CARU, with its Advisory Board of distinguished experts on child development and communications, and leaders of industry, have developed guidelines to address

issues ranging from clear product presentation and accurate claims, to the more subjective areas of undue sales pressure and appropriate pro-social role models. CARU's function at its most basic is to ensure that advertising to children is truthful, accurate and sensitive to the particular nature of its audience.

In 1991, we initiated a new informal procedure which is predicated on prompt responses and resolution. When a commercial raises questions for CARU, it requests product and advertising samples from the advertiser. If they receive a response within five business days, and the advertising either complies fully with the Guidelines or is capable of being modified within five additional days, no formal case is opened. The results, however, are reported in the Activity Report section of our Case Reports. Of course, if there is no prompt response, or no resolution can be quickly reached, CARU will open a formal case with the same opportunity for NARB appeal or government referral. It is worth noting that in CARU's entire history there have been four referrals, one to the FCC and three to the FTC, and no appeals. Over the years advertisers and their agencies have come to understand what CARU's parameters are. We rarely see any problems in the areas of product presentation, method of operation, disclosures or balanced breakfast depictions any more. CARU, clearly, has raised the standards of ethical advertising behavior over two decades.

In spite of what government and consumer activists consider an impressive level of compliance, there are some remaining areas which continue to create real problems in children's advertising in the USA. These have to do with the most subjective of CARU's Guidelines and Principles; they center on what might be called "lifestyle" or "social" issues. Their very subjectivity makes them the most difficult to enforce; since the issues involved are a reflection of prevailing attitudes and mores, there's no reason to believe that they will disappear any time soon. I'd like to review with you through three CARU inquiries - two formal cases and one informal - which illustrate these issues.

McDonalds

This spot illustrates the flexibility of the Guidelines to evolve in their interpretation, and how in applying the guidelines, CARU can act with a high level of sensitivity to current attitudes required of advertisers.

The relevant Guideline reads, "Advertisers should not portray adults or children in unsafe situations, or in acts harmful to themselves or others." In the past, this Guideline has been applied to athletic activities requiring helmets or knee-pads, crossing streets against traffic, and the like. But now, things are different. Leaving kids unattended, where some clown can just walk into the yard and play fantasy games with the children is a quintessentially nineties unsafe situation. When CARU notified McDonalds of our concerns about the spot, they decided to modify it; the re-worked spot was on the air within eight days. Interestingly, during those few days, one of the networks received complaints from two organizations which deal with missing and abused children.

IronKids

This is the most clear cut of the three. Two of CARU's Self-Regulatory Guidelines for Children's Advertising which deal with sales pressure and product presentation respectively address advertising which portrays children in a negative fashion. The first provides, "...Advertisers should not convey the impression that possession of a product will result in more acceptance of a child by his or her peers. Conversely, it should not be implied that lack of a product will cause a child to be less accepted by his peers." The second provides, "The advertising presentation should not mislead children about benefits from use of the product. Such benefits may include, but are not limited to, the acquisition of...status [and] popularity...".

Additionally, one of CARU's underlying Principles refers to the potential of advertising to influence the behavior of young children. It states, "Advertisers are urged to capitalize on the potential of advertising to influence behavior by developing advertising that, wherever possible, addresses itself to positive and beneficial social behavior, such as friendship, kindness, honesty, justice, generosity and respect for others."

This was one of the few cases CARU has had which was initiated by a consumer complaint - a mother wrote in extremity upset because her young son, who's always loved wheat bread wouldn't eat it any more because he didn't want to be a "dork".

It seemed pretty clear to CARU that both the explicit and implied message of the commercial was in violation of the Principle just cited. Any kid who eats wheat bread is a "dork"; to be cool you've got to eat IronKids bread. The advertiser disagreed; it based its disagreement on what it considered the inappropriateness of CARU's staff relying on its judgement in such a subjective matter, and pointed out that the kind of insulting humor used in the spot was no different from what we'd see in network television shows every night. Since there is no way to "prove" or "substantiate" such a claim, we were left agreeing to disagree, but after more friendly persuasion, the advertiser agreed to modify the commercial.

Squish Bugs

The next two spots came up against the same Guidelines and Principle as the IronKids commercial.

CARU deemed the juxtaposition of the "nerdy" kids doing what they're supposed to in entomology class, and the "cool" kids terrorizing their sisters and fathers as at least an implication that you're not cool if you don't have Squish Bugs. The play patterns in both spots, reinforced by the voice-over didn't strike us as addressing itself to positive beneficial social behavior, such a friendship,... and respect for others.

The "Squish/Sticky" commercial raised a final serious concern for CARU. Another of CARU's Guidelines on Product Presentation states, "Products should be shown used in safe ways, in safe environments and in safe situations." In the section dealing with Safety, the Guidelines state, "Imitation, exploration and experimentation are important activities to children. They are attracted to commercials in general and may imitate product demonstrations and other demonstrations without regard to risk." And "Advertisers should not portray adults or children in unsafe situations or in acts harmful to themselves or others." The behavior of the boys shooting the toys at the girl' s and man's face, if imitated by a child, could cause injury.

Here again, as in the bread commercial, these were not issues that could be handled with proof or substantiation. The advertiser disagreed with our position, but it is a measure of how responsive and committed the children's industry is to self-regulation that the advertiser substantially modified the spots for future use on children's television.

What I've tried to illustrate for you is how the same basic set of Principles and Guidelines have remained applicable to a rapidly changing and growing children's marketplace. This adaptability is currently being put to the test on the Internet.

CARU and its Advisory Board recognized early on that the new electronic interactive media posed new and unique questions for the industry and our self-regulatory system. At out June 1996 Advisory meeting we set ourselves the initial task of learning as much as we could about the new media. We sorted out

where the Internet presented unique issues which weren't addressed by the existing Guidelines. This was complicated by the very complexity and newness of the emerging children's online marketplace - that newness which engendered a new kind of distrust on the part of parents who were themselves unfamiliar with the new technology. They were in fear of their own inability to control access to the Internet.

By the December 1996 Advisory meeting we had identified privacy as the most critical new issue for CARU. In the offline world, if a young child wants to fill out a form and send in a boxtop, or join a kids' club, chances are she'll ask Mom for a stamp, or Dad for a ride to the Mall, and the parent has the opportunity to say, "Wait a minute, honey, I don't think I want you sending, or joining, that." So in keeping with one of our guiding Principles which holds that advertisers should respect a parent's prime responsibility to provide guidance for the child, we didn't feel the need for advertising guidelines to intervene. But when a child is sitting in front of a screen with a mouse and a keyboard, and action is only a click away, the opportunity for parental mediation becomes remote.

At that point we had learned enough about the online environment to know that our knowledge was still woefully inadequate. CARU staff, its Advisors, and NARC partners solicited input from an array of experts beyond our core CARU supporters. These included advertisers, technology and privacy experts, trade associations, regulators and consumer and advocacy groups.

We were still involved in this process in the Spring of 1997, when the Center for Media Education issued its report on Websites for kids and, with the Consumer Federation of America, petitioned the FTC to regulate children's online content. While there were areas where we didn't agree with the report, our concerns over privacy and data collection from children were pretty much the same as theirs. But while the consumer activists called for the government to step in, we believed then, as we do now, that our existing self-regulatory system is the most appropriate and effective means of shaping online practices. We are convinced we can transfer what was effective in traditional media to the Internet.

The challenge has been to come up with a set of Guidelines substantive enough to provide real protection for children and their families, yet flexible enough to allow the medium to realize its full creative potential. Just as important, guidelines had to be drawn specifically enough to give real direction to those who would follow them, yet be broad enough to allow, and indeed encourage, technological and creative innovation. The revised Guidelines we published earlier this year meet these criteria. They set forth a threshold of protections for children which will grow and evolve as the Internet does.

In many cases, the existing Guidelines adequately addressed issues in the new media - with a minor adaptation of the language to clarify their applicability. The only areas which warranted completely new guidelines were data collection and online sales. The sales area was pretty straightforward - the goal was to ensure that the person responsible for the costs of any transaction, in this case the parent or guardian, was given the means to control the transaction.

Our challenge in the area of content was the potential blurring of the line between advertising content and informational or entertainment content online. This distinction has been fairly simple on television; we use what we call bumpers; we alert children that they're about to see advertising by saying something like "We'll be right back after these messages". But in a medium without borders or time, it becomes much more complicated.

Our first task was to identify just what we meant by "advertising" online. We rejected the idea that anything containing branded characters automatically constitutes advertising. Consistent with our guidelines for other media, where we drew the line around advertising online was where there was a

traditional product "sell". Thus, a section of the Kellogg site giving the history of Tony the Tiger or containing a coloring page of Toucan Sam would not be considered advertising. But Tony saying "Frosted Flakes taste great!" would be considered advertising as would an offer of a Tony the Tiger T-shirt. Needless to say, in the online media as in all others, host-selling is prohibited not just by CARU but by the Federal Commerce Commission, and Tony will not be permitted to be the pitch tiger for that Tony the Tiger T-shirt.

Once we defined what we meant by advertising, the rest was relatively easy. Our existing guidelines for character-driven print provided that advertising needs to be clearly labeled as such. By broadening the language we applied the same requirement online. Here again, the guideline is drawn so as to leave to the advertiser the responsibility and creative freedom to devise the means of meeting this goal.

The industry has responded with varying levels of creativity. Some, like the Galoob Toys Website, chose to label their whole sites as advertising.

Others have come up with special icons which show up whenever advertising content does. The Kidscom Company has its "AdBug" - when product information or advertising appears, the AdBug is there, and if you click on it, it takes to a message about advertising. Nabisco has its "AdBreak" which pops up with the message, "Hi Kids, when you see me ... it means you are viewing a commercial message designed to sell you something" And it goes on to say, "Remember, if you are under 18 years old you should have your parents' permission before you leave any information about yourself, or try to buy anything online."

Which brings me to the final focus of the guidelines, and the one which has been generating the greatest controversy lately:

Privacy

In the area of content involving data collection, the goal was to make sure that parents have notice, choice and control over what information is being collected from and about their children, and what's being done with that information. Our approach has always been to give guidance and set goals, but not to prescribe the means of meeting those goals. Consistent with that approach, the Guidelines call for advertisers to make "reasonable efforts" in light of the latest available technology, to ensure that a parent's permission is obtained. This leaves the advertiser with both the freedom and responsibility to figure out how to go about empowering the parent. It is in defining this reasonable efforts standard that we will be constantly raising the bar.

In the nine months since the Guidelines were revised, our approach of letting the industry itself find the solutions has been validated; advertisers and Website developers have come up with several innovative ways of meeting the need to provide parents with the means of exercising choice and control. Last summer, after participating in and hearing the concerns expressed at the FTC Workshop on Consumer Privacy, and seeing what was available and feasible, we began to sharpen our definition of reasonable efforts depending on the type and sensitivity of the information collected. Here's our current definition:

* In all cases, the information collection or tracking practices must be clearly disclosed, along with the means of correcting or removing the information. The disclosure notice should be prominent and readily accessible before any information is collected. For instance, in the case of passive tracking, the notice should be on the page where the child enters the site.

* For real world, personally identifiable information, which would enable the recipient to directly contact the child offline, the company must obtain prior parental consent, regardless of the intended use.

* When personally identifiable information (such as email addresses, screen names) will be publicly posted so as to enable others to communicate directly with the child online, or shared with third parties, the company must obtain prior parental consent.

* For other identifiable information, such as email addresses (which won't be posted), first names, hometowns, the company must directly notify the parent of the nature and intended uses and offer the opportunity to remove or correct the information.

* For all other anonymous or aggregate information, whether gathered directly or through passive means, the company must clearly disclose the nature and intended uses of the information.

These guidelines are now being implemented on numerous sites, Kidscom, Kelloggs, Disney, Microsoft Kids, Avery, Mattel, Colgate Kids to name a few.

We have in place a set of Guidelines which provide guidance to the industry and protection to children and their parents. We have in place a remarkably effective self-regulatory system to oversee and enforce the implementation of those Guidelines. And we have before us one great opportunity to see to it that we as an industry live by those Guidelines, and to get and keep our own house in order on the Internet as we have done in traditional media for over 20 years.

For now, both the White House and the Federal Trade Commission have indicated a preference for letting industry take the lead in setting and enforcing the parameters of acceptable behavior online. But we have to do it right and we have to do it fast. At forum after forum, whether it be from Ira Magaziner, President Clinton's Strategic Policy Planner; Chairman Pitofsky of the Federal Trade Commission, or industry or privacy experts, the message I hear loud and clear is that children's protection is the "wedge issue". No matter how well industry handles the pressing privacy concerns of the general public, if we don't get the children's component of it right, the Internet will be regulated by the government.

For a moment let me move away from children on the Internet to business practices on the Internet.

Another tool we, at the CBBB, Inc. have introduced for the Internet, is named BBB On Line. It deals with ethical business practices. Companies who meet six qualifications can display a seal on their Website. Next to the seal is an instruction: click to check. When the Internet user clicks, he/she will learn if the seal is authentic and, with one more click, the user can read the six standards that company has met in order to qualify for BBB On Line. Over 1 000 companies have already signed up to use the BBB On Line seal as a sign that they are ethical businesses. This evening I shall be in the demonstration area, if you'd like to stop by and talk about BBB On Line, or any other areas where we are involved in self-regulation. They are:

- become a member of the appropriate local Better Business Bureau;

- provide the BBB with information regarding company ownership and management and the street address and telephone number at which they do business, which will be verified by the BBB in a visit to the company's physical premises;

- be in business a minimum of one year (with limited exceptions);

* have a satisfactory complaint handling record with the BBB;

* agree to participate in advertising's self-regulation program; to correct or withdraw online advertising determined to be unsubstantiated or not in compliance with CARU's advertising guidelines;

* respond promptly to all consumer complaints;

* agree to binding arbitration, at the consumer's request, for unresolved disputes involving consumer products or services advertised or promoted online;

* before concluding, let me address one of the questions asked in the title of this section of the conference: why has self-regulation been effective?

For us, the answer is one word, one concept. Ownership.

In the USA, the advertising industry believes - intellectually and emotionally - that the system of voluntary self-regulation is theirs. Advertising started it 27 years ago. The ANA took the lead. It created a practitioner based, user-friendly system. It is more than a consumer re-dress mechanism. It is distinguished from other societal controls by its true purpose: to promote higher standards of ethical behavior on an industry wide basis.

Has it worked? Five sources of evidence suggest yes:

- Advertising investment is accelerating at a faster rate than the economy in the USA.
- New companies/industries are using advertising to build their business.
- There is a 95 per cent compliance rate among national advertisers.
- Consumer complaints have shown a significant decline: to less than 5 per cent of case work.
- Robert Pitofsky, Chair of the FTC has said, "I recognize that advertising today is more truthful and more informative than was the case twenty five years ago. It (advertising) has the best self-regulatory device in American industry."

Now returning to Children, Content and Commerce on the Internet, I'd like to highlight certain critical issues. I believe private industry has the will power and ability to self-regulate advertising on the Internet. I'm convinced that private industry will be driven by enlightened self-interest; that dual dimension will create trust and confidence among consumers as they do business on the Internet. We can provide guidelines to advertisers for use as navigational aides in the creation and placement of Websites and advertising. We can develop tools for consumers to use to protect themselves from those few who will be unscrupulous in their use of the Internet. We can introduce seals of approval to protect parents and children. And we can make self-regulation effective through an enforcement consequence:

1. companies must pre-qualify for a seal
2. periodic audits: self, competitor, and the self-regulatory system itself
3. when out of compliance,
   * remove the seal from offender's Website
   * publicize the infraction and the reason action was taken
   * refer to the appropriate government body.

We can do all this. But, time is running out. If we do not act decisively and immediately, we will forfeit much of the freedom private enterprise needs to develop the Internet's full commercial potential. When confronting the issues of responsibility and timeliness at a critical time for his country, a wise man once asked: "If not us, whom? If not now, when?"

So, to my colleagues here in the private sector, I ask; If not us, whom? If not now, when?

Panel No. 2: What are key industry codes of conduct and corporate practices and why do they work?

Kazuko Otani
Telecom Services Association (TELESA)

For Sound Development of Internet Services
Guidelines for codes of practices for Internet Service Providers

Slide One
What is TELESA ?

- The Sole Association of TYPE II Telecommunications Business Providers in Japan
- Members as of January 1998: 403 companies

Slide Two
Activities (JUN 1996-FEB 1998) of Internet Service Providers' Ethics Committee

Slide Three
Background of our Guidelines
Widespread Use of the Internet in Japan
Increase of -

- Social problems (diffusion of harmful content for children, etc.)
- Crime using Internet
- Disputes (copyright infringement, defamatory statements on BBS, etc.)

Promotion of Self-regulation Framework

Slide Four
Increasing ISPs
[chart]

Slide Five
Increasing Internet Crimes
[chart]

Slide Six
Increasing disputes and lawsuits
Tokyo District Court May 26, 1997

- sysop's liability
- online service provider's liability

Slide Seven
Trend of Self-regulation

Slide Eight
Chapter 1: Purposes

- To protect Users by responding appropriately to various problems arising from providing telecommunications services

- Internet Connection Services etc. will make sound growth

Slide Nine
Chapter 1: Four Principles

- Principle 1 - the freedom of expression of the sender should be respected
- Principle 2 - the principle that the sender should have self-responsibility for the contents should be given priority
- Principle 3 - the secrecy of communications and personal data should be protected
- Principle 4 - consideration should be given to the sound growth of minors

Slide Ten
Scope of the Guidelines
Communication open to the public

Slide Eleven
Chapter 2: Protection of Users
Protecting Personal Data and Privacy

Slide Twelve
Chapter 2: Protection of Users
Selection of information received
ISPs should make efforts:
- to build a system which protects minors from information which

- hampers their sound growth
- allows guardians to select information which they feel inappropriate for minors

- to enable users to install technological measures to select information they receive, such as rating and filtering software

Slide Thirteen
Conditions to be Specified in Chapter 3: Agreements with Users
ISPs should specify in Agreements with Users:

- that Users should not deliver nuisance communication and disguised communication
- that Users should not dispatch illegal or harmful communication
- measures ISPs can take when they become aware of Users' violations

Slide Fourteen
Chapter 4: Contents of Measures by ISPs

- Request the sender to stop the violation
- Prevent users from receiving illegal or harmful information, nuisance communication or disguising communication
- Terminate use by the sender or cancel Agreements with users
- If ISPs can specify the sender...when ISPs know the violation of their user...ISPs can take such technological measures

Slide Fifteen
Chapter 4: Contents of Measures by ISPs
When ISPs takes measures mentioned in this Chapter, ISPs should take into consideration the following items:

- Secrecy of Communication
- Take proportional measures
- Co-operation with other ISPs

Slide Sixteen
Chapter 5: Responding to Complaints

- Clarification of Section to Deal with Complaints
- Confirmation of the Contents of Complaints
- Encouraging resolution by themselves
- Collection of Cases

Slide Seventeen
Chapter 6: Response to Various Kinds of Reference
Response to forced investigation
To confirm the confiscation list and warrant issued by court
Response to voluntary investigation and other reference
Not to disclose the information classified in the secrecy of communication
Response to various inquiries
To identify the inquirer as the user

Slide Eighteen
Chapter 7: International Co-operation
Taking into consideration the fact that the Internet is spreading information on a global scale, we will deal with Illegal or Harmful Information and Nuisance or Disguised Communication in co-operation with ISPs organization in the other countries.

Slide Nineteen
Tasks to be performed:

- To prepare help desk manual which carries collected cases to deal with various complaints concerning illegal or harmful information
- To draft a Model Agreement for Internet Connection Services
- To encourage members and other ISPs to comply with the Guidelines

References

- Guideline for Codes of Practice for Internet Service Providers (February 1998) (TELESA, Japan): *http://www.telesa.or.jp/e_guide/e_guid01.html*
- The Rules for the Flow of Information on the Internet (December 1997), Report of the Study Group on the Rules for the Flow of Information in the Telecommunication Services - Ministry of Posts and Telecommunications (MPT), Japan): *http://www.mpt.go.jp/policyreports/english/group/telecommunications/index-e.html*

Panel No. 2: What are key industry codes of conduct and corporate practices and why do they work?

Margo Langford
Canadian Association of Internet Providers (CAIP)

Industry Codes of Conduct The "Reality Check"

Slide One
Potential Liabilities - ISPs or Web Owners

- defamation
- obscenity
- child pornography
- consumer protection
- content quotas
- privacy
- data protection
- intellectual property

Slide Two
Who has "control" over the technology?
Laws need to address Internet actors by their functions:

- packet carriers: NAPs, NSPs, ISPs
- client side: software, systems administrators & operators, users
- server side: Webmaster, Website host, Website owner, content provider, navigation assistance, content editor or content aggregator

Slide Three
What an ISP controls:

- can block IP addresses (Web sites, newsgroups, users)
- can choose not to host or distribute certain illegal content
- ISP contracts with users and Web owners generally allocate liability
- should also specify both the jurisdiction for interpreting laws and the venue for bringing lawsuits

Slide Four
What User Can Do:

- can limit the applicable territory on the Website (but different risks between passive & active business)
- can install content controls (software that filters or selects from categories)
- can call hotlines, or register complaints with ISPs
- can encourage rating systems
- can employ privacy techniques

Slide Five
What's REALLY happening:

- low level of awareness of Code of Conduct by public or ISPs (introduced 18 months ago with publicity, none since)
- very few complaints to ISPs, and CAIP
- no uniformity of response
- continuous media coverage of the "ills" of the Net (arrests of pedophiles etc.)

Slide Six
Case Study
Facts:

- user put unauthorized, unreleased Van Halen recording belonging to Warner Music (USA) at: *members.octonline.com/DERBY/WOY*
- music industry anti-piracy group IFPI internationally now employs a Web "crawler" to look for music files

Slide Seven
Case Study (cont'd)
Process:

- USA anti-piracy body (RIAA) found the infringing content on the Web site
- RIAA searched Internic records to discover the billing address for Domain Name "octonline" (this was iSTAR Internet in Canada)
- RIAA directed the Canadian office CRIA to contact iSTAR, demand letter sent

Slide Eight
Case Study (cont'd)
Response:

- iSTAR called and discussed: "O" is a local ISP that buys a dedicated connection from iSTAR. Contract states: "*the customer is responsible for the content hosted on their services"*
- "O" hosted alleged illegal customer subject matter on Web site hosted on "O" premises - no control by iSTAR

Slide Nine
Case Study (cont'd)

- iSTAR gave CRIA the "O" contact details (was this a violation of customer privacy?)
- "O" was a marginal ISP about to go out of business, hadn't paid iSTAR
- did ask user to remove the Van Halen recording
- recording was removed, CRIA will not say if a suit is to follow against any of the parties

Slide Ten

Improving Response

- Web site domain yellow pages directory with site owners/addresses listed?
- Education of User groups about infringement
- Education of creators about enforcement
- Procedure and tools provided to ISP to more effectively respond

Panel No. 2: What are key industry codes of conduct and corporate practices and why do they work?

Professor Michel Vivant
University of Montpellier

CODES OF CONDUCT: FRENCH INITIATIVES

It will be remembered that the proposal that the OECD should concern itself with the question of self-regulation was first made by France.

A substantial body of work

France has indeed done a great deal of work in this area, to the point that it can on occasion look somewhat disorganised. A better term would be prolific. There have been numerous and varied initiatives, stemming from different sources and having different objectives.

To begin with, mention should be made of the first *"Charte de l'Internet"* (Internet charter) document presented in March 1997 by Mr. Beaussant, who had been given this task by the then Minister for Telecommunications, Mr. Fillon. The aim of the document was an ambitious one: "*To promote the harmonious development of the Internet,... lay down rules and practices, within the framework of laws and treaties, and facilitate their implementation by means of a simple and pragmatic tool for self-regulation: the "Conseil de l'Internet*" (Internet Council).

With the failure to achieve unanimity on this question, the *"Commission juridique"* (legal committee) I chaired moved, during the summer of 1997, towards drawing up a manifesto incorporating the major principles on which net users had to agree. As far as the preparation of the said manifesto was concerned, the French chapter of 'Internet Society', by Mr. Oudet and Mr. Kahn, acted as a driving force.

User associations launched their own projects.

Other initiatives were less "globalising" and more professional: professional codes of ethics, corresponding to a given activity, rather than users' charters. Thus, there was the code of ethics of the GFII *(Groupement des Fournisseurs d'Information en Ligne,* or on-line information suppliers' group), which is built around a system of labelling and professional discipline. The AFA *(Association des fournisseurs d'accès,* or association of access providers) has also conducted its own studies.

Following on from the above, a Commission headed by Mrs. Falque-Pierrotin (author of a celebrated report on the Internet in 1996) is at present responsible for producing some in-depth thinking about what form an Internet regulation adapted to the specific nature of the network might take.

The quest for a "soft law" to supplement the "hard law"

In all of these cases, and doubtless more in the case of "globalising" initiatives, the decision has been taken to look for a "soft law" to supplement the "hard law". This is a law which, by its very nature, would have the advantage of being not only national, but of being able quite naturally to acquire an international dimension. It has to be accepted as fairly indisputable that the problems posed by the Internet are the same in Paris, Washington and Tokyo, so it is natural to assume that, cultural differences and differences in legal traditions apart, the answers will be, if not the same, then at least similar.

Since the word "self-regulation" has sometimes been a source of concern, it should be added that it is obviously not a question of getting round vital, basic rules. It is a matter of fitting practical standards into the minute opening left by binding legislation (to repeat an expression I have already used).

1. From the content point of view, this means that the quest for 'soft legislation' has to be and is seen as a quest for a law that is appropriate (deriving from reality) and "flexible" (flexible law).

Two examples will serve to illustrate this point.

The first has to do with the law of civil liability. An individual's responsibility is gauged in French law by reference to an abstract reference individual: the "good father"(or "reasonable person" in Quebec law). But nobody knows in principle what the good father (or reasonable person) is on the network. Taking a reasonable, received practice may be the way to bring this sort of standard to light.

A second example may be found in the field of international law. In a number of European conventions, it is the law (Rome Convention) or judge (Brussels and Lugano Conventions) of the consumer's own country which applies in certain circumstances, and especially when the supply was preceded by advertising specifically targeting that consumer. However, the lack of differentiation between messages on the networks means that it is not always possible to identify what is strictly advertising. A reference to professional standards based on practice and identifying the advertising message may provide the judge with a strong indication.

Law which is flexible, therefore, realistic and not dogmatic, but nevertheless law.

2. From the practical point of view, i.e. the practice to be adopted in order to give actual form to self-regulation, it may be deduced from what has been said above that there can be no question of drawing up a sort of rigid legal monument.

As conceived, self-regulation implies information, training and exchanges of views: information about problems, challenges and the solutions that might be found; information for the users involved and the authorities, training for these users and for the public; exchanges - especially between national regulatory authorities, etc.

The idea now taking shape is that hot lines should be set up which can deal with the problems encountered by network users quickly and flexibly and which are based on gradually emerging practices.

There is obviously no question at this stage of revealing the conclusions that will be arrived at by the working party headed by Mrs. Falque-Pierrotin. That will happen this summer. It can at least be said, however, that , in addition to the setting up of hot lines, there will probably be a recommendation to create an advisory, private law body bringing together representatives of Internet users and qualified individuals. The purpose of such a body could be to advise users on correct practices, but in no circumstances would it be able to enforce its recommendations.

The choice is certainly to introduce a soft law which is in line with the "received" law but is adapted to the reality of the Internet.

Panel No. 3: User empowerment technologies and why do they work?

Marilyn Cade
AT&T, USA

MATERIALS UNAVAILABLE

Panel No. 3: User empowerment technologies and why do they work?

Akio Kokubu
Electronic Network Consortium

Slide One
What is the ENC ?

- A trade organization for major online service providers in Japan
- To solve problems which providers encounter when they operate services

Slide Two
Work Items

- Ethical guidelines for running services
- Recommended etiquette for users
- Guidelines for protecting personal data
- Operation of an electronic authentication system
- Operation of a label bureau

Slide Three
The Internet and Law in Japan

- Secrecy of communications and no censorship
- The constitution and the telecommunication business law
- When inadequate materials are posted on Web pages by users
- Primarily user's responsibility
- Provider's responsibility ?

Slide Four
Protection of Human Rights

- Murder case by a boy in Kobe-city
- The great impact on the Japanese society because of the cruelty
- Freedom of reports or human rights
- Most providers deleted users' contents which included his name and photos
- Cannot control contents from foreign sites

Slide Five
Control of Pornography

- Hardcore pornography is illegal
- Illegal contents from foreign sites
- Pornographic materials inadequate for children are sold all over Japan
- Regulated by bylaw of local governments
- Child pornography
- Seen as a kind of pornography

- Violation of the child welfare act

Slide Six
No Censorship and Self-Regulation

- Enlightenment with guidelines
- Ethical guideline for running services
- Recommended etiquette for users
- Provision and dissemination of filtering capabilities
- Development of filtering software
- Operation of a label bureau

Slide Seven
Filtering Software

- PICS compliant
- Works with Netscape 3.0 and IE 3.0
- Rating by teachers and parents
- Besides third-party-rating and self-rating
- Free software for Windows 95 and Macintosh
- As an infrastructure for the Safety Internet
- More than 20 000 users downloaded

Slide Eight
Label Bureau

- Label bureau functions
- Co-operation with search engines
- Rating system
- Extension of RSACi
- Label database
- 13 000 pages in Japanese were rated
- Database update
- Daily work

Slide Nine
Further Works

- Co-operation with the "one-hundred-school networking project”
- Creation of multiple rating systems and multiple label bureaus
- Co-operation with international standardization work

Panel No. 3: User empowerment technologies and why do they work?

Don S. Sandford
NetShepherd, Inc.

Slide One

Objective: outlining the basic principles Net Shepherd believes Internet Filtering companies should consider in designing products and services.

Net Shepherd firmly believes in providing tools and services that empower users to self-regulate Internet use.

In the following presentation I will provide insight into the challenges Net Shepherd has experienced and the actions we took, and continue to take, to uphold the principles we believe all Internet filtering companies should support in their products and services.

Slide Two

Principle one: ***empowering the user with total control***

Design filtering products and services that enable the user to set the degree of filtering. All filters should be set to 'no filtering' as the default. Controls must be very user friendly and easily accessible to accommodate all levels of users.

Principle two: ***freedom of choice***

Users of the technology must be given a range of filtering options to choose from (ie. multiple databases). First, second and third-party ratings must all be available and the user should have the choice to select the most appropriate database for their own filtering needs. Filtering should not be legislated. Community-based databases offer the greatest opportunity for multiple perspective representation on the Internet. Databases can be directed by communities of interest such as: demographic, vertical market, cultural, language, etc. ***Choice creates an alternative to censorship***.

Principle three: ***diversity***

Government should encourage industry to develop as many filtering solutions as possible. (AT&T study authored by Ms. Laurie Craner and Dr Paul Resnick covers a range of technology options on the market.)

Principle four: ***intelligence***

Characterization of Internet Content, by end users of the Internet is superior to key word blocking. Machine indexing of Content currently exists but is incapable of providing the contextual Content information end-user communities can deliver. The combination of Machine Indexing and Contextual Characterization using a virtual rating community is very powerful. 'Controversial content guidelines' together with the ability to evaluate content in real-time through leveraging aggregates of people (i.e. communities and technology) allows for the reflection of local community standards.

Principle five: ***Guidance***

Solutions must be designed that enable a filter to act both as a *screen* and a *lens for focusing*. Net Shepherd believes 'positive guidance' will win out over 'blocking access to inappropriate content' as the greatest driver of new Internet users.

Slide Three

Principle six: ***disclosure*.**

Every company must employ a clear and visible disclosure of information so users can make informed decisions regarding the use of that service (e.g. provide information regarding rating criteria, selection of raters, processes, etc.).

Principle seven: ***privacy*.**

Users must be made aware of the use of cookies, information obtained at registration, collection and use of footprints, etc.

Principle eight: ***liability*.**

Placing the user in control, using third-party ratings and rating Internet content according to opinion will all impact the potential liability of various parties.

Principle nine: ***co-operation*.**

The Internet Industry as a whole should understand the laws pertaining to illegal Internet content and the trafficking of illegal content. The industry should co-operate with law enforcement agencies within the context of the law.

Principle ten: ***standards*.**

Standards are required to advance the use, economic development, and adoption of Internet technology. Net Shepherd firmly supports the PICS label bureau standard (Platform for Internet Content Selection).

Slide Four

At Net Shepherd we have used the above principles to create competitive advantage. Net Shepherd was the first company to rate the Internet using a third-party virtual community. (e.g. +500 000 Web site ratings = millions of URL's provided by the World's largest rating community).

In Partnership with Digital Equipment Corporation's, AltaVista Search Group, Net Shepherd has firmly taken Internet filtering technology to the next level with the invention of Intelligent Filtered Browsing and Intelligent Filtered Search. Net Shepherd has been nominated for a ComputerWorld Smithsonian Award for its groundbreaking technology. Net Shepherd has also been inducted into the Smithsonian's Permanent Research Collection and Archival Museum. With AltaVista we have identified that the demand and future potential for filtering technology is in relevant information retrieval (positive guidance), not just screening of inappropriate content.

The true filtering business opportunity lies in aggregating Internet Content, not providing protection software. It has been clearly demonstrated that people will always prefer choice over censorship and therefore special consideration must be given to: privacy, security and disclosure policies relating to the Internet.

Panel No. 3: User empowerment technologies and why do they work?

Gordon Ross
Netnanny Ltd (USA)

Filtering Tools & Solutions

Slide One

- Filtering.
- Rating Systems.
- Access Control.

Slide Two

Filtering History

- January 1995 PC's.
- May 1995 MAC's.
- 1996 - Other Platforms.
- 1997 - Over 20 Companies Involved.

Slide Three

Filtering … User "EMPOWERMENT"

- Should We Monitor?
- What is accessed?
- Who is Accessing Data?
- Should We have Wide Open Access?
- Who should have unlimited access?
- What should be accessed?

Slide Four

Filtering Methods.

- A Standard - Platform For Internet Content Selection. (PICS) Early 1996.
- Self - Rating Systems.
- Site Address Lists.
- Words & Phrases.

Slide Five

Filtering at "ISP"

- Under ISP Control.
- User is not fully "Empowered".
- Owner sets "their" own rules as set out by the ISP.
- Liability Is with the ISP.
- User Relies on Others.

- What happens when child jumps to another system?

Slide Six
Filtering at the "PC"

- Under User Control.
- User is "Empowered".
- Owner sets "their" own rules.
- Liability Is with the Owner.
- Does not need to Rely on Others.

Slide Seven
Blocking & Filtering Today is...

- Flexible.
- Allows for Custom Controls.
- Audit Trails.
- Block or Allow Lists.
- Can be done at the Terminal or Server.

Slide Eight
Blocking & Filtering.

- 2-Way Communication Blocking.
- Incoming Data.
- Outgoing Data.
- Applications (Word, Write, etc.).
- Operating Systems (Files, Drives, etc.).

Slide Nine
Concerns
Education.

- Lack of Understanding of the Internet.
- Policy Makers.
- Law Enforcement.
- Educators.
- Parents and Children.
- The Internet is a Great Resource.
- Open Global Communication for all Countries.

Slide Ten
LEGISLATION.

- A country's law is only applicable to its own citizens.
- Internet has NO boundaries.

- Law enforcement funding.
- Educational funding.

Slide Eleven
LAW ENFORCEMENT.

- Need Funding for Training.
- Need Additional Resources.
- Focus more and more on Cyber Crime.
- Need Community Involvement.

Slide Twelve
EDUCATION.

- Educate Policy Makers.
- Educate Teachers.
- Educate the “Lost Generation”.

Slide Thirteen
ACCESS

- Individual ID’s.
- Passwords.
- Smart Cards.
- PINs. (Personal Identification Number.)
- Biometrics.

Slide Fourteen
Summary.

- Technology IS available today.
- Cost of Technology is Dropping.
- Hardware & Software Solutions.
- Security is Dependent on PEOPLE.

Slide Fifteen
Contacting Us:

World Wide Web: http//:www.netnanny.com

Email: netnanny@netnanny.com

Telephone: (425) 688-3008 or (604)662-8522

Panel No. 3: User empowerment technologies and why do they work?

Susan Getgood
The Learning Company, Inc.

The Learning Company was honored to be invited to represent the filtering industry and demonstrate our Internet filtering software Cyber Patrol at the OECD's Educational Forum on Internet content and the role of regulation. We were asked to demonstrate the Cyber Patrol filtering software, provide some background on our experiences with self-regulation and the content debate in the United States, and discuss how filtering software and self-regulation might apply to the questions being addressed by the OECD.

It has been our experience that Internet filtering technology provides users with the ability to more effectively manage the content children may access over the global Internet than the various national laws proposed to-date.

Cyber Patrol is based on a foundation of choice and user empowerment. It is an excellent option for parents, teachers and others who wish to protect children from inappropriate Internet content. In the US Supreme Court's decision on the Communications Decency Act, Cyber Patrol was cited by the court as a way of protecting children that did not infringe on Americans' right of free speech. Since the court's decision, the software has grown in popularity and sophistication.

Cyber Patrol allows parents to tailor access to the Internet to each individual child according to age and maturity. The software filters Internet content based on a proprietary list of sites compiled over more than two years by a team of teachers and parents who have researched more than 5 million sites on the World Wide Web. This list, called the CyberNOT list (*see below*), contains more than 60 000 sites deemed inappropriate because of nudity, violence, hate speech, graphic and shocking images, and material that encourages the inappropriate use of drugs and alcohol. Cyber Patrol software also contains a list of kid-friendly sites that parents can use for younger children as a restricted "cyber playground." This educational and entertaining sites are known as the CyberYES list. The lists are constantly updated.

Parents can add or delete individual sites to customize the list to a family's own values and beliefs. Parents also can choose to filter using a system known as PICS. PICS systems in use today include rating systems that support self-labelling by Web site owners and independent, third-party labelling bureaus.

The Cyber Patrol software does more than simply control access to the Web. Families can control the amount of time each week children spend surfing the Net and select which hours each day a child is allowed online. Parents can control participation in chat rooms, while a feature called ChatGard allows families to protect their children from inadvertently divulging personal information to strangers online.

Cyber Patrol is the most international of the leading US filtering software products. It is available in multiple languages and can be downloaded over the Internet from anywhere in the world. This year, The Learning Company will introduce localized, retail versions of the Cyber Patrol software in France, the Netherlands and the United Kingdom, with Spanish and German language retail versions to follow. A Japanese language version is already available through a distributor in Japan. In addition, Cyber Patrol is available in French and German to European subscribers accessing the Internet over CompuServe, and is offered by a growing number of telecommunications companies that provide Internet access.

In addition to being the filtering software most widely-used by families and schools wishing to manage children's access to the Internet, a growing number of businesses throughout Europe are using network versions of Cyber Patrol to manage employee access to the Internet.

In the United States, Cyber Patrol is the parental control technology offered by America Online, CompuServe, Prodigy, AT&T, Ameritech, GTE and dozens of individual Internet Service Providers.

More information about Cyber Patrol Internet filtering software and a 7-day trial version can be obtained at the Web site: www.cyberpatrol.com. Route 6-16, The Learning Company's fun and educational site for kids, can be found at www.cyberpatrol.com/616.

Cyber Patrol CyberNOT List Criteria

The CyberNOT criteria pertain to advocacy information: how to obtain inappropriate materials and or how to build, grow or use said materials. The categories do not pertain to sites containing opinion or educational material, such as the historical use of marijuana or the political situation in Germany during the 1930s and subsequent World War II.

Microsystems Software, Inc., a subsidiary of The Learning Company, Inc., has used what we believe to be reasonable means to identify and categorize CyberNOTs, but we cannot guarantee the accuracy or completeness of our screens and we assume no responsibility for errors or omissions. Please report errors and omissions using the Site Investigation Report.

Category Definitions, 11/5/97

Violence/Profanity:
Pictures or text exposing extreme cruelty, physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Obscene words, phrases, and profanity defined as text that uses, but is not limited to, George Carlin's 7 censored words more often than once every 50 messages (Newsgroups) or once a page (Web sites).

Partial Nudity:
Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia. The Partial Nudity category does not include swimsuits (including thongs).

Full Nudity:
Pictures exposing any or all portions of the human genitalia.

Please note: The Partial Nudity and Full Nudity categories do not include sites containing nudity or partial nudity of a wholesome or non-prurient nature. For example: Web sites for publications such as National Geographic or Smithsonian Magazine or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

Sexual Acts:
Pictures or text exposing anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior, including masturbation, copulation, pedophilia, intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, adult personal ads, CD-ROM's and videos.

Gross Depictions:
Pictures or descriptive text of anyone or anything which are crudely vulgar or grossly deficient in civility or behavior or which show scatological impropriety. Includes such depictions as maiming, bloody figures, autopsy photos or indecent depiction of bodily functions.

Intolerance:
Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Satanic or Cult:
Satanic material is defined as: Pictures or text advocating devil worship, an affinity for evil, or wickedness. A cult is defined as: A closed society, often headed by a single individual, where loyalty is demanded, leaving may be punishable, and in some instances, harm to self or others is advocated. Common elements may include: encouragement to join, recruiting promises, and influences that tend to compromise the personal exercise of free will and critical thinking.

Drugs/Drug Culture:
Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This category does not include material about the use of illegal drugs when they are legally prescribed for medicinal purposes (e.g., drugs used to treat glaucoma or cancer).

Militant/Extremist:
Pictures or text advocating extremely aggressive and combative behaviors, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes "how to" information on weapons making, ammunition making or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.

Sex Education:
Pictures or text advocating the proper use of contraceptives. This topic would include condom use, the correct way to wear a condom and how to put a condom in place. Also included are sites relating to discussion about the use of the Pill, IUD's and other types of contraceptives. In addition to the above, this category will include discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries. The Sex Education category is uniquely assigned; sites classified as Sex Education are not classified in any other category. This permits the user to block or allow the Sex Education category as appropriate, for example, allow the material for an older child while restricting it for a younger child.

Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Sex Acts category.

Questionable/Illegal & Gambling:
Pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission) and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting, including non-monetary dares and "1-900" type numbers.

Alcohol & Tobacco:
Pictures or text advocating the sale, consumption, or production of alcoholic beverages or tobacco products, including commercial sites in which alcohol or tobacco products are the primary focus. Pub and restaurant sites featuring social or culinary emphasis, where alcohol consumption is incidental are not in this category.

Note: Web sites which post "Adult Only" warning banners advising that minors are not allowed to access material on the site are automatically added to the CyberNOT list in their appropriate category.

Panel No. 4: Government and private sector roles in self-regulation: what are the conditions for successful self-regulation?

Markku Roppenen
Finnish Internet Service Providers Association

I will briefly present as a basis for discussion the view of the Finnish Internet Service Providers' Association (ISPA Finland) on the responsibility of different actors involved in the information chains of Internet for illegal and harmful content, grounds for self-regulation, as well as the impact of this view on self-regulation.

ISPA Finland is a trade association launched in December 1997 for the purpose of promoting the co-operation of its members in the field of legal issues, including issues relating to industry self-regulation.

RESPONSIBILITY FOR CONTENT

The major Finnish Internet operators participated in a joint project organised in 1997 under the "Tiveke Program" of the Finnish Ministry of Transport and Communications, which aimed to identify and define the different actors intervening in the information chain between the information provider and the end users, as well as their rights and responsibilities for the contents published in Internet.

ISPA Finland promotes the results of the project and has adopted them as ISPA Finland's view on horizontal liability and self-regulation.

Accordingly, ISPA Finland proposes that for the purpose of regulation, public network communication is to be divided into two distinct categories, namely '*public personal communication'* (such as news services and network meetings) and '*content distribution'* (including audio-on-demand, video-on-demand etc).

Liability for the content of the various actors under Finnish law is based on the actor's actual knowledge of the content and therefore the actors' positions vary according to their respective roles in the information chain. The responsibility lies with parties such as:

- users in public personal communication (on basis of creation and sending of messages);
- supervisors of public personal communication (in supervised news services or network meetings on basis of choosing/approving of the messages);
- content producers; and
- final service providers (the actors providing the user with the end service /content);
- (users).

Actors not liable for the content include technical carriers i.e. actors who have neither created the content nor decided on its delivery or publication, such as:

- data transmission service providers;
- access providers etc; and
- host-service providers (Web-hosting services).

GROUNDS FOR SELF-REGULATION

The general idea behind the widely discussed industry self-regulation, is that Internet industry would be able to restrict the distribution of harmful and criminal materials within the network.

Even if this were technically feasible, there must be a discussion on what kind of measures are allowed by the existing legal framework. A general misconception is that even far-reaching self-regulatory measures could be used by actors such as access providers against third parties. This is not, however, the case in respect of most of the measures. For instance, blocking is a measure which is allowed for the actors who, in their normal course of business, choose the material which is delivered to the users or placed in the network for the users to access, but generally not allowed for technical carriers such as Internet operators.

IMPACT

I believe that all Internet service providers are willing to participate in regulating the distribution of illegal and harmful content in the Internet. Industry self-regulation should, however, be organised at different levels taking into account the different roles of various actors in the information chain.

Content providers, final service providers and users, i.e. the parties having the right to choose the distributed and received contents, have a key role in respect of any successful self-regulatory action. Participation of technical carriers especially by restrictive or “take-down” measures however, requires the creation of a legal framework.

Panel No. 4: Government and private sector roles in self-regulation: what are the conditions for successful self-regulation?

Dr. Fred EISNER
Association of Dutch Internet Service Providers

Internet Content self-regulation: The Dutch experience

I'd like to share with you our experiences in The Netherlands concerning combating illegal content on the Internet, especially and very specifically child pornography.

I'll focus on some of the parameters and pitfalls that influence success or failure . .

First I have to state that I am not (NOT) representing the Information industry, but the ISP-industry! Why is that important? ISP's are not responsible for third-party content, so for self-regulation in regard to illegal and harmful content to work governments will have to address the proper industry, being the information (and amusement) industry.

ISP's have one major task/responsibility that supersedes all others, and is also the condition *sine qua non* for the Internet, and that is: to expedite and maintain an orderly flow of IP-traffic.

1. History. Internet evolves, content grows and diversifies, reports on illegal and harmful or otherwise unwanted content start to come in, public, ISP's and official concern grows (in that order) . . .

2. Legal situation.
   a) Very unclear in the beginning.
   b) At present: ISP's (all carriers in fact, and somewhat like publishers) are *not* responsible/liable for third-party content. For several reasons, of both historical/principal and technical nature (freedom of speech/expression, freedom of information, censorship *ex ante* absolutely being forbidden; and because it is technically impossible or not proportional to the goal to monitor every bit and byte that is passing through networks . .).
   c) One exception: When an ISP knows something illegal is actually residing "on" his machine/server/hard disk, and he has knowledge of that fact, he is responsible/liable and has to act accordingly.

3. Responsibilities.
   a) Police is responsible for tracking down and prosecuting law-violators (ISPs are obliged to assist when asked of course).
   b) ISPs are not responsible for third-party content, except in some well-defined cases.
   c) ISPs do feel a social/moral responsibility to assist where they can to minimise illegal and potential harmful content, and to protect minors and human dignity. But they have to stay within the laws!

4. Actions.
   a) ISPs, concerned citizens, and police got together and decided that everybody (police, ISPs, legal clarity) was helped when incidents could be reported somewhere (neutral).
   b) Together they/we started a hotline (setting up, advertize, etc . .).

5. Experiences so far is good:
    a) Fits in well with Dutch culture and procedures in lots of other sectors.
    b) After a troublesome time of getting-to-know-each-other (very different backgrounds/ expectations/demands in the beginning) all actors involved work together, share knowledge, help in quickly becoming effective and efficient is not yet good enough:
    c) Financing (who finances, how much, hotline is kind of independent but . .).
    d) Prosecuting (no experience, no money, no trained personnel, no priority), both national and (even more so) international.
    e) The understanding of the possibilities and the problems of using the Internet, by the public, the press, the politicians.

6. Conclusions.
    a) All parties concerned, with their different responsibilities, agree that this self-regulation is "best practice", giving the best obtainable result.
    b) Mind that everybody has to give in a little!
    c) Concept of self-regulation: mind the trap/danger of becoming third-party-regulation!
    d) In this case, and at this point of time, Public Private Partnership is important, and probably the best and only solution . . .

Panel No. 4: Government and private sector roles in self-regulation - what are the conditions for successful self-regulation?

James R. Savary
Consumer's Association of Canada
York University

Self-Regulation: A Consumer Perspective Based On Canadian Experience

Slide One
Where We Are Going

- The nature of the issue makes self-regulation particularly appropriate
- Canadian experience in developing its privacy code shows consensus can be reached
- Self-regulation makes international co-operation easier to achieve while both protecting and empowering the consumer

Slide Two
Consumer Priorities

- Privacy of personal information
- Illegal or offensive content

Slide Three
Why Self-Regulation of Illegal/Offensive Content?

- managing content liability
- managing third party issues
- provides tools to users

Slide Four
Will Self-Regulation Work?

- Canadian Code for the Protection of Personal Information provides a model for self-regulation of content:
- developed by stakeholders
- code became a national standard (CSA Q-830)
- code has been proposed as international standard

Slide Five
Some General Principles

- Essential to build consensus
- All interested parties at the table
- Compromises important in leading to development of a standard
- Government an equal partner at the table
- Government may act as mediator as necessary

Slide Six
Why Would This Work in Dealing With Illegal/Offensive Content?

- Content is an emotional issue. Self-regulation is therefore appropriate
- No market failure as arises in the case of privacy
- Can significantly reduce the need for government intervention

Slide Seven
Confers Both Rights and Responsibilities

- Right to develop one's business free of governmental regulation
- Responsibility to adhere to the spirit as well as the letter of the standard

Slide Eight
Who Makes It Work?

- Industry Associations
- Individual content providers
- Service providers
- All three are better equipped to deal with complaints than are other potential regulators

Slide Nine
What Problems Are Likely to Arise?

- Mandatory or Voluntary?
- Mandatory essential or free-rider problem
- Sanctions?
- Implicit, if mandatory is to be meaningful

Slide Ten
Filtering Software

- User-controlled gives choice; this is the essence of consumer sovereignty
- Complements codes of conduct and corporate practices

Slide Eleven
Other Approaches

- No regulation
- Full regulation

Slide Twelve
No Regulation

- Leaves it to courts administering existing law
- Slow, cumbersome, expensive and after the fact
- Therefore not a viable option

Slide Thirteen
Full Regulation

- Much less flexible
- May limit new initiatives

- Compliance may be costly to demonstrate
- Regulations difficult to enforce in a borderless cyber-world

Slide Fourteen
Conclusion

- Internationally agreed-upon standards; otherwise, content havens likely to emerge
- Self-regulation to those standards
- Market monitors compliance
- At its best, self-regulation can provide the umbrella under which consumers can be both protected and empowered

Panel No. 4: Government and private sector roles in self-regulation: what are the conditions for successful self-regulation?

Christophe Sapet
Association des Fournisseurs d'Accès (AFA)

What are the respective roles of governments and the private sector in the context of Internet self-regulation?

Prior to analysing the distinctive characteristics of Internet self-regulation, I would like to respond to the following question:

What are the respective roles of government and the private sector in the "real" -- off-line -- society?

Simply put, one might say that :

- the authorities establish norms
- and the private sector applies them.

In practice,

- the relationship between the private and public sectors is more complex,
- thus, the development of new norms calls for an exchange, a dialogue between the two parties.

As regards the Internet, must the issue of relations between the public and private sectors be re-examined?

1) We know that the Internet is an innovative means of communication

Before the Internet, the diffusion of data was conceived as being:

- principally within national borders,
- one-way only, from sender to receiver,
- and only limited to a certain number of carriers

Now, the Internet is:

- global,
- interactive,
- and allows everyone, professionals or private individuals, to diffuse content

Consequently, efforts to control the diffusion of content are facing new challenges, which we must learn to overcome.

2) Is it necessary to re-think the relationship between the public and private sectors due to the newness of the Internet?

This does not seem reasonable to us, because:

- the Internet does not call for a review of the "real" -- off-line -- society,
- the Internet is "simply" a new space, one that we must learn to manage together.

For the AFA, there are two crucial conclusions:

I) the Internet does not call for a review of the "real" society,

nor does it compound the question of the respective roles of the public and private sectors.

II) the Internet is a new space to conquer,

requiring relations between the public and private sectors to evolve.

I) First point : The Internet does not call into question the respective roles of the public and private sectors.

On this point, it is necessary to eliminate the misconceptions surrounding the term "self-regulation," a term commonly associated with the Internet.

For the AFA, "self-regulation" does not mean that the competence of the judicial and administrative authorities should be compromised,

but rather, the ability of the private sector to manage the space in which it carries out its activities.

In fact,

- in a consistent manner, the question of the conditions for liability of Internet actors comes back to the Court,
- and all other institutions, however representative of civil society, can only be restricted to providing advice and information.

II) Second point : The Internet is new, thus an evolution of the relations between the private and public sectors is necessary.

The Internet poses three different problems:

- the distribution of data is instantaneous,
- the Internet is constantly developing,
- the Internet is global.

These problems are not insurmountable, and we feel that they can be resolved in the following manner:

- Regarding the instant distribution of data,

The AFA believes that the problem posed by the distribution of harmful content can be controlled through the **creation of hotlines,**

and only light infrastructures able to react in a quick and flexible manner, while awaiting final Court rulings,

- Regarding the constant evolution of the Internet,

The AFA believes that it is **necessary to create institutions representative of society and specialising in the Internet**

whose mission is **to enlighten the judiciary and the legislature,** and to provide definitions of those notions such as “reasonable behaviour”, “appropriate law”, etc.

- Regarding the global nature of the Internet,

The AFA believes that control of the Internet environment will develop through **co-ordination :**

- **co-ordination of these institutions at the international level,**
- **and more generally, co-ordination between the public and private sectors, at both the national and international levels.**

CONCLUSION

One of the main objectives of the AFA is to facilitate co-ordination among Internet actors, with government co-ordination being one of its priorities.

The requirements for setting up these institutions (e.g. hotlines, consultative councils) still need to be determined, in particular their financing, but the AFA hopes from now on to be, and is already, an active participant in their setting up and operation.

Thank you for your attention.

Panel No. 4: Government and private sector roles in self-regulation - what are the conditions for successful self-regulation?

Guy Verbeeren
Police Judiciaire, Belgium

Our service has a specific and official task, namely the fight against child pornography on the Internet, and it is about this that I am going to say a few words to you today. I am aware of course that our working methods are altogether different from yours, since our term of reference is the Penal Code.

One consequence of the tragic events which have made headline news in Belgium since August 1996, was that the police felt compelled to set up a judicial Web site on the Internet which would allow members of the public to give information about child pornography.

On the proposition of the Criminal Investigation Department ("*police judiciaire*"), and with the approval of the Minister for Justice, an official and national "child pornography" contact service has been created within the Department.

This service was set up in December 1996. Members of the public who come across child pornography on the Internet can contact us through our E-mail address (*contact@gpj.be*).

It is the National Computer Crime Unit, created within the National Brigade of the Criminal Investigation Department in Brussels, of which I am a member, which administers this official contact service and processes the messages sent in.

The National Computer Crime Unit also carries out searches on the Internet for child pornography and supplies, at the request of other brigades, "technical" assistance in identifying and tracing those responsible.

***

In Belgium, the distribution of pornographic material is an offence against public decency ("*outrage aux moeurs*" -- Article 383 of the Penal Code). If the offence is committed in the presence of minors, sentences are heavier (Article 386 and 386bis of the Penal Code).

Under these provisions, the law punishes all offences against public decency no matter how committed, be it through publication of the printed word, images or figures.

A good starting point is Article 383 of the Penal Code which is perfectly adapted to new methods of distributing pornography, since it provides for punishing anyone who displays or distributes pornographic material by means of a computer network (such distribution need not be for commercial gain).

Under an Act of 13 April 1995, a new Article 383bis punishing child pornography was introduced into the Penal Code.

This Article provides *inter alia* that anyone who displays, sells, rents, distributes or delivers emblems, objects, films, photos, slides or other visual formats representing sexual positions or acts of a pornographic nature involving or showing minors under 16 years of age, or who manufactures, possesses, imports or arranges for import, or delivers to a transport or distribution agent for commercial or distribution purposes, is punishable by imprisonment and a fine of between 500 and 10 000 francs, and anyone knowingly in possession of any emblems, objects, films, photos, slides or other visual formats referred to in paragraph 1, is punishable by imprisonment of between one month and one year, and a fine of between 100 and 1 000 francs.

Thus, the Article punishes not only the display, sale, renting, distribution, delivery, manufacture, import, etc. of child pornography, but also its possession.

It does not impose any conditions as to the type of media used to distribute child pornography, referring to emblems, objects, films, photos, slides or other visual formats.

Distributing child pornography via a computer network -- e.g. posting such material in news groups -- can thus be punished on the basis of current legislation.

But the possession of pornography on hard disk, diskette, or any other electronic or optical format is also covered by the provisions of the Act since the Article in question provides for: "... or other formats".

Pornographic material and other documents of a sexual nature are in large part accessible via international networks (like the Internet). American studies have demonstrated that most of this material consists of photos and texts, with the emphasis on paedophilia.

Pornographic material may be offered on the Internet in different ways, via in particular:

1. E-mail
2. News groups
3. IRC
4. WWW

In addition, photos may be circulated/exchanged through a BBS (Bulletin Board System), accessible to a more restricted number of persons.

***

Through the central E-mail address of the Criminal Investigation Department, it is thus possible for members of the public to contact, in their own language, the competent police service responsible for investigating notifications. Discretion and, where appropriate, anonymity, are thus guaranteed.

The method or procedure followed may be described thus:

1. An Internet user sends a message to the contact address.
2. Our service investigates the content of the message.
3. If it concerns child pornography, a report is drawn up. This report is then sent to the competent service which opens a file for the local magistrate.

If we receive a message concerning a foreign country, with information which is both relevant and worth following up, the message is sent to the competent foreign service.

Only a small number of all messages received are useful and worth following up. But some have nevertheless given rise to judicial investigations.

In 1997, our service received some 2 000 messages or opinions, most of which were not useable for various reasons.

For example:

1. The message did not contain any information but was from someone simply trying to access our contact address.
2. The message concerned something already known to our service.
3. The message contained a point of view concerning paedophilia.
4. The allegations concerned actions not punishable under Article 383bis of the Belgian Penal Code.
5. The message was simply criticising the contact service itself.
6. And sometimes, messages are received from Internet users who think that we can pass on good addresses or even send photos.

Thus, only a small number of the messages received are useable by our service. In 1997, of all messages received, only five gave rise to judicial investigations with subsequent arrests in Belgium or abroad.

As of today, 1998, two judicial files have been opened.

I should also add that we undertake further investigations only if we are absolutely sure that the child concerned is under 16 years of age.

If there is the slightest doubt about this, the assessment is negative and the information non-useable. Assessments are also negative in cases where we are informed of photos in the David Hamilton style or simply, if you will excuse the expression, of "classic" pornographic photos.

While there are cases in which we cannot be sure if the children involved are minors, we can of course tell, even from a photo, whether a child is aged about 10, about 5 or even younger.

From time to time we also receive information about other offences, for example "spamming" or pyramid games. In such cases, we proceed in the same fashion as for child pornography.

***

Given the way we work, we need the co-operation of Internet access suppliers, and I must say that so far, suppliers have been highly co-operative. We have found that in Belgium, as indeed everywhere else, access suppliers want to offer their subscribers and customers a quality product, and make every effort to do so, as proved by the initiatives that they have taken.

The industry has drawn up "self-censorship" proposals, mainly in connection with pornography and child pornography, and a number of such proposals exist already on the Internet.

But it is only by means of a well thought-out response and co-ordinated international action that the problem can be resolved in a satisfactory fashion.

***

Recommendations have already been made at the international and official level, that specialised services responsible for the protection of minors and for investigating offences against minors should be set up, and that the exchange, at international level, of all information concerning such offences be centralised.

As far as Belgium is concerned, a “disappearances” office has been set up within the Police’s Central Research Bureau, and the National Computer Crime Unit within the National Criminal Investigation Brigade.

The “Innocent Images” enquiry in the United States confirmed that setting up specialised services is the only logical, efficient and effective way of identifying and tracing persons who use the Internet for the sole purpose of sexually exploiting children.

In conclusion, I should like to add the following, more general comments.

Protecting children against pornography on the Internet undeniably involves a shared responsibility.

Thus:

- the authorities must take the necessary measures, first to define responsibilities clearly, and secondly, to offer service providers, Web page owners and Internet users a wide legal framework enabling them to develop their activities fully;
- service providers must work together to create a safe medium;
- and those responsible for children -- parents for example -- must also take steps to protect them by using, for example, software packages and/or passwords,

so that children are not banned from accessing the Internet, since this would be the worst solution of all.

Panel No. 5: General discussion

Dr. Michael Baker
Electronic Frontiers Australia (EFA)

Background
Representing EFA which is a member of Global Internet Liberty Campaign (GILC).
Dr. Baker also has a personal interest in these issues as he has a 9 year old daughter.

The Internet is not an industry.
It is a means to multiple ends.
The Internet is not for delivering consumers to business, because users are not just consumers.

A number of important points from the "Impact of Self-Regulation and Filtering on Human Rights to Freedom of Expression" paper (available at *http://www.gilc.org/speech/ratings/gilc-oecd-398.html*), prepared by GILC for the meeting, include:

- "Self-Regulation" in terms of Internet content is a misnomer.
- Not all content is commercial.
- ISPs are not police.

The supposed benefits of self rating should not be oversold.
It will create false expectations which will not be met.
Self-rating won't work - there are no incentives for content providers to self-rate.

The only content which should be banned is that which is banned in all countries.
Such material could be called "Internet illegal"
There is no point in banning material which is protected by the US 1st Amendment. Such material will be available in all countries.

As follow up to the meeting, a dialogue in the (northern) spring was proposed to include:

- ISPs - National Organisations & Individual ISPs
- NGO's
- User Groups

Panel No. 5: General discussion

David Kerr
Internet Watch Foundation (IWF)

Speaking on a general panel in the wash up session of this event means that I do not know in advance precisely what I will be saying. There is however one principle that I wish to illustrate from UK and European experience and one key question that it points to in this global context.

"Self-regulation" in the UK is a misnomer. Yes, the UK Internet industry is regulating itself, but it is doing so under the terms of a jointly agreed approach with government and police, which only limits free speech where it is illegal in the UK, primarily pictures of child pornography.

Developments in the European Commission have followed the same pattern with: joint involvement in the production of policies; government, industry and user support to those policies (Bonn Conference declarations); consultation on the Action Plan to implement the policies, and direct involvement of industry and NGO organisations in the delivery through match funding of a (proposed) substantial EU budget.

The question at the end of this Forum is "Do we have an agreed basis for 'self-regulation' on a global scale which balances the interests of governments, industry, users and freedom of speech?" And the corollary "What is the forum in which it will be developed and adapted for the future?"

All the references in my introductory remarks can be found on the IWF Web site directly or as links to other documents. All I would ask you to remember, or take away, is therefore the URL:

http://www.iwf.org.uk

N.B. There is one important link not yet made on the site - the latest version of the EU Action Plan on promoting safe use of the Internet at: *http://www2.echo.lu/iap/*

Panel No. 5: General discussion

David W. Phillips
AOL Bertelsmann Online (Europe)

Self-Regulation: What are we regulating?

Need to understand key attributes of the new medium and how it differs from traditional media

- Interactive
- Interdependent
- Ubiquitous & Open

Key Attributes

Interactive

- Users empowered -- content generally pulled not pushed
- Users can become global publishers and distributors
- Providers can potentially track where users go and what they do

Interdependent

- Links between different Websites
- Seamlessness of physical borders places limitations on nations' ability to regulate

Ubiquitous and Openness

- Regulatory regimes of telecoms and broadcast industries should not apply
- Broadcast - limited spectrum; content pushed; limited user tools
- Telephone - State granted monopolies

Regulatory Models

Market
Self-Regulation
Government Regulation
Reality is mixture

Market Model

Companies will self-regulate own behavior for fear of loosing customers and tarnishing brand
Dependent on transparency of information and consumer choice

- dependent on degree of market competition, consumer bargaining power and consumer press

Advantages: low cost, allows companies and consumers maximum freedom
Disadvantages: doesn't protect individual consumer

Government Regulation

Advantages: Clarity, Enforcement
Disadvantages: Cost, Rigidity

Self-Regulation

Advantages

- Draw upon industry expertise
- Flexibility
- Internalization of values by industry

Special advantages given global and dynamic nature of medium

Disadvantages : Lack of enforcement teeth

Best of Breed Combination

Promote competition and transparency

Promote Self-Regulation measures with legislative, enforcement, and adjudicatory elements

Address market and self-regulatory failures carefully

- Narrowly tailor government regulations
- Maintain flexibility
- Two government regulatory examples are failures

  - US -- Communications Decency Act
  - Germany - Multimedia Law