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

OLIS : 07-Jul-1999
Dist. : 09-Jul-1999

Or. Ang.

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

DSTI/ICCP(98)18/FINAL
Non classifié

COMPTE RENDU SUCCINCT DU FORUM OCDE/BIAC SUR L'AUTOREGULATION DU CONTENU SUR INTERNET

Paris, 25 mars 1998

79882

Or. Ang.

REMERCIEMENTS

Le Comité consultatif économique et industriel auprès de l'OCDE (BIAC) et l'OCDE, qui ont co-patronné le Forum sur l'autorégulation du contenu sur Internet, souhaitent remercier de leurs contributions ***IBM Corporation*** (qui a mis ses locaux à disposition pour la réunion), ***AT&T Corporation***, le ***Groupe Bull*** et ***Oracle Corporation***, qui ont rendu ce patronage possible.

TABLE DES MATIÈRES

SYNTHÈSE

Le Forum sur l'autorégulation du contenu sur Internet s'est tenu le mercredi 25 mars 1998 dans les locaux d'IBM, Tour Descartes, Paris-La Défense, France. Il était organisé par un comité directeur composé de représentants des délégations nationales (piloté par les États-Unis et le Canada[1]) et placé sous les auspices du BIAC et de l'OCDE.

Plus de 150 participants représentant les gouvernements, le secteur des entreprises, des organisations internationales publiques et privées et des groupes de défense d'intérêts communs ont pris part à cette réunion. La plupart des orateurs étaient des représentants de l'industrie (dont plusieurs experts juridiques), notamment de fournisseurs de services sur Internet (FSI) et d'associations de FSI, d'entreprises spécialisées dans les logiciels de filtrage, de fournisseurs de contenus et de publicitaires. Étaient également représentées des associations de consommateurs, des groupes de défense de la liberté de parole et un service de police actif dans ce domaine.

Les participants ont examiné un certain nombre de questions concernant l'autorégulation du contenu sur Internet, notamment :

- Les pressions en faveur de l'autorégulation et leur origine.
- Les principaux codes de conduite et bonnes pratiques et les raisons de leur efficacité.
- Les technologies centrées sur les usagers et les raisons de leur efficacité.
- Les rôles des pouvoirs publics et du secteur privé dans l'autorégulation : les conditions d'une autorégulation réussie.

Le principal thème abordé a sans doute été la nécessité d'assurer une éducation permanente : des utilisateurs, des parents, des enseignants et des enfants pour leur apprendre à utiliser la technologie et à prendre leurs responsabilités ; du secteur des entreprises ; des responsables des politiques ; et enfin des autorités de police.

Les participants au Forum ont fait valoir qu'une collaboration était nécessaire entre les entreprises, les pouvoirs publics et les utilisateurs, notamment dans le domaine de l'application des lois. Ils ont en outre constaté que les utilisateurs devaient être associés à l'élaboration du système d'autorégulation.

Certains FSI se sont dits préoccupés par leur rôle de coopération avec les autorités de police. Beaucoup conviennent que les questions de responsabilité, notamment concernant les contenus fournis par des parties tierces établies à l'étranger, devaient être soigneusement étudiées et éclaircies. Plusieurs d'entre

1. Le comité directeur chargé de l'organisation du Forum était composé de représentants de la Belgique, du Canada, des États-Unis, de la Finlande, de la France, de la Hongrie, du Japon, du Royaume-Uni et du Comité consultatif économique et industriel auprès de l'OCDE (BIAC).

eux ont expressément indiqué qu'ils craignaient de se trouver dans une situation où ils devraient suppléer aux autorités de police.

Un certain nombre de domaines ont été recensés, dans lesquels une autorégulation pourrait être utilement instaurée par les fournisseurs de services Internet : pour ce qui est des contenus, il s'agissait principalement des contenus choquants et illégaux, de la protection des informations à caractère privé, de la censure, du spamming et du copyright ; les autres domaines évoqués comprenaient la protection des consommateurs et l'anonymat.

L'autorégulation est utilisée dans divers domaines où des lois de caractère général s'appliquent aux contenus en ligne. L'autorégulation répond également aux pressions du marché, comme dans le cas des contenus choquants dans lequel les technologies axées sur l'utilisateur semblent offrir des perspectives très intéressantes. Plusieurs stratégies d'autorégulation ont été examinées : codes de conduite, politiques d'entreprises, programmes de sensibilisation, lignes directes, étiquetage et logiciels de filtrage.

Certains participants sont d'avis qu'une « soft law », notamment des codes de conduite, pourrait compléter la « hard law », ou estiment que l'autorégulation a besoin d'un cadre juridique pour être vraiment efficace et utile.

Les participants ont indiqué qu'ils souhaitaient participer aux prochains débats internationaux entre l'industrie d'Internet, les fournisseurs de contenu, les utilisateurs et le secteur public afin de promouvoir la collaboration internationale et l'échange d'expériences dans le domaine de l'autorégulation.

ORDRE DU JOUR

Note d'ouverture par les co-présidents du Forum :

Dr. Etienne Gorog, Président, PIIC/BIAC et Richard Beaird, Président, PIIC/OCDE

Panel N° 1 - Quelles sont les pressions pour l'autorégulation et d'où viennent-elles?

Modérateur : Roger Cochetti, IBM (USA)

Panelistes:

-- Manuel Kohnstamm, Time Warner Europe

-- Lisa Balaban, Sympatico/Medialinx Interactive, L.P. (Canada)

Panel N° 2 - Quels sont des exemples importants de codes industriels de conduite et de pratiques corporatives et pourquoi sont-ils efficaces?

Modérateur : Yves LeRoux, Digital Equipment Corporation (France)

Panelistes :

-- Stephano Lamborghini, Associazione Italiana Internet Providers (AIIP) (Italie)

-- Wally O'Brien, National Advertising Review Council, Inc., (USA)

-- Kazuko Otani, Telecom Service Association (TELESA) (Japon)

-- Margo Langford, Canadian Association of Internet Providers (Canada)

-- Professor Michel Vivant, Université de Montpellier (France)

Panel N° 3 - Les technologies centrées sur les usagers et pourquoi sont-elles efficaces?

Modérateur : Claude Boulle, Groupe Bull (France)

Panelistes :

-- Marilyn S. Cade, AT&T (USA)

-- Akio Kokubu, Electronic Network Consortium (ENC) (Japon)

-- Don S. Sandford, NetShepherd Inc. (Canada)

-- Gordon Ross, NetNanny, Ltd. (USA)

-- Susan J. Getgood, The Learning Company, Inc. (USA)

Panel N° 4 - Les rôles du gouvernement et du secteur privé dans l'auto-régulation - quelles sont les conditions pour une autorégulation réussie?

Modérateur : Peter Upton, Australian Information Industries Association (Australie)

Panelistes :

-- Marku Ropponen, Internet Service Providers Association (Finlande)

-- Dr. A. Eisner, Association of Dutch Internet Service Providers (NLIP) (Pays-Bas)

-- 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 (Belgique)

17:00 Panel N° 5 - Discussion générale

Modérateur : Maria Livanos Cattaui, Chambre internationale de commerce

Panelistes :

-- Michael Baker, Electronic Frontier (Australie)

-- David Kerr, Internet Watch Foundation (Royaume-Uni)

-- David Phillips AOL Bertelsmann Online (Allemagne)

Notes de clôture par les co-présidents du Forum.

COMPTE RENDU

Le Forum est co-présidé par **M. Etienne GOROG**, Président du Comité de la politique de l'information, de l'informatique et des communications du BIAC et par **M. Richard C. BEAIRD**, Président du Comité de la politique de l'information, de l'informatique et des communications de l'OCDE. Il est organisé dans le but d'étudier les possibilités d'autorégulation du contenu sur Internet en examinant les dispositions et technologies qui pourraient permettre de résoudre les problèmes de contenus préjudiciables ou illégaux sur Internet. M. Gorog souligne l'importance des solutions techniques et appelle le secteur privé à offrir aux utilisateurs d'Internet une panoplie d'outils technologiques qui leur permette de choisir le contenu qu'ils souhaitent visualiser sur Internet.

M. Beaird souligne l'utilité d'un dialogue entre l'industrie et les gouvernements sur le problème du contenu sur Internet. Il salue la solidité des relations entre le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE (PIIC) et du Comité Consultatif économique et industriel auprès de l'OCDE (BIAC), qui forment la pierre angulaire de l'action de l'OCDE dans ce domaine et dans d'autres domaines appelant une contribution active du secteur privé. Il constate que la communauté des utilisateurs professionnels de même que l'industrie des technologies de l'information sont bien représentées au Forum qui offre ainsi aux gouvernements des pays Membres l'occasion de dialoguer avec les principaux acteurs de ce secteur en plein essor.

PANEL 1 : Quelles sont les pressions en faveur de l'autorégulation et d'où viennent-elles ?

Le premier panel est présidé par **Roger J. COCHETTI** d'IBM, qui lance la réflexion en décrivant les pressions en faveur d'une autorégulation de l'industrie qui se sont exercées suite à la polémique concernant l'accès des mineurs aux contenus préjudiciables et illégaux sur Internet. La sensibilisation du public et l'intérêt des gouvernements pour ces questions, ainsi que la rapide croissance d'Internet, constituent un défi pour le secteur privé. Les solutions technologiques constituent l'instrument le plus efficace et le plus performant pour répondre aux préoccupations du public concernant les contenus illégaux et préjudiciables et les progrès réalisés dans ce domaine apparaissent prometteurs. M. Cochetti évoque en particulier la plate-forme PICS (*Platform for Internet Content Selection*) qui est actuellement l'instrument technologique le plus important pour contrôler l'accès aux contenus Internet. Il constate que la faible utilisation de ce système inquiète les pouvoirs publics mais ajoute que la situation dans ce domaine est en train d'évoluer. M. Cochetti explique que la plate-forme PICS est plus efficace lorsqu'elle est incorporée dans le logiciel de navigation sur Internet et note que désormais Microsoft et Netscape incluront le système PICS dans leurs programmes de navigation, ce qui fait qu'elle sera pratiquement universellement utilisable.

Manuel KOHNSTAMM de Time Warner Europe présente Time Warner qui est l'un des premiers fournisseurs de contenus sur Internet et qui exploite cinq des sites actuellement les plus visités (CNN, Warner Brothers, Time, Fortune et Money). Il indique que Time Warner se charge également de fournir l'accès Internet à des écoles et à des collectivités. L'expérience de Time Warner apporte à cet égard un éclairage utile sur l'industrie d'Internet. M. Kohnstamm constate qu'une autorégulation apparaît aujourd'hui nécessaire dans cette jeune industrie et décrit certains avantages et faiblesses des systèmes de réglementation et d'autorégulation. Il évoque les conséquences des pouvoirs éditoriaux exercés par les fournisseurs de contenus dans leurs décisions quotidiennes concernant ce qu'ils vont publier sur support traditionnel et en ligne, en soulignant qu'ils sont tenus de founir des matériaux non expurgés mais en reconnaissant que les utilisateurs doivent être en mesure de choisir le contenu qu'ils souhaitent visualiser. Il insiste sur la nécessité de protéger la liberté de parole, notamment sur Internet.

M. Kohnstamm indique que Time Warner estime que les systèmes volontaires de classification (cotation) constituent une des options qui permettraient de résoudre les questions de contenu sur Internet, mais qu'ils devraient être développés dans un environnement concurrentiel offrant divers mécanismes de classification et ne devraient pas être imposés par défaut. Il existe divers outils de filtrage et la plate-forme PICS n'en est qu'un parmi d'autres. Il est également important de disposer de plusieurs systèmes de classification pour répondre aux besoins des différents pays et différentes cultures. Il précise toutefois que ces systèmes ne doivent pas se substituer au contrôle des parents sur les activités de leurs enfants sur Internet. Selon lui, une image de marque forte pourrait servir de référence aux parents. Ceux-ci connaissent souvent moins bien les ordinateurs que leurs enfants, c'est pourquoi l'industrie doit contribuer à les éduquer, et partant à les habiliter à exercer un contrôle. Comme tout fournisseur d'informations, l'industrie doit diffuser des matériaux sérieux. Les entreprises comme Time Warner sont particulièrement désireuses de fournir des contenus adaptés aux enfants pour conserver leur image de marque auprès des consommateurs et partant, leur clientèle. L'industrie des médias possède l'expérience nécessaire pour trouver un juste milieu entre le contrôle du contenu et la liberté d'expression, et il n'y a aucune raison que ces compétences ne s'appliquent pas à Internet. *(Documentation présentée : diapositives)*

Lisa BALABAN de Sympatico commence son exposé en expliquant qu'elle a du rapidement se former au droit d'Internet et à l'autorégulation lorsque sa société, l'un des premiers fournisseurs de services Internet du Canada, a été lancée l'année dernière en l'espace de six semaines en français et en anglais. Elle constate qu'en raison du caractère foncièrement international d'Internet, il est parfois difficile de déterminer quelles réglementations s'appliquent aux contenus en ligne et remarque que dans l'environnement actuel en pleine mutation, ce sont les politiques et non les lois qui pèsent le plus sur le comportement des entreprises fournissant des contenus sur Internet.

Répondant à une question concernant l'existence d'un "droit du cyberespace", Mme Balaban décrit la situation du Canada où il n'existe pas de droit spécifiquement applicable au cyberespace mais où le gouvernement canadien (Industrie Canada) contrôle le développement de la cyberindustrie. La responsabilité concernant le contenu sur Internet fait partie des nombreuses questions de droit auxquelles se heurtent les fournisseurs de services Internet (FSI) et d'autres acteurs de l'industrie en ligne. Si les FSI créent un contenu, ils doivent en assumer la responsabilité. D'un autre côté, comment un FSI peut-il être responsable d'un contenu qu'il ne contrôle pas ? L'environnement en ligne suscite également d'autres problèmes juridiques concernant notamment la propriété intellectuelle, la protection de la vie privée et le commerce électronique. D'une façon plus générale, les aspects relevant de l'action des pouvoirs publics concernent l'établissement d'un environnement Internet sûr pour renforcer la confiance des consommateurs ; donner plus de pouvoirs aux utilisateurs (c'est-à-dire permettre à chacun de se protéger des contenus jugés indésirables), faciliter le plus possible l'accès des utilisateurs à Internet ; et instaurer une coopération entre les pouvoirs publics, l'industrie et les organisations de consommateurs.

Mme Balaban, décrit comment sa société fait face à ces problèmes cruciaux. Les contrats de service conclus par Sympatico avec les utilisateurs et les sites Web comportent un certain nombre de clauses et les visiteurs des sites Sympatico se voient notifier les modalités et conditions d'utilisation en ligne. Sympatico part du principe que puisqu'il est fournisseur de contenu canadien, les lois du Canada s'appliquent aux contenus de son site Web et les utilisateurs sont informés de cette disposition par la présence de petits drapeaux canadiens sur les sites (une pratique empruntée au droit maritime). Sympatico estime que la responsabilité du contenu doit revenir à la partie qui le contrôle. La société n'exerce pas de censure sur les contenus mais répond aux plaintes de non respect de la loi et s'engage à fermer les sites contenant des documents illégaux. En conclusion, Mme Balaban souligne la nécessité d'une coopération entre les FSI, le public et le gouvernement, en vue d'éduquer les utilisateurs de réseaux et de mettre au point des politiques répondant aux attentes de toutes les parties. *(Documentation présentée : diapositives, notamment modalités et conditions d'utilisation et recommandations concernant le site Web de Sympatico).*

PANEL 2 : Quels sont les principaux exemples de codes de conduite et de bonnes pratiques et pourquoi sont-ils efficaces ?

Le second panel est présidé par **Yves LE ROUX** de Digital Equipment Corporation, qui fait remarquer que puisque les participants opèrent tous dans des environnements réglementaires différents, le forum devrait permettre de se faire une idée des situations rencontrées un peu partout dans le monde.

Le premier intervenant, **Stefano LAMBORGHINI** de l'*Associazione Italiana Internet Providers* (AIIP), indique que l'AIIP a mis au point un code de conduite pour les fournisseurs de services Internet en Italie. Pour ce faire, l'AIIP a passé en revue toutes les initiatives menées dans ce domaine en Europe et ailleurs. En mai 1997, le code a été soumis pour approbation au Ministère des communications italien puis adopté au début de 1998 par les membres de l'AIIP, à l'issue d'un débat constructif entre les opérateurs de télécommunications et les groupes de consommateurs. La prochaine étape consistera à examiner comment ce code fonctionne sur le terrain.

Le code a pour but principal d'assurer sur Internet un environnement propice au développement culturel et à l'éducation, ainsi qu'au commerce. M. Lamborghini souligne la nécessité de mettre en place un environnement positif sur Internet et de renforcer la confiance des utilisateurs. Outre un certain nombre de principes généraux et d'obligations pour les FSI, le code comporte trois grands points relatifs à l'autorégulation des activités des FSI : la responsabilité, l'identification et l'anonymat. S'agissant de la responsabilité sur Internet, en vertu du code, celle-ci revient à celui qui diffuse le contenu sur Internet, qu'il s'agisse d'un site commercial ou individuel. Il prévoit aussi la possibilité de retrouver les fournisseurs de contenu et de vérifier leur identité afin d'établir les responsabilités. Toutefois, le code reconnaît aussi qu'il est important de protéger l'anonymat aux fins de la diffusion des informations et données et de la protection de la vie privée, cherchant un juste équilibre entre la préservation de l'anonymat et la possibilité pour les autorités chargées d'appliquer les lois d'identifier les internautes qui mènent des activités illégales sur le réseau. Le code souligne aussi la nécessité de protéger la dignité humaine et les mineurs. M. Lamborghini note que le code préconise l'utilisation de mécanismes de filtrage, de blocage et de classification, bien que certains défenseurs des droits de l'homme considèrent qu'il s'agit là d'une forme de censure. Le code aborde enfin les questions de propriété intellectuelle.

S'agissant de la gestion et de la mise en application du code de conduite de l'AIIP, deux types d'organes d'autorégulation sont prévus : le premier devrait s'occuper des problèmes initiaux de mise en oeuvre du code et de son éventuelle révision à la lumière des situations nouvelles ; le second serait chargé de régler les différends et de faire appliquer le code en réprimant les infractions et en imposant des sanctions. De plus, l'AIIP entend créer un système d'arbitrage en ligne en liaison avec la Cour suprême italienne et la Chambre de commerce de Milan. L'AIIP coopère en outre à divers projets avec l'EuroISPA et d'autres associations européennes et américaines de FSI, afin de conserver une vision mondiale des évolutions et d'encourager l'harmonisation des règles d'autorégulation. *(Documentation présentée : notes d'exposé)*

Walter J. O'BRIEN du *National Advertising Review Council* (NARC) présente un exposé sur le contenu Internet en évoquant le cas de la publicité destinée aux enfants. Il explique le rôle du *National Advertising Review Council* dans l'autorégulation du secteur publicitaire aux Etats-Unis. Dans ce secteur, l'autorégulation donne de bons résultats depuis 20 ans aux Etats-Unis, partant du principe que le gouvernement a un rôle à jouer et que les publicitaires ont aussi un rôle à jouer en s'autorégulant. Le *Children's Advertising Review Unit* (CARU) est l'un des trois organes du NARC. Il a été créé par le secteur de la publicité destinée aux enfants et gère des Lignes directrices applicables à la publicité destinée aux enfants de moins de 12 ans, visant à assurer que la publicité est véridique, exacte et adaptée au public visé. Le CARU met en oeuvre ces lignes directrices en s'appuyant sur la collaboration volontaire des publicitaires.

M. O'Brien se dit préoccupé par les nouveaux modes de communications électroniques interactifs et par les nouveaux problèmes qu'ils posent au secteur publicitaire, ainsi que par l'incidence d'Internet sur les systèmes d'autorégulation existants. La complexité du nouvel environnement en ligne accessible aux enfants rend la situation encore plus préoccupante. M. O'Brien explique comment, avec une souris et un clavier, les enfants peuvent choisir par un simple click quel contenu visualiser, ce qui rend la médiation parentale beaucoup plus difficile. Dans le cas des contenus publicitaires en ligne, le principal danger réside dans le brouillage possible de la frontière entre les contenus publicitaires et les contenus informatifs ou ludiques. Selon lui, les contenus publicitaires devraient être clairement signalés, par exemple en y faisant figurer un petit personnage fixe ou animé facilement reconnaissable par les enfants, sur le modèle des "*Ad bugs*" du CARU qui ont pour fonction de prévenir les enfants qu'il s'agit de publicité. Différents sites utilisent ce procédé, notamment ceux de Galoob Toys et de Kellogs.

La collecte de données en ligne auprès de mineurs constitue un autre problème important qui affecte l'industrie en ligne. Le NARC considère que la protection de la vie privée des enfants, passe par l'information et le libre choix des parents qui doivent savoir comment l'information est collectée et quel usage en sera fait ultérieurement. Ses lignes directrices invitent l'industrie à déployer des "efforts raisonnables" pour obtenir le consentement des parents avant de recueillir des informations sur leurs enfants. On espère que le fait de fixer des objectifs sans imposer les moyens de les atteindre laissera aux publicitaires la liberté et la responsabilité de décider de la meilleure façon d'éduquer les parents et de les habiliter à faire des choix. Kidscom, Kellogs, Disney et Microsoft Kids, pour ne citer qu'eux, se conforment à ces lignes directrices.

M. O'Brien termine son exposé en décrivant une initiative nouvelle et novatrice dans le domaine de l'autorégulation à savoir BBBOnline, un instrument de certification mis au point par le *Council of Better Business Bureaus*, qui encourage une éthique commerciale reposant sur six critères. A l'heure actuelle, plus de 1000 entreprises l'ont adopté. Le label BBBOnline certifie qu'une entreprise respecte certaines pratiques commerciales en ligne et l'utilisateur peut vérifier l'authenticité du label en cliquant sur une icône. Il est prévu de développer un système analogue axé sur la protection de la vie privée. Selon M. O'Brien, il appartient au secteur privé de définir des lignes directrices à l'intention des publicitaires ; de mettre au point des outils permettant aux consommateurs de se protéger ; de lancer des labels de type "testé et approuvé" pour aider les parents à protéger leurs enfants ; et de prévoir des sanctions pour assurer l'efficacité de l'autorégulation. Il pense que la solution réside dans l'autorégulation et engage l'industrie à prendre des mesures pour protéger la vie privée des mineurs afin de prévenir l'instauration d'un traitement législatif. *(Documentation présentée : notes d'exposé)*

Kazuko OTANI, de l'Association des services de télécommunications du Japon (TELESA), qui réunit 18 % des fournisseurs japonais de services Internet, présente les lignes directrices de TELESA destinées aux Codes de conduite des fournisseurs de services Internet. Ces lignes directrices ont été mises au point en réponse à l'explosion du nombre de FSI au Japon, à la prolifération des contenus préjudiciables et d'autres activités criminelles sur Internet, et à la multiplication des différends concernant les activités en ligne, notamment les contrefaçons littéraires, les propos diffamatoires et la responsabilité. Ces lignes directrices visent à protéger les utilisateurs et à fournir à l'industrie un cadre en matière d'autorégulation.

Mme Otani résume les principaux aspects abordés dans les lignes directrices en insistant tout particulièrement sur les principes fondamentaux suivants :

- Protection de la liberté d'expression du fournisseur de contenu.

- Responsabilité des fournisseurs de contenu pour les contenus qu'ils diffusent.

- Protection de la confidentialité des communications et des données personnelles.

– Protection des mineurs : les FSI doivent utiliser des systèmes permettant aux parents ou aux responsables des enfants de prendre les mesures nécessaires pour les protéger.

Mme Otani appelle également l'attention sur les dispositions des lignes directrices relatives à la mise en oeuvre et au respect de l'application. Les FSI sont invités à inclure certaines clauses dans les contrats souscrits avec les utilisateurs. Par exemple, les FSI doivent spécifier dans les conditions du contrat, que les utilisateurs sont censés se comporter de façon adéquate en ce qui concerne les contenus qu'ils diffusent via le FSI et énoncer les mesures qui peuvent être prises en cas de violation par un utilisateur. Une autre section des lignes directrices est consacrée aux procédures de plainte et aux réponses du FSI aux enquêtes officielles et autres investigations menées sur les utilisateurs. Enfin, les lignes directrices encouragent la coopération internationale avec d'autres organisations de FSI compte tenu de la dimension mondiale d'Internet. TELESA s'efforce actuellement d'encourager ses membres et d'autres FSI à se conformer à ces lignes directrices. *(Documentation présentée : diapositives)*

Margo LANGFORD de l'Association canadienne des fournisseurs Internet évoque la création du code de conduite du CAIP qui marque une première étape vers la mise en oeuvre d'initiatives d'autorégulation dans ce domaine. Elle énumère plusieurs aspects qui pourraient relever de la responsabilité des FSI : diffamation, obscénité, protection de l'enfance, protection des consommateurs, contingentement des contenus, protection de la vie privée, des données et de la propriété intellectuelle. Tous les FSI et fournisseurs de contenus devraient réfléchir sérieusement aux problèmes très divers que suscite leur activité en ligne ; toutefois, si les grandes entreprises disposent des ressources nécessaires pour mener une telle réflexion, les entreprises plus petites n'ont pas les moyens de traiter ces problèmes et ne savent pas comment les résoudre efficacement. C'est ici que des organisations professionnelles de FSI comme la CAIP peuvent jouer un rôle important.

S'agissant de la question des responsabilités potentielles assumées par les FSI et les propriétaires de sites, Mme Langford indique qu'il importe de déterminer qui a la maîtrise de la technologie. La loi doit s'appliquer aux acteurs d'Internet selon la fonction qu'ils exercent. Les FSI ont à leur disposition plusieurs moyens pour gérer les risques en la matière : ils peuvent bloquer des adresses IP, refuser d'héberger ou de diffuser des contenus illégaux, opérer un partage contractuel des responsabilités et spécifier la juridiction en cas de recours. Les utilisateurs, de leur côté, peuvent utiliser des technologies de filtrage des contenus et de protection de la vie privée, encourager les systèmes de classification et utiliser des procédures d'enregistrement des plaintes. Malheureusement, trop peu de gens connaissent l'existence du code du CAIP et les médias continuent de donner une image négative d'Internet. En outre, très peu de plaintes sont actuellement déposées et les réponses ne sont pas systématiques.

Mme Langford cite un cas dans lequel des menaces de poursuites judiciaires et de sanctions économiques ont été utilisées à l'encontre d'un FSI pour le contraindre à retirer un contenu illégal placé sur un site Web par un utilisateur local (dans ce cas un enregistrement piraté). Cette situation a soulevé un autre problème juridique encore non résolu pour déterminer si la divulgation, par le FSI, des coordonnées du client constituait une atteinte à la vie privée de l'utilisateur. Mme Langford constate que si, dans ce cas, les matériaux illégaux ont été retirés du site, on ne peut raisonnablement engager des poursuites dans le monde entier contre tous les petits sites coupables de diffuser des contenus illégaux.

Les moyens techniques ne peuvent apporter à eux seuls la solution : l'information et l'éducation de tous les acteurs, notamment des FSI, des groupes d'utilisateurs et des créateurs de contenus sont également indispensables pour résoudre ces questions et assurer le développement de mécanismes efficaces d'autorégulation. On pourrait aussi, pour assurer une meilleure transparence en matière de contenus en ligne, créer des "pages jaunes" sur le Web contenant les noms et adresses des propriétaires de sites. Mme Langford pense que l'éducation doit se faire à l'échelle mondiale. Les groupes d'utilisateurs doivent être informés des violations, les créateurs de sites, des mesures coercitives et les FSI doivent être

encouragés à devenir plus réceptifs en améliorant leurs outils et procédures. *(Documentation présentée : diapositives)*

Le dernier intervenant du panel, **Michel VIVANT**, évoque les initiatives récentes lancées en France dans le domaine du contenu sur Internet. Il décrit la proposition française de Charte de l'Internet présenté en 1997, document ambitieux destiné à favoriser le développement harmonieux de l'Internet en définissant les règles et usages de ses acteurs et en établissant un organisme d'autorégulation, le Conseil de l'Internet. Cette proposition n'ayant pas reçu un large soutien, une commission juridique, présidée par le Professeur Vivant a préparé un manifeste énonçant les grands principes que devraient accepter les utilisateurs du réseau. M. Vivant décrit les codes de conduite professionnels des FSI mis au point par le Groupement des Fournisseurs d'Information en Ligne (GFII) et par l'Association des fournisseurs d'accès (AFA). Il note enfin qu'une commission gouvernementale mène actuellement une étude approfondie sur ces questions pour déterminer comment adapter la réglementation de l'Internet à la nature spécifique de l'environnement réticulaire.

Selon le Professeur Vivant, une "soft law" plus souple, réaliste et adaptée à l'Internet, pourrait compléter la "hard law". Les critères de responsabilité juridique, fondés sur la définition de l'individu rationnel, offrent un exemple dans lequel la législation traditionnelle doit être complétée pour pouvoir s'appliquer à Internet, car on ne sait pas bien ce qu'est un comportement rationnel sur Internet. Autre domaine dans lequel la "soft law" pourrait utilement compléter la hard law : les conventions internationales sur les compétences, qui pourraient ne pas donner les mêmes directives pour l'espace en ligne et pour l'espace hors ligne étant donné le caractère transfrontière d'Internet.

M. Vivant conclut en soulignant, à l'instar des autres intervenants, que l'autorégulation passe par l'éducation des acteurs, des utilisateurs et des autorités en charge de l'Internet. Partant, les premières mesures prises en France pour développer une méthode souple adaptée à la réalité d'Internet comprendront la création et la gestion d'une ligne directe (*hotline*) pour donner des conseils au cas par cas et la mise en place d'une autorité qui jouera un rôle consultatif et celui de médiateur. *(Documentation présentée : notes d'exposé)*

PANEL 3 : Les technologies centrées sur les usagers ; pourquoi sont-elles efficaces ?

Le troisième panel est présidé par **Claude Boulle**, du Groupe Bull, France. Il constate qu'il existe sur le marché divers outils permettant aux utilisateurs de mieux maîtriser leurs choix sur Internet et indique que seuls quelques uns de ces outils seront décrits par les participants.

En ouvrant la séance, **Marilyn S. CADE** d'AT&T Corporation souligne qu'il est nécessaire de donner aux utilisateurs les moyens d'agir par eux-mêmes sur Internet et de mettre au point des solutions acceptées au plan mondial. Internet apporte diverses contributions positives à la société et offre des perspectives également pour les enfants, en tant qu'outil éducatif et espace de loisirs, mais son succès dans ce domaine exige une collaboration. Au cours des deux dernières années, AT&T a cherché à réunir toutes les parties intéressées, groupes de défense des intérêts des mineurs, représentants de l'industrie, représentants des autorités chargées de l'application des lois et responsables gouvernementaux, pour mettre au point des outils efficaces susceptibles de permettre aux utilisateurs de mieux maîtriser l'accès en ligne aux contenus de leur choix, et aux médias d'aménager un environnement sans danger pour les enfants.

Mme Cade compare Internet à une ville en construction dans laquelle se trouvent des quartiers sans danger et d'autres moins sûrs ou en cours d'aménagement. Dans cet environnement, les parents et les enseignants doivent disposer d'outils permettant de faire d'Internet un espace sans danger pour les enfants. AT&T s'intéresse de près à la protection des mineurs mais craint qu'un traitement législatif se révèle inutile ou inapproprié. Par exemple, le *US Communications Decency Act* aurait contraint les fournisseurs

de services Internet à jouer un rôle coercitif, ce qui aurait été difficile et onéreux. Mme Cade fait remarquer que la mise en oeuvre des proposition visant à rendre obligatoire les logiciels de filtrage ou de blocage freinerait l'innovation et empêcherait le progrès sur Internet. S'agissant de l'attitude à adopter face aux contenus préjudiciables et illégaux, elle préconise de s'appuyer simultanément sur des moyens techniques, les lois existantes et l'éducation, notamment pour encourager les parents à intervenir davantage et leur donner plus de prise dans ce domaine.

Mme Cade évoque quatre résolutions importantes du secteur privé adoptées à un sommet tenu à la Maison blanche fin 1997. Les FSI doivent n'avoir aucune tolérance vis-à-vis des contenus préjudiciables et illégaux ; lancer des programmes de sensibilisation et de formation à l'intention des utilisateurs et des responsables chargés de faire appliquer la loi ; encourager la mise en place d'une "Cyber-Tipline" (financée par le Congrès et l'industrie) où les questions et les plaintes pourront être adressées ; et dresser un inventaire complet des outils technologiques existants. Pour conclure, Mme Cade reconnaît que des règles pourraient se révéler nécessaires, mais elle engage les gouvernements à rester souples et patients en attendant que les travaux sur l'éducation des utilisateurs et sur les technologies susceptibles de leur donner une plus grande maîtrise progressent.

Akio KOKUBU présente l'*Electronic Network Consortium*, une organisation professionnelle pour les fournisseurs de services en ligne au Japon, qui a pour vocation de résoudre les différents problèmes rencontrés par les FSI dans l'exercice de leur profession. M. Kokubu décrit les activités actuelles de l'ENC dans le domaine de l'autorégulation, qui comprennent l'élaboration de lignes directrices déontologiques pour l'exploitation de services en ligne, l'établissement de règles comportementales ("Netiquette") à l'intention des utilisateurs et la création du premier bureau de labélisation "compatible-PICS".

M. Kokubu décrit les dispositions prévues par la loi japonaise envers les contenus illégaux et préjudiciables sur Internet en évoquant le principe du secret des communications, la nécessité d'éviter la censure, le problème des responsabilités concernant les contenus illégaux et la protection des droits de l'homme. Pour illustrer la difficulté de réguler Internet, M. Kokubu relate une affaire criminelle qui s'est déroulée récemment au Japon et qui a mis en scène un mineur dont l'identité et la vie privée étaient protégées par la loi japonaise sur les mineurs. Des photos du suspect publiées sur Internet avaient suscité un tollé général. La plupart des sites japonais ont accepté de détruire les photos du garçon mais les sites étrangers ont ignoré les lois japonaises. La police japonaise a eu du mal a faire respecter les lois japonaises dans ce cas et dans celui d'autres contenus illégaux placés sur des sites étrangers. Le Japon est soucieux de lutter contre la pornographie illégale diffusée sur Internet, en particulier lorsqu'elle met en scène des enfants.

M. Kokubu décrit les activités d'autorégulation menées dans ce domaine au Japon, notamment les efforts déployés pour développer et mettre en oeuvre les lignes directrices de l'ENC à l'intention des fournisseurs de service et des utilisateurs. Selon lui, pour donner les meilleurs résultats, les lignes directrices de l'ENC doivent être complétées par la fourniture et la diffusion de capacités de filtrage de type PICS. A ce jour, plus de 20 000 utilisateurs japonais ont téléchargé des logiciels de filtrage PICS. Parallèlement à ses efforts en vue de promouvoir des systèmes de classification par un tiers ou d'auto-classification, l'ENC a invité les enseignants et les parents à contribuer à l'établissement de systèmes de classification et à encourager l'utilisation de logiciels de filtrage. Les approches technologiques présentent certaines lacunes qui peuvent être comblées par une participation des utilisateurs. M. Kokubu décrit le système du bureau japonais de labélisation chargé de promouvoir un système de classification des pages Web japonaises à utiliser en combinaison avec un logiciel de filtrage. Pour conclure, il présente les futurs travaux de l'ENC, notamment "le projet de connexion de 100 écoles" à l'Internet, la mise au point de plusieurs systèmes de classification et bureaux de labélisation et la coopération avec les travaux de normalisation menés au plan international. *(Documentation présentée : diapositives)*

Don SANDFORD de *Net Shepherd* présente les activités de sa société qui propose des outils et services permettant aux utilisateurs d'autoréguler l'usage d'Internet. M. Sandford présente dix principes de base observés par *Net Shepherd*, que les entreprises devraient appliquer pour la mise au point de produits et services de filtrage. L'utilisateur doit être en mesure de pleinement maîtriser ce qu'il fait à l'aide d'outils et services de filtrage simples et accessibles, lui permettant de déterminer le degré de filtrage, l'option "pas de filtrage" étant appliquée par défaut. La censure ne s'impose plus dès lors qu'un choix est possible au niveau de l'utilisateur, celui-ci devant être libre de choisir parmi différentes options, notamment entre différents systèmes de classification personnelle, d'auto-classification ou de classification par un tiers. Les pouvoirs publics devraient encourager l'industrie à développer le plus possible d'options de filtrage. L'intelligence humaine devrait intervenir dans le processus de classification de façon à tenir compte du contexte et à refléter les normes de la collectivité concernée, ce que ne permet pas un indexage automatique, ni un système de blocage par mot-clé. Les utilisateurs d'Internet doivent recevoir des informations positives afin que les technologies de filtrage puissent être utilisées pour arrêter les contenus indésirables mais aussi pour repérer les contenus recherchés. Les entreprises doivent diffuser aux utilisateurs des informations claires et transparentes pour qu'ils puissent choisir leurs services en toute connaissance de cause (en fonction des critères et procédures de classification). Pour assurer le respect de la vie privée, les utilisateurs doivent être informés de la collecte et de l'utilisation des données les concernant. Le fait de passer les commandes aux utilisateurs, d'utiliser des classifications de tiers et de classifier les contenus Internet modifiera les responsabilités potentielles des différentes parties. L'industrie d'Internet doit bien mesurer la portée des lois relatives aux contenus illégaux sur Internet et coopérer avec les autorités chargées d'appliquer les lois dans ce cadre. Des normes sont nécessaires pour faire progresser l'utilisation, le développement économique et l'adoption de la technologie d'Internet.

M. Sandford poursuit en décrivant comment *Net Shepherd* s'est appuyé sur ces dix principes pour se doter d'un avantage comparatif. Depuis décembre 1997, plus de 500 000 sites ont été classifiés par une communauté virtuelle, ce qui a donné naissance à la plus grande base de données proposant des classifications critiques sur Internet. Ce système d'appréciation est à la base du Service *Net Shepherd World Opinion* et permet à *Net Shepherd*, en collaboration avec *Alta Vista Search*, d'opérer des recherches intelligentes filtrées sur Internet. Cette initiative a été proposée pour le *Computerworld Smithsonian Award. (Documentation présentée : notes d'exposé)*

Gordon ROSS, représentant *Net Nanny Ltd*., passe en revue les différentes options de filtrage des contenus sur Internet. Le filtrage est important pour protéger les mineurs, mais il est aussi indispensable de préserver la liberté de parole et de permettre aux différents utilisateurs et organisations de gérer les contenus en fonction de leurs valeurs. Il engage vivement le Forum à étudier si l'accès à Internet doit être complètement libre ou s'il importe de contrôler les contenus et les personnes qui y accèdent. M. Ross explique comment fonctionnent les différentes méthodes de filtrage, notamment la norme "*Platform for Internet Content Selection*" (PICS) (utilisée par *Net Nanny* et *Safe Surf*), les systèmes d'auto-classification, les listes d'adresses de sites Web et les système de filtrage par "mots et phrases".

M. Ross indique les différences entre un filtrage au niveau du Fournisseur d'accès Internet et au niveau du PC et évoque certaines conséquences de chaque méthode. Lorsque le filtrage s'opère au niveau du FAI, ceux-ci sont responsables des contenus illégaux ou indésirables susceptibles de passer, tandis que l'utilisateur n'est pas pleinement habilité à agir et délègue son pouvoir de décisions en matière de contenus. Si le filtrage s'opère au niveau du PC, l'utilisateur contrôle personnellement les contenus filtrés et la responsabilité revient au "propriétaire" du contenu. M. Ross fait valoir les avantages des derniers mécanismes de blocage et de filtrage, notamment leur souplesse et la possibilité de procéder à des contrôle de douane et de vérifier les voies suivies par l'information. Aujourd'hui, le blocage et le filtrage peuvent intervenir au niveau d'un terminal ou d'un serveur, ils peuvent être effectués par le système d'exploitation ou par une application et peuvent s'appliquer aux données entrantes ou sortantes.

Au sujet des inquiétudes actuellement suscitées par Internet, M. Ross rappelle qu'Internet est un outil remarquable et indique que l'éducation pourrait être la clé de bien des problèmes : les responsables des politiques, les parents et les éducateurs doivent se familiariser avec Internet dans le cadre de programmes d'enseignement efficaces présentant les aspects positifs et négatifs d'Internet. Un financement et une formation adéquates devraient être dispensés au personnel chargé d'appliquer les lois. Il constate en outre que le contrôle de l'accès, les mécanismes d'identification et la vérification des voies suivies par l'information peuvent encourager l'usage responsable d'Internet. M. Ross est convaincu qu'il existe aujourd'hui plusieurs solutions techniques susceptibles de régler le problème du contenu sur Internet. *(Documentation présentée : diapositives)*

Susan J. GETGOOD évoque le succès de *Cyber Patrol*, technique de filtrage mise au point par la *Learning Company. Cyber Patrol* repose sur un système de choix donnant aux utilisateurs une meilleure maîtrise. Dans la décision de la Cour suprême des Etats-Unis relative au Communication Decency Act, *Cyber Patrol* a été citée en tant qu'outil de protection des mineurs compatible avec le droit de parole garanti par la loi américaine.

Cyber Patrol donne aux parents et aux enseignants la possibilité d'aménager l'accès à Internet pour chaque enfant, en fonction de son âge et de sa maturité. Le logiciel filtre les contenus Internet figurant sur une liste propriétaire de sites mise à jour constamment : une liste noire de plus de 60 000 sites a été établie d'après un certain nombre de critères notamment la violence, l'intolérance, la représentation de la nudité et la drogue (liste CyberNOT) et également une liste (blanche) de sites recommandés pour les enfants (CyberYES). *Cyber Patrol* peut aussi aider les parents à contrôler combien de temps leurs enfants passent en ligne et empêcher ceux-ci de divulguer par inadvertance des informations personnelles à des étrangers en ligne.

Mme Getgood fait valoir l'avantage unique de *Cyber Patrol* qui permet d'adapter le filtrage aux besoins des différentes communautés. Pour cette raison, *Cyber Patrol* est utilisée dans divers pays et la *Learning Company* lance des versions locales du logiciel dans plusieurs pays d'Europe et d'autres régions du monde. Le logiciel est disponible en plusieurs langues et peut être téléchargé de n'importe où via Internet. *Cyber Patrol* existe désormais en français et en allemand pour les abonnés européens à CompuServe et est proposé par un nombre croissant d'entreprises de télécommunications fournissant l'accès Internet. *(Documentation présentée : notes d'exposé)*

PANEL 4 : Les rôles des pouvoirs publics et du secteur privé dans l'autorégulation - quelles sont les conditions d'une autorégulation réussie ?

Peter UPTON, de l'*Australian Information Industry Association* (AIIA) préside les quatre séances qui réunissent des représentants de fournisseurs d'accès Internet et de groupes de consommateurs, ainsi qu'un représentant de la police spécialiste des problèmes d'Internet.

Markku ROPPONEN représente l'Association des fournisseurs finlandais de services Internet (ISPA Finlande), association professionnelle créée en décembre 1997 pour promouvoir la coopération entre les FSI concernant les problèmes juridiques et l'autorégulation du secteur. S'agissant de la répartition des responsabilités entre les divers acteurs d'Internet, ISPA Finlande se fonde sur les résultats d'un projet mené récemment par le Ministère des transports et des communications de la Finlande afin d'identifier et de définir les acteurs intervenant dans la chaîne de distribution de l'information, du fournisseur à l'utilisateur final, ainsi que leurs droits et responsabilités relatifs aux contenus publiés en ligne. Aux fins de la régulation du réseau public de communications, ISPA Finlande propose d'établir une distinction entre les "communications publiques personnelles" (par exemple, services d'information) et la distribution de contenus (par exemple, vidéo à la demande). En vertu de la loi finlandaise, la responsabilité du contenu dépend de la connaissance du contenu par l'acteur. En conséquence, la responsabilité en matière de

contenu varie en fonction du rôle joué dans la chaîne de distribution de l'information ; par exemple, s'agissant des communications publiques personnelles, les utilisateurs sont responsables du contenu de leurs communications, alors que les transporteurs qui n'ont ni créé le contenu, ni décidé de sa livraison ou de sa publication ne sont pas responsables.

Selon M. Ropponen, la séparation entre l'autorégulation et la régulation du contenu sur Internet doit être revue ; il évoque certains problèmes techniques et juridiques posés par l'autorégulation de l'industrie dans ce domaine. Selon lui, si l'on veut limiter la diffusion de documents préjudiciables et criminels sur le réseau, un cadre juridique doit être mis en place pour appuyer l'industrie d'Internet. Certains acteurs ne sont pas en mesure, ni techniquement, ni juridiquement, de bloquer certains contenus. Pour donner de bons résultats, l'autorégulation doit tenir compte du rôle de chaque acteur et s'inscrire dans un cadre défini par les autorités. Les FSI doivent réfléchir pour définir les contenus acceptables et inacceptables, sensibiliser les parents aux aspects positifs et négatifs d'Internet, promouvoir la coopération internationale pour trouver des solutions et soutenir les activités de la police, notamment les lignes directes. *(Documentation présentée : notes d'exposé)*

Fred EISNER, de l'Association des fournisseurs néerlandais de services Internet, passe en revue les conditions nécessaires au bon fonctionnement de l'autorégulation d'Internet et évoque l'expérience des Pays-Bas dans ce domaine. Il constate qu'il ne faut pas confondre le secteur de l'information qui s'occupe des contenus et celui des fournisseurs de services Internet qui se charge essentiellement d'acheminer des flux d'informations et d'assurer la bonne marche du trafic Internet. A l'heure actuelle aux Pays-Bas, les FSI ne sont pas responsables des contenus tiers qu'ils acheminent ; les Pays-Bas attachent en effet une grande importance à la liberté de parole et d'expression et toute censure préalable est interdite. D'autre part, il serait pour un FSI techniquement impossible, ou disproportionné, par rapport au but recherché, de contrôler chaque élément d'information véhiculé sur le réseau, et une telle responsabilité ne ferait que freiner la croissance d'Internet et empêcher le progrès technique. Le FSI peut être toutefois tenu pour responsable d'un contenu dans un cas : lorsqu'il sait qu'un contenu illégal se trouve sur son système. Un service de police est chargé de repérer et de poursuivre les contrevenants et les FSI sont tenus de l'aider si nécessaire. En dépit de cette situation, M. Eisner constate qu'aux Pays-Bas, les FSI se sentent socialement et moralement responsables et font tout leur possible pour limiter au maximum la diffusion de contenus illégaux et préjudiciables et pour protéger les mineurs et la dignité humaine. Cependant, même s'ils sont appelés à coopérer avec la police, les FSI doivent également respecter la loi : ainsi, ils ne peuvent pas communiquer de noms ni d'adresses sans injonction des tribunaux.

Pour illustrer une initiative d'autorégulation réussie, M. Eisner cite l'exemple de la *hotline* créée aux Pays-Bas pour répondre à l'inquiétude du public face à la pornographie mettant en scène des enfants sur Internet. Les FSI, les citoyens intéressés et la police ont décidé d'un commun accord qu'une autorité neutre devait être mise en place pour recevoir les messages relatifs aux contenus illégaux sur Internet. Cette ligne permanente a été établie dans le cadre d'un partenariat public/privé, structure bien adaptée à la culture néerlandaise, et applique les mêmes procédures que les autres secteurs. Les diverses parties intéressées ont appris à collaborer, à mettre en commun l'information et à contribuer à la mise en place d'une ligne directe efficace et performante. Toutefois, certaines questions doivent encore être réglées, notamment en ce qui concerne le financement de la ligne directe, la poursuite des contrevenants (l'expérience dans ce domaine est insuffisante, il n'existe pas de personnel spécialisé ni de priorités clairement définies) et le traitement des différends au plan national et international. M. Eisner indique que, selon lui, ce type d'autorégulation dans le cadre d'un partenariat public/privé offre la meilleure solution pour traiter les problèmes de contenus, mais il note que la mise en oeuvre d'un tel système exige des concessions de toutes les parties en présence. *(Documentation présentée : notes d'exposé)*

James R. SAVARY de l'Association des consommateurs du Canada présente le point de vue des consommateurs sur l'autorégulation, à la lumière de l'expérience canadienne. Selon lui, le problème des

contenus est le type même de problème susceptible d'être résolu par un système d'autorégulation ; pour illustrer ses propos, il cite la norme nationale canadienne sur la protection de la vie privée mise au point d'un commun accord dans le cadre d'un processus d'autorégulation. Les préoccupations prioritaires des utilisateurs d'Internet concernent actuellement la fiabilité des transactions électroniques, la protection de la vie privée et la sécurité. Les problèmes de contenus illégaux ou choquants n'arrivent qu'après, parce qu'ils suscitent des réactions plus contrastées, opposant ceux qui privilégient la liberté d'expression à ceux qui pensent que les utilisateurs, notamment les mineurs, doivent être protégés contre les contenus préjudiciables. La norme nationale canadienne sur la protection de la vie privée constitue néanmoins un modèle d'autorégulation mis au point par les différentes parties intéressées et adopté comme norme nationale, et peut servir de point de départ à une coopération internationale.

M. Savary énonce plusieurs principes importants qui devraient guider les initiatives d'autorégulation. Il est capital de parvenir à un consensus entre toutes les parties concernées intervenant dans le débat, y compris les pouvoirs publics. M. Savary constate que contrairement aux problèmes de protection de la vie privée, il ne devrait pas y avoir de "défaillance du marché" : en effet, les utilisateurs savent généralement qu'ils sont en présence d'un contenu illégal alors que leur droit à la protection de la vie privé peut être violé à leur insu. Ce type de démarche autorégulatrice rend bien moins nécessaire une intervention des pouvoirs publics, mais elle exige des utilisateurs d'adhérer à l'esprit et à la lettre de la norme. Un tel code ne peut fonctionner qu'avec la participation de tous les acteurs. L'adoption de ce code devrait en outre être obligatoire et des sanctions prévues en cas de non-respect ; il reste cependant à préciser quelles seront ces sanctions. Il fait remarquer que le marché favorisera la mise en conformité, la question des contenus étant subjective et donc propice aux plaintes. Les logiciels de filtrage employés par les utilisateurs pour opérer leurs propres choix peuvent compléter utilement les normes et codes de conduite. M. Savary conclut que les codes d'autorégulation conformes aux normes internationales, conjugués aux technologies-utilisateur apparaissent comme la solution idéale, puisqu'ils assurent une souplesse maximale pour l'industrie et la protection des consommateurs ainsi habilités à mieux maîtriser leurs choix. *(Documentation présentée : diapositives)*

Christophe SAPET représente l'Association des fournisseurs d'accès à des services en ligne et à Internet (AFA). M. Sapet constate tout d'abord que le rôle des pouvoirs publics et du secteur privé n'a pas changé avec l'apparition d'Internet ; Internet n'est qu'un nouvel espace que les secteurs public et privé doivent apprendre à gérer de conserve. Internet est un moyen de communication novateur, mondial et interactif qui permet à quiconque de diffuser des contenus, c'est pourquoi la question des contenus pose de nouveaux défis. Il constate une certaine confusion concernant le sens de l'"autorégulation" dans le cas d'Internet. Du point de vue de l'AFA, l'autorégulation ne remet pas en cause la compétence des autorités réglementaires et juridiques mais fixe le rôle du secteur privé dans la gestion de l'espace où se déroulent ses activités. Dans ce cadre, l'AFA jouera un rôle consultatif et informatif pour aider le gouvernement à établir les normes qui seront appliquées par le secteur privé.

M. Sapet met l'accent sur trois aspects particuliers d'Internet qui posent des problèmes au niveau de la réglementation et de l'action des pouvoirs publics, à savoir le fait que la distribution des données soit instantanée, qu'Internet soit en perpétuel développement et qu'il ait une dimension mondiale. Pour lutter contre la diffusion de contenus préjudiciables, l'AFA préconise la création de lignes directes assorties de mécanismes de réaction rapides et souples. Des organes consultatifs représentatifs spécialisés dans l'Internet pourraient participer à l'élaboration des lois en conseillant les législateurs au sujet de l'évolution rapide et des tendances futures des technologies Internet. Enfin, les questions difficiles liées à la nature du réseau Internet pourraient être résolues plus facilement grâce à une coordination internationale. Pour conclure, M. Sapet indique que l'AFA entend poursuivre son action dans ce domaine en réunissant les acteurs de l'Internet, en collaborant avec les pouvoirs publics et en oeuvrant au lancement d'une *hotline* et d'initiatives de consultation. *(Documentation présentée : notes d'exposé)*

Le dernier intervenant, **Guy VERBEEREN** de la Police Judiciaire belge (Département des enquête judiciaires) évoque les activités menées par la Belgique pour combattre la pornographie impliquant des enfants sur Internet. Les événements tragiques survenus en Belgique en 1996 ont entraîné la création du *Child Pornography Internet Contact Point*, service-relais officiel pour les questions de pornographie impliquant des enfants, administré par le *National Computer Crime Unit* (NCCU). Le NCCU mène aussi des recherches pour repérer la pornographie mettant en scène des enfants sur Internet et à la demande d'autres unités de la Police Judiciaire, fournit une assistance technique pour localiser et identifier les responsables. Ce site-relais permet au public de communiquer à la police des informations sur la pornographie impliquant des enfants.

Dans la législation belge, la diffusion de pornographie par quelque media que ce soit est un fait répréhensible. La législation a été étendue pour couvrir la diffusion ou la possession de pornographie impliquant des enfants, sans précision du type de média ou de la technologie utilisée, c'est à dire qu'elle s'applique aux réseaux informatiques, aux disques durs ou tout autre support électronique ou optique, et donc à Internet et aux technologies numériques. En pratique, la diffusion de pornographie impliquant des enfants via toute application Internet, notamment par courrier électronique, via des groupes de discussion, l'IRC ou sur le *World Wide Web*, tombe actuellement sous le coup de la loi belge.

En passant par l'adresse électronique centrale de la Police Judiciaire, le public peut communiquer, dans sa propre langue, au NCCU des informations concernant la pornographie mettant en scène des enfants. En 1997, environ 2 000 messages ou informations ont été reçus, mais seulement cinq ont entraîné des enquêtes ou des arrestations, à l'étranger et en Belgique. En 1998, deux enquêtes ont été engagées. Lorsqu'un message contient des informations pertinentes et sérieuses concernant un contenu illégal sur un site étranger, il est transmis aux autorités compétentes du pays concerné. Le service reçoit aussi occasionnellement des messages concernant d'autres délits, notamment pour signaler des cas de "spamming" ou de "pyramides", en quels cas le message est également transmis aux autorités compétentes. M. Verbeeren note que dans le cadre de cette initiative, la police belge a eu de bonnes relations de coopération avec les FSI concernés.

Pour clore la séance, M. Verbeeren récapitule comment, selon lui, ces problèmes pourraient être résolus de façon satisfaisante. Les autorités doivent fixer, à l'intention des acteurs d'Internet, un cadre juridique clair et les fournisseurs de services doivent collaborer pour assurer la sécurité de leur média. S'agissant de la protection des enfants, les responsabilités doivent être partagées entre les services de police, les FSI et les personnes plus directement responsables des enfants comme les parents et les enseignants. Par exemple, il revient aux parents d'utiliser des techniques de filtrage et des mots de passe pour protéger leurs enfants contre les contenus illégaux et préjudiciables sur Internet. Cela dit, il faut également veiller à ne pas complètement limiter l'accès des enfants aux ressources éducatives de qualité disponibles sur Internet. *(Documentation présentée : notes d'exposé)*

PANEL 5 : Discussion générale

En ouvrant la séance finale, **Maria LIVANOS CATTAUI** de la Chambre Internationale de Commerce (CIC) souligne l'opportunité de ce Forum compte tenu de l'évolution de la technologie et du commerce électronique. Elle prend note de la Conférence sur le "Démantèlement des obstacles au commerce électronique mondial" tenue par l'OCDE en novembre 1997 à Turku, Finlande, et de la réunion ministérielle qui se tiendra à Ottawa, Canada, du 7 au 9 octobre 1998, intitulée "Le commerce électronique : un monde sans frontières : concrétiser le potentiel du commerce électronique mondial". Elle souligne l'importance de l'éducation pour promouvoir l'utilisation des technologies de réseau et mieux faire connaître les avantages offerts par Internet.

Michael BAKER représente *Electronic Frontiers Australia* (EFA) qui est membre de la *Global Internet Liberty Campaign* (GILC). M. Baker rappelle tout d'abord aux participants qu'Internet constitue un formidable nouvel outil de communication ; que ce n'est pas seulement une industrie, ni un simple outil de développement du commerce électronique et que tous les contenus Internet ne sont pas commerciaux. A l'heure actuelle, la régulation des contenus concerne la régulation des contenus non commerciaux, c'est pourquoi les responsables des politiques doivent veiller à ne pas porter atteinte aux droits des individus. Il est à craindre que le type d'autorégulation préconisé actuellement contraigne les FSI à jouer un rôle coercitif vis à vis des utilisateurs. Il rappelle qu'il est important d'associer tous les utilisateurs finals au processus d'élaboration de mécanismes d'autorégulation. Selon lui, le débat sur les contenus Internet doit tenir compte à la fois de la liberté de parole et de l'intérêt des enfants. M. Baker met en garde contre les faux espoirs placés dans les technologies de filtrage et de blocage car, selon lui, certains de ces outils risquent de ne pas remplir toutes leurs promesses. Il s'interroge sur les initiatives actuelles de classification des fournisseurs de contenus, et pense qu'en proposant ce type de solution, on risque de donner l'illusion de maîtriser le problème. Selon lui, la solution résiderait plutôt dans le renforcement des possibilités de contrôle offertes aux parents et dans l'éducation.

M. Baker évoque la réflexion menée récemment dans ce domaine en Australie. Par exemple, compte tenu de la dimension internationale d'Internet, il pourrait être opportun de revoir les critères utilisés pour déterminer ce qu'est un contenu légal et illégal sur Internet. Il a été proposé d'interdire uniquement les contenus interdits dans tous les pays et d'adopter le terme "illégal-Internet" pour désigner quelque chose qui doit être considéré comme illégal dans le monde entier. La pornographie impliquant des enfants est actuellement le seul contenu entrant dans cette catégorie. S'agissant des autres contenus, M. Baker estime qu'il serait inutile de procéder à des contrôles parce que les contenus censurés réapparaîtraient ailleurs. M. Baker encourage vivement la poursuite du dialogue sur ces questions au plan international et propose d'organiser au cours de l'année prochaine des débats spécifiques associant un plus grand nombre de FSI, de militants et d'utilisateurs.

David KERR de l'*Internet Watch Foundation* (IWF) rappelle comment l'IWF a été créé il y a 18 mois lorsque les autorités britanniques ont décidé de poursuivre des FSI pour diffusion de contenus préjudiciables et illégaux. A l'issue d'un très large débat, il a été décidé d'un commun accord de traiter les problèmes de contenus sur Internet en instaurant un système d'autorégulation et une coopération a été établie entre les autorités policières, le secteur des FSI et les représentants des utilisateurs britanniques. L'IWF offre une forme d'autorégulation dans le cadre de laquelle le secteur s'engage à respecter une série de normes élaborées en concertation avec tous les acteurs, notamment les FSI et la police. En réponse à certaines observations formulées précédemment concernant les mécanismes d'auto-classification, M. Kerr estime qu'il est intéressant de proposer un tel service sur le Web si l'on veut faire approuver un site Web par les parents et en favoriser l'accès pour les enfants. Il fait état des conclusions du comité consultatif d'IWF sur les systèmes d'auto-classification, qui sont disponibles sur le site Web d'IWF (http://www.iwf.org/uk).

L'IWF est favorable à la formation de partenariats au plan international et prévoit d'étendre ses activités au niveau européen. L'Union européenne a aussi engagé un processus de consultations faisant intervenir les secteurs public et privé. Les initiatives d'autorégulation, telles que les lignes directes, seront financées conjointement par l'Union européenne et l'industrie. M. Kerr reconnaît le rôle important joué par l'OCDE qui offre un lieu de dialogue unique pour l'examen des problèmes relatifs aux contenus au plan international et encourage vivement la poursuite de débats ciblés de ce type. *(Documents présentée : notes d'exposé)*

David W. PHILLIPS d'AOL Bertelsmann Online, Europe, commence son exposé en évoquant ce qu'il considère comme les grands atouts d'Internet et ce qui le distingue des média traditionnels : le réseau mondial est interactif, interdépendant et ouvert. Sa nature interactive apparaît dans le fait que le

contenu Internet est généralement sélectionné par les utilisateurs (il est appelé et non imposé) et n'importe qui peut fournir des contenus très divers à différents niveaux. De ce fait, les technologies axées sur l'utilisateur et les "courtiers d'informations" tiers peuvent jouer un rôle important dans la gestion des contenus Internet. La force du *World Wide Web* réside dans les liens entre différents sites, indépendamment de leur localisation physique ; cette dimension mondiale fait que le réseau est interdépendant et limite la capacité de réglementation des gouvernements. Enfin, l'ubiquité et l'ouverture d'Internet le distinguent des média plus traditionnels comme le téléphone et la radiodiffusion, c'est pourquoi les régimes réglementaires appliqués aux secteurs des télécommunications et de la radiodiffusion ne peuvent lui convenir.

Compte tenu de ces caractéristiques d'Internet, différents modèles de réglementation doivent être envisagés. Les principales options considérées actuellement sont le modèle marchand, l'autorégulation et la réglementation gouvernementale. De l'avis de M. Phillips, le modèle marché, dans lequel on considère que la confiance du consommateur est nécessaire pour maintenir la relation avec les clients, ne fonctionne pas toujours. Dans un environnement concurrentiel de libre circulation des flux d'informations, les consommateurs ont plus de choix et, partant, un plus grand pouvoir de négociation. Pour ce qui est de la réglementation par les pouvoirs publics, à ce stade du développement d'Internet, il serait prématuré d'imposer des réglementations gouvernementales rigides, car elles pourraient freiner le progrès technologique. Autre inconvénient de cette option, les gouvernements n'ont pas les moyens de veiller à l'application ni d'assurer le respect des réglementations. De plus, il peut arriver que les lois des pays empiètent les unes sur les autres et soient incompatibles. M. Phillips maintient que le système de réglementation gouvernementale ne doit intervenir qu'en cas de défaillance du marché et en l'absence d'autorégulation pertinente. Il constate que l'autorégulation ne se réduit pas uniquement à des codes de conduite et qu'elle présente trois aspects importants : législatif, adjudicatif et réglementaire. L'un des grands avantages de l'autorégulation est qu'elle met à profit l'expérience de l'industrie et tient compte de l'évolution rapide de ce secteur.

Pour conclure, M. Phillips indique que la meilleure façon de régler les problèmes de contenus sur Internet est de conjuguer les trois modèles. Il engage les responsables des politiques à favoriser la concurrence et la transparence dans l'élaboration de leurs choix et les invite à repérer les cas d'échec du marché et d'inadéquation de l'autorégulation. Les lois devraient être précisément ciblées et bien adaptées aux aspects visés ; elles ne devront pas, si possible, susciter plus de problèmes qu'elles n'en résolvent. A l'appui de ces propos, il cite la *Communications Decency Act* des Etats-Unis et la loi allemande sur le multimédia qui offrent deux exemples d'initiatives de réglementation gouvernementales qui ont échoué parce qu'elles étaient trop générales et ne donnaient pas d'orientations concrètes sur l'application de la loi.

Remarques de clôture des co-présidents

Les deux présidents remercient les organisateurs de la réunion et constatent que l'OCDE et le BIAC ont offert un lieu de dialogue utile et permis aux principaux acteurs de l'industrie de rencontrer les représentants des pouvoirs publics et d'échanger leurs points de vues et expériences concernant l'autorégulation des contenus illégaux et préjudiciables sur Internet. Ils constatent avec satisfaction que les exposés et les débats ont fait ressortir une convergence de vues sur de nombreux points. Ils perçoivent l'émergence d'un partenariat entre les gouvernements et le secteur privé, à l'initiative de celui-ci, comme un signe encourageant.

La documentation qui suit n’existe qu’en anglais

DOCUMENTS ET SITES WWW DE REFERENCE

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.

BIOGRAPHIES DES INTERVENANTS

Co-Présidents

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.

LISTE DES 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

PRESENTATIONS DES INTERVENANTS

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

Access

- 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)

Employees and Consultants

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