The IT Law newsletter

La lettre du Droit des TIC

The IFCLA is the federation of 15 national IT Law Associations in the World. Created in 1986 to contribute to the development of Computer and Telecommunication Law, it acts as an international forum.

The IFCLA members are happy to transmit you this newsletter. It presents some of the major topics of the IT Law that will be developped at the IFCLA 2008 conference.

L'IFCLA est la fédération de 15 Associations nationales du Droit de l'informatique. Créée en 1986 pour contribuer au développement du Droit des nouvelles technologies, elle agit comme un forum international.

L'IFCLA est heureuse de mettre à votre disposition cette newsletter. Elle présente certaines thématiques majeures du Droit de l'informatique qui seront développées lors de la conférence IFCLA 2008.

DON'T MISS THE
IFCLA 2008 CONFERENCE:
PARIS - June 5th & 6th 2008
IFCLA 2008 Conference
AUTOMOBILE CLUB DE FRANCE
www.ifcla.com

Who are we? the IFCLA Members

Belgian Association for Computer Law

Brazilian Association of Computer and Telecommunication Law (ABDI)
www.abdi.org.br

Canadian IT Law Association (IT/Can)
www.it-can.ca

Danish forum for IT-Law
www.it-retsforum.dk

Finnish IT-Law Association
www.it-oikeus.org

French Association of Computer and Telecommunication Law (AFDIT)
www.afdit.asso.fr

German Association for Law and Information Technology (DGRI)
www.dgri.de

Latin American Institute for High Technology Informatics and Law (ILATID)
www.ilatid.org

Netherlands Association for IT and Law (NVvIR)
www.nvvir.nl

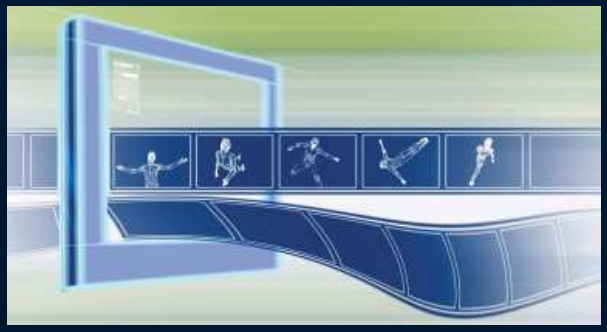
Norwegian Computer and Law Association (NFJE)
www.nfje.no

Portuguese Association for Computers and Law

Swedish Society for Computers and Law
www.adbj.se

Society for Computers and Law (SCL)
www.scl.org

Observers:
ITechLaw – International Technology Law Association
www.itechlaw.org



La conférence sera donnée simultanée simultanément en anglais et en français. Pour télécharger la version française et vous inscrire : www.ifcla.com

Paris, june 5th & 6th, 2008

IFCLA's 2008 Conference

IFCLA

EFE
ÉDITION FORMATION ENTREPRISE
www.efe.fr

IT LAW CHALLENGES

in a changing world: global, virtual, open & outsourced

More than 70 international speakers, renowned IT Law experts

More than 300 attendees coming from all over the World

June, 5th 2008		June, 6th 2008	
Legal norms in a global World: the internet case		Outsourcing of Information Systems: the new governance practices	
Data Protection: what prospects after 30 years of regulation?		Intellectual property and Internet: new issues	
E-commerce and distant selling issues	Should World IT Companies be regulated?	Web 2.0	IT/IP disputes: Mediation & Arbitration
E-commerce: e-money, e-invoices, tax on distant transactions	Software contracts: any move towards customer-oriented contracts?	Media update: new contents and social networking websites	Telecommunication networks and Converging Technologies
Civil and criminal liability of the internet Operators: USA & Europe	Open Source Software: current situation & trends; the GPL licenses	Virtual Reality in the Cyberworld	State monopolies & online gambling update

Our Partners

FIDAL · BIRD & BIRD · Latournerie Wolfrom & Associés, Société d'Avocats · DentonWildeSapte...

Media Partners

Computer Law Review International · CRi · DomainesInfo · Communication Commerce Électronique · Echanges Internationaux · Décideurs Stratégie Finance Droit · Droit & Technologies

With the support of

WIPO Arbitration and Mediation Center · ITechLaw.org International Technology Law Association · ADIJ · AFJE

For more information and to get the detailed program: **www.ifcla.com**

Address from the IFCLA's President

By André Meillassoux(*), BMH Avocats

Dear Colleagues and IT lawyers,

We are happy to send you IFCLA's newsletter, with information on our next Paris Biannual Conference, in June 5 & 6, 2008, with some of IFCLA's history and articles on hot legal issues from some of our speakers.

Our works over the last 2 years to prepare our next Paris conference,

"IT LAW CHALLENGES IN A CHANGING WORLD : GLOBAL, VIRTUAL, OPEN & OUTSOURCED",

have led to the Conference program, which is now available in its latest version (www.ifcla.com).

The conference will present 16 panels on most current legal issues, 80 high profile speakers, 300 awaited attendees from 22 countries.

Personalities from prestigious institutions will be present: French Authorities (Conseil d'Etat, CNIL: the French Data Protection Authority, AFNIC -the ".fr" authority- etc). The French Secretary of State for Human Rights and the new French Secretary of State for the Development of Digital Economy are considering our invitation. Also present: the European Commission; International Organizations like WIPO and ICC; the Academic world ; the industry and major international actors.

Most National and International IT or generalist Law societies, IFCLA's affiliates or sister organizations are active members of the event and send their representatives.

The law practice from different countries, the current presidents of the French Bars Council (CNB) and Paris Bar will also be present, all of them allowing for intellectual exchanges and networking.

We would like you to join us in Paris to enjoy our legal debates and Paris summer season.

(*) Andre Meillassoux is partner at BMH Avocats, Vice President of the French Computer and Telecommunication Law Association (AFDIT) and President of the IFCLA. André has been attorney-at-law since 1983.

Allocution du Président de l'IFCLA

Par André Meillassoux(*), BMH Avocats

Chers Collègues et Confrères Juristes du Droit de l'Informatique,

Nous sommes heureux de vous envoyer la newsletter IFCLA. Elle vous présentera l'IFCLA et sa prochaine conférence biennale qui se tiendra les 5 et 6 juin prochains.

Nos travaux préparatoires débutés il y a deux ans pour donner vie à cet événement,

"LES DEFIS DU DROIT DE L'INFORMATIQUE DANS UN MONDE CHANGEANT: GLOBAL, VIRTUEL OUVERT ET EXTERNALISE"

Ont conduit au programme qui est maintenant disponible dans sa version aboutie.

La conférence présentera 16 panels sur la plupart des questions juridiques actuelles animées par 80 intervenants prestigieux et devant 300 participants.

Des personnalités représentant de prestigieuses institutions seront présentes: les Autorités françaises (Conseil d'Etat, CNIL, AFNIC etc.). Le Secrétaire d'Etat aux Droits de l'Homme et le Secrétaire d'Etat chargé de la Prospective, de l'Evaluation des politiques publiques et du Développement de l'économie numérique ont également été conviés. La Commission européenne, des Organisations internationales comme l'OMPI et la CCI, des Universitaires et des représentants d'acteurs majeurs de l'industrie seront également présents.

La plupart des associations nationales et internationales affiliées à l'IFCLA ont largement contribué à l'élaboration de ce programme et seront représentées lors de la conférence.

La pratique comparée du Droit dans différents pays sera abordée et le Président du Conseil National des Barreaux (CNB) ainsi que le Bâtonnier de Paris seront également présents, contribuant aux riches échanges qui se tiendront à cette occasion.

Nous serions heureux que vous preniez part aux débats qui se dérouleront Place de la Concorde à Paris.

(*) Andre Meillassoux est associé au cabinet BMH Avocats, Vice-Président de l'AFDIT et Président de l'IFCLA. André est avocat au Barreau de Paris depuis 1983.

Many thanks to all the Association Members of the IFCLA and the Actors of the IT Law who contribute to the success of the conference!

IFCLA and its third conference in Paris

By Dinant T.L. Oosterbaan (*)
Oosterbaan Advocaten

On the occasion of IFCLA's 22nd anniversary and its third conference in Paris it is appropriate to start this invitation to attend the IFCLA Paris 2008 conference with an introduction about IFCLA's history and its achievements.
IFCLA, the International Federation of Computer Law Associations, was founded in December 1986 in a meeting in Brussels attended by representatives of the Belgian, French and Dutch Computer Law Associations. At that time there already existed several international groups and associations involved in computer law, including the computer law committees of the IBA and AIJA. The initiators of IFCLA felt that these existing groups had some limitations and that an international federation in which the national computer law associations would be brought together, was a worthwhile initiative. Computer or IT law as a new subject was in the process of establishing its own associations, its own academic institutions and its national and international journals.
At the time of the first IFCLA meeting it was thought that the primary purpose of IFCLA would be to promote international collaboration and exchange of information in computer law in the broadest sense. The members of IFCLA would be national associations and not private persons. As activities the following was suggested. A major international computer law conference would be organized every two years. The conference would be an important event and it was expected that it would continue to attract those active in computer law. The fact that IFCLA is now celebrating its 22nd anniversary demonstrates that this prediction proved to be true.

The years 1987 and 1988 were used to enlarge the IFCLA membership with the following associations: the UK Society for Computers and Law, the German Association for Computers and Law DGRI, the Norwegian Association, the South American Instituto Latino Americano de Alta Technologies, Informatica y Derecho, and IT Law associations from Portugal, Finland, Sweden, Australia, Demark and Brazil.
The Amsterdam 1988 conference was opened by the Minister of Justice of the Netherlands F. Korthals Altes. A total of 115 delegates from 15 countries attended the Amsterdam conference. The conference started the IFCLA tradition of a visit to a museum and a joint dinner of all participants in a special location, in this case Museum van Loon.

In June 1989 the French Computer Law Association AFDI hosted the first "working day" of IFCLA. It was held in the historic Panthéon law school and attracted about 50 delegates. The discussion oriented meeting on National Issues in International Contracts for the Distribution or Edition of Software was held in both French and English, each speaker choosing the language in which he or she was most familiar.
The 1990 conference entitled "Information Technology: Trading with Europe – West and East" took place in Munich and was hosted by DGRI. More than 140 delegates attended. Its major subjects were the proposed EU Software Protection Directive and the opportunities and pitfalls of doing business in Eastern Europe. Not only the quality of the speakers and delegates but also the social aspects confirmed IFCLA's reputation.
The 1992 conference was another highlight. It was organized by the Swedish Law and Informatics Research Institute in cooperation with the Swedish Society for Computers and Law. Although its title "Software Procurement" was limited, the subjects covered were much broader including competition law, conflict resolution and the law of software in a Soviet perspective. For the first time a book of conference papers was published in the Nordic Law and Informatics series. A total of 147 delegates from 16 countries attended.

In 1994 the Society for Computers and Law hosted the IFCLA conference in the world heritage city of Bath, England. The prestigious Assembly Rooms were the conference facilities for the program entitled "Computer Law and Business in the New Europe and Beyond". The subjects covered ranged from developments in information law to data protection and transborder data flows, distribution issues, software piracy and software protection, multimedia and telecommunications regulations and transactions. The reception in the famous Roman Baths and the dinner in the classic Pump Room provided the appropriate facilities for the 184 delegates and the 26 guests from over 22 countries.

The 1996 conference was held in Brussels: "Multimedia and the Internet: Global Challenges for Law". Not only did the conference concentrate on new and groundbreaking issues such as the Information Society, the Internet, convergence and conflicts of laws in cyberspace, it continued the tradition of having interesting social events.

In 1998 the IFCLA conference moved to Norway. The conference "Electronic Commerce: the real trade" concentrated on electronic commerce and included such subjects as Uncitral's rules on electronic signatures, liability of online intermediaries and more general Internet related issues. Three representatives from South America presented developments from their part of the world. In smaller parallel discussion sessions the hot Y2K issue, data protection and intellectual property were discussed. The conference was attended by 125 delegates from 21 countries. The Canadian IT Law Association IT.Can joined IFCLA as a new member.
The 2000 Paris conference "Computer Law in the Millennium Perspective" was another very successful IFCLA conference, held in the prestigious surroundings of the Paris Chamber of Commerce. The organizing committee consisting of Yves Bismuth, Alain Bensoussan, Jérôme Huet, Stéphane Lemarchand and Xavier Linant de Bellefonds did a splendid job. Full autonomy was given to Yves and his French colleagues and all planning meetings were held in French. The very successful Paris conference was held in both French and English with simultaneous translation both ways. Xavier was the general editor of the conference papers published on CD-Rom and in an upon-demand book. In addition to several attendees invited from the French judiciary, the administrative and academic world, there were over 160 delegates from 17 countries. Obviously, in view of the Internet hype the subject focus of the conference had shifted to Internet based subjects, including electronic commerce, websites, intelligent agents, data protection, and national and international regulation of the Internet.

"New Views on Global IT" was the subject of the 2002 conference, hosted by the German Computer Law Society DGRI. Again Internet related subjects played a major role, including cybercrime and cyberspace, rights of security vs. liberties in the online world, privacy, safe harbour, domain names, taxation, implementation of TRIPS and Internet jurisdiction and enforcement. There were also various subjects on new business models, such as ASP, B2B, location-based services and not to forget the effects of new technologies on the protection and exploitation of musical works and other copyright related issues relating to new technologies.
The 2004 IFCLA conference moved for the second time to England. It was hosted again by the Society for Computers and Law, this time in Oxford at Keble College. The program was composed around four main themes: international outsourcing, international technology contracts, data protection and electronic and mobile commerce. Attendance was again from approximately 20 countries with over 130 delegates.

The 2006 IFCLA conference was held in Amsterdam. The interesting program centered around several themes: privacy and data protection, new technologies, ADR, outsourcing, public procurement, new business models for licensing and several internet related issues. Over 100 delegates attended.
To conclude this history it is obvious that IFCLA has been able to attract to its conferences organized every two years a consistent number of international delegates. Many have joined our conferences several times: at the Paris 2008 conference there will be many speakers and delegates who attended prior IFCLA conferences. IFCLA has thus fulfilled its first and most important objective of providing speakers and delegates the opportunity to learn and benefit from an international exchange of ideas and opinions. IFCLA's long term goals have always been and will continue to be exchanges of information, and promotion of harmonization and integration in IFCLA's broad field of interest. All who have participated in the IFCLA conferences as faculty, delegates and organizers have contributed to this interchange of ideas and opinions among international IT lawyers with different ideas, perspectives and experiences in the legal profession. In short, the members of "the IFCLA Community" have contributed to and benefited from the 22 year IFCLA leadership in international IT law conferences. I am sure that the Paris 2008 conference under the leadership of André Meillassoux and the broad based planning group will be another IFCLA success story.

(*) Dinant T.L. Oosterbaan was the IFCLA President between 2004 and 2006

Contrats informatiques : des contrats plus orientés au bénéfice des utilisateurs?

Par Emmanuel CAUVIN,
Juriste d'entreprise

Contrats informatiques : des contrats plus orientés au bénéfice des utilisateur? C'est la question à laquelle la table ronde consacrée aux contrats de logiciel essaiera de répondre. Comparée à d'autres secteurs comme l'industrie de la construction, mon opinion est que le secteur IT est encore dominé par l'Offre. La technologie ainsi que les fonctionnalités sont encore conçues par les fournisseurs informatiques sur la base du chiffre d'affaire qu'ils espèrent en tirer puis protégées par toutes sortes d'outils techniques et juridiques, avant d'être mis sur le marché. Les besoins et les contraintes du client sont pris en compte mais seulement au cours d'une étape ultérieure, dans le contexte des services après-vente ("paramétrage").

Les contrats proposés par les fournisseurs informatiques reflètent cette approche unilatérale. En réalité, le marché ne propose pas de contrat basé sur l'idée de solution. Ce que le marché propose, d'un point de vue contractuel (sans parler des slides des vendeurs…) est toujours une combinaison de deux éléments: produit standard et/ou services.

Produit standard ? Littéralement, un produit standard n'est pas une solution. Les deux termes n'ont pas le même sens. Services ? La fourniture de services est simplement un moyen, pas un résultat. Même avec le mot « informatique », l'expression « services informatiques » reste purement générique.

Il est rare de voir un contrat proposé par une société informatique incluant le mot "solution". Tous les risques sont donc assumés par les clients, ce qui peut paraître assez étrange quand on se rappelle que les clients n'ont pas accès au code source et n'ont aucune influence sur les évolutions futures du logiciel.

D'où vient que dans la plupart des cas les contrats informatiques sont 100% orientés en faveur du fournisseur ? Ne serait-il pas possible d'intégrer les objectifs business du client dans les contrats de licence ? ou dans les contrats de service ? Y a-t-il une alternative à l'approche « c'est à prendre ou à laisser » habituellement adoptée par les fournisseurs informatiques ? Concernant les clauses de responsabilité, pourquoi est-il (presque) impossible de faire en sorte que le fournisseur soit au moins en partie comptable de ses manquements et responsable des dommages causés au client ?

Telles sont quelques unes des questions ouvertes qui seront traitées par un panel d'experts venant de différents pays et de différents métiers.

Software Contracts: any move towards customer-oriented contracts ?

By Emmanuel CAUVIN,
In-house Lawyer

Software Contracts: any move towards customer-oriented contracts ? The Round Table dedicated to Software contracts will try to answer this question. Compared with other sectors such as the construction industry, it is my opinion that the IT sector is still driven by the Offer. The technology and the functionalities are still designed by the IT providers on the basis of the revenue expected and then protected by all kinds of legal and technical tools before being put on the market. Customer's needs and constraints are taken into account but only at a later stage, in the context of after-sales services ("customization").

The contracts proposed by IT suppliers reflect this unilateral approach. As a matter of fact, the market never offers solution-based contracts. What the market offers, contractually speaking (not talking about the slides presented by IT sales men…), is always a mixture of the two following elements: Standard Product and/or Services.

Standard Product ? Literally, a Standard Product is Not a Solution. The two terms do not have the same meaning. Services ? The provision of services is just a mean, not an end-result. Even with the word "IT", "IT Services" remains a purely generic term.

It is really rare to see a contract proposed by an IT Company, with the word "solution" included in it. All risks are thus taken by the customers, which may appear to be rather strange when remembering that the customers have no access to the source code, and no influence on the future updates of the software.

How is it that IT contracts are in most cases 100% vendor-oriented ? Wouldn't it be possible to capture customer's business objectives in Software licenses ? or in services agreements ? Is there any alternative to the "Take it or Leave it" approach usually adopted by IT suppliers ? Concerning liability clauses, why is it (almost) impossible to ensure that the supplier will be at least partly accountable for its own failure and responsible for the damages caused to the customer ?

These are some of the open questions that will be answered to by a panel of experts from various countries and from various backgrounds.

The IFCLA would like to thank its partners on the conference:

L'IFCLA remercie ses partenaires pour la conférence:

Our Partners:

With the support of

Arbitration and Mediation Center
Centre d'arbitrage et de médiation

Media Partners:

Les flux transfrontières de données à caractère personnel : un processeur d'universalité des droits

Par Alain Bensoussan (*)
Alain Bensoussan Avocats

La loi Informatique et libertés constitue le socle des droits de l'homme virtuel. Trente ans après leur élaboration, les principes consacrés en 1978 sont restés pertinents, malgré les mutations profondes des technologies de l'informatique. La France, à travers la directive communautaire 95/46 [1] , a influencé le monde entier. La directive joue en effet, le rôle d'un processeur d'universalité par le biais de la réglementation des flux transfrontières. En imposant une réglementation stricte pour l'exportation des données à caractère personnel hors Union européenne dans les pays n'ayant pas une protection suffisante, ce mécanisme incite ces pays à se doter d'une réglementation organisant un haut niveau d'encadrement des informations nominatives, similaire à celui en vigueur au sein de l'Union européenne. Cette évolution consacre l'entrée d'un droit à la protection des données à caractère personnel au sein des droits fondamentaux en vigueur dans les sociétés démocratiques.

Compte tenu de leur nature, les données à caractère personnel ne peuvent circuler dans des conditions qui ne respecteraient ni la vie privée des personnes concernées ni les libertés et droits fondamentaux auxquels elles peuvent prétendre. D'un autre côté, le développement des communications entraîne la nécessité, pour la plupart des activités, de transférer des données concernant des personnes physiques.

Il existe en effet, de nombreuses situations susceptibles de générer des transferts internationaux de données et dont il faut tenir compte lors de la déclaration de traitement et lors de son exploitation. Ainsi des entreprises françaises qui communiquent avec des partenaires, des sociétés filiales ou mères ou qui ont des activités situées hors de l'Union européenne sont des situations dans lesquelles se produiront des transferts internationaux de données à caractère personnel. De même, la centralisation intra-groupe de la base de données de gestion des commandes et de la comptabilité clients, la centralisation intra-groupe de la base de données de gestion des ressources humaines d'un groupe multinational, la délocalisation de centres d'appel et le transfert le fichier correspondant pour démarchage ou qualification ou le recours à des systèmes internationaux de maintenance informatique constituent autant de situations qui entraîneront des transferts de données à caractère personnel hors des frontières communautaires.

Les transferts de données à caractère personnel vers des pays non membres de l'Union européenne sont soumis à des formalités particulières [2] . La loi Informatique et libertés a en effet introduit des règles précises pour encadrer de tels transferts notamment lorsque les pays tiers n'ont pas un niveau suffisant de protection de la vie privée, des libertés et des droits fondamentaux.

Ces règles sont issues de la directive européenne du 24 octobre 1995 et prévoient que tout transfert vers un pays extérieur à la Communauté européenne est interdit si ce pays n'assure pas un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard des traitements dont ces données font l'objet.

La Commission européenne a établi une liste des pays accordant une protection adéquate. Il s'agit des vingt-cinq pays de l'Union européenne, des pays membres de l'Espace Economique Européen (Islande, Liechtenstein, Norvège), des pays ayant fait l'objet d'une reconnaissance de protection adéquate (Argentine, Canada, Guernesey, Ile de Man, Suisse, entreprises américaines adhérentes au Safe Harbor). En ce qui concerne plus particulièrement les Etats-Unis, un accord a été négocié avec la Commission européenne [3].

Pour ces pays, la Cnil n'a pas à autoriser les transferts dans la mesure où les données à caractère personnel font l'objet d'une protection adéquate. L'existence de tels transferts est gérée dans le cadre des formalités préalables déclarations ou autorisations.

En ce qui concerne les pays tiers n'ayant pas une protection suffisante, l'opération de transfert n'est possible que dans la mesure où s'applique l'une des dérogations définies de manière restrictive à l'article 69 de la loi du 6 janvier 1978 (consentement de la personne concernée, sauvegarde de la vie de la personne ou de l'intérêt public, etc.). Si l'opération n'entre dans aucune de ces dérogations, le transfert ne pourra être effectué que sur la base d'une autorisation de la Cnil, laquelle s'obtient en encadrant le flux d'échanges par une convention de flux transfrontières ou des règles internes.

La Commission européenne a élaboré des clauses contractuelles type offrant des garanties adéquates au regard de la vie privée et des libertés et droits fondamentaux des personnes, qui peuvent être reprises dans une convention de flux transfrontières ou dans des règles internes d'entreprise. Elle a par ailleurs publié trois conventions types. Deux de ces conventions concernent les flux entre deux responsables du traitement pour l'exploitation des données à caractère personnel, la troisième organise les relations entre le responsable du traitement et un sous-traitant.

(*) Alain Bensoussan est le fondateur du cabinet éponyme créée en 1978, date à laquelle la première loi garantissant les droits de l'individu face aux développements de l'informatique a vu le jour. Alain Bensoussan assiste de grandes entreprises dans la mise en place de leur politique en matière de technologie et libertés. Il est co-fondateur de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP), l'auteur d'un ouvrage intitulé « Informatique et libertés », paru en février 2008 aux éditions Francis Lefebvre.

[1] Directive CE 95/46/CE du 24/10/1995.
[2] Pour une étude, cf. « Informatique et libertés », éd. Francis Lefebvre 2008.
[3] Décision 2000/520/CE du 26-7-2000.

Cross-border flows of personal data: a catalyst for univeral rights

By Alain Bensoussan (*)
Alain Bensoussan Avocats

The French Data Protection Act is the bedrock of the digital human rights. Thirty years after their elaboration, its principles established in 1978 continue to be relevant today despite the profound changes that have taken place in computer technology during the same period. France, through Community Directive 95/46 [1], has influenced the whole world. The Directive regulating cross-border flows has had a ripple effect and promoted the spread of universal rights. Its tough regulations on the export of data from the European Union to countries not providing sufficient protection encourage these countries to follow suit and adopt laws and regulations establishing a high level of protection for personal data similar to the one adopted within the EU. This change definitely establishes a right to the protection of personal data among the fundamental rights applicable within democratic societies.

Because of their nature, personal data cannot be transferred in conditions that would not respect the privacy or fundamental rights and freedoms of data subjects. On the other hand, nowadays the development of communications makes it necessary for most businesses to transfer data about individuals.

There are a number of situations in which international transfers of data occur. For example when a French company communicates with partners, subsidiaries or parent companies located outside the European Union or performs activities outside the European Union. Similarly, when a multinational corporate group centralizes its order management, accounts receivable or human resources databases or when a company uses the services of a foreign call center or computer maintenance specialist, this implies the transfer of personal data beyond the borders of the European Union.

Transfers of personal data to countries not belonging to the European Union are subject to special requirements [2]. The French Data Protection Act has established specific rules to regulate such transfers, in particular where the non-EU recipient countries have not a sufficient level of protection of the privacy and fundamental rights and freedoms of individuals.

According to these rules, modeled on the principles embodied in the European Directive dated October 24, 1995, no data transfer may be made to a country outside the EU if such country does not ensure a sufficient level of protection of the privacy and fundamental rights and freedoms of the individuals with regard to the processing of their data.

The European Commission has established a list of countries providing adequate protection. Such list includes the twenty-five Member States of the European Union, the member countries of the European Economic Area (Iceland, Liechtenstein, Norway) and countries recognized as providing adequate protection (Argentina, Canada, Guernsey, Isle of Man, Switzerland, US companies adhering to the Safe Harbor). Concerning more particularly the United States, an agreement has been signed with the European Commission [3].

Transfers of personal data to countries providing an adequate level of protection do not have to be authorized by the French Data Protection Authority, the CNIL. The existence of such transfers should nonetheless be notified when carrying out the prior formalities, notifications or authorizations required for the data processing.

In contrast, transfers of personal data to non-EU countries not providing sufficient protection are possible only in the situations strictly listed in Section 69 of the French Data Protection Act of January 6, 1978 (consent of the data subject, protection of the data subject's life, protection of the public interest, etc.). If none of these limited exemptions apply, the transfer cannot be made without the authorization of the CNIL. Such authorization is granted subject to the adoption of a transborder data flow agreement or binding corporate rules offering adequate safeguards.

The European Commission has approved standard contractual clauses offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals, which may be incorporated into transborder data flow agreements or binding corporate rules. It has also published three model contracts. Two of these model contracts concern transfers between data controllers and one concerns transfers between a data controller and a data processor.

(*) Alain Bensoussan is the founder of the eponymous law firm established in 1978, year on which the first law protecting the rights of individuals against the developments of information technology was passed. Alain Bensoussan advises and assists large companies in implementing their IT and privacy policies. He is the co-founder of the French Association of Data Protection Officers (AFCDP) and the author of the book "Informatique et libertés" published in February 2008 (Editions Francis Lefebvre).

[1] Directive EC 95/46/EC dated 10/24/1995.
[2] For further information, see "Informatique et libertés", Ed. Francis Lefebvre 2008.
[3] Decision 2000/520/EC dated 07/26/2000.

Les flux transfrontières de données à caractère personnel : un processeur d'universalité des droits (suite)

Les règles internes constituent pour les groupes de sociétés une alternative à la convention de flux transfrontières. En effet, les règles internes adoptées de manière unilatérale par la direction du groupe, évitent de conclure autant de contrats qu'il existe de transferts de données en son sein. En outre, la Cnil, en tant qu'autorité de coordination, se charge de soumettre les règles internes à l'appréciation des autres autorités européennes de contrôle et de relayer leurs commentaires.

Cross-border flows of personal data: a catalyst for univeral rights (continuation)

For corporate groups, binding corporate rules ("BCR") are an alternative to transborder data flow agreements. Binding corporate rules adopted unilaterally by the group headquarters avoid entering into an agreement for each data transfer made within the group. Furthermore, the CNIL, as the coordination authority, will be in charge of transmitting theses rules to the other European supervisory authorities concerned for evaluation and comments.

Bankruptcy & Insolvency Risks in Outsourcing Transactions: A Wake-Up Call

By John Beardwood, Attorney-at-law (*)
Fasken Martineau DuMoulin LLP

The following is a brief excerpt of a more comprehensive paper which will be presented at the IFCLA Conference (Paris, 2008).

1. Introduction

In today's unsettled markets, outsourcing practitioners have needed to become increasingly focused on how to structure their outsourcing arrangements to take account of the circumstance where one of the parties – most significantly, the service provider – has suffered from an event of bankruptcy or insolvency. While the specific effects of the event may vary depending on the nature of the event (e.g. in Canada, whether the party is bankrupt, undergoing a plan of arrangement, or in receivership), the general theme is that in practice such an event in many cases will render moot the carefully crafted language of the outsourcing agreements, even where the agreements expressly contemplate such an event.

This paper focuses on certain elements of a model outsourcing transaction as examples of some of the implications for a customer of the bankruptcy or insolvency of a service provider and suggests methods by which customers can seek to minimise and manage the risks of such events. For the sake of simplicity, and in light of the brevity of this paper, we will use the term "insolvency event" as a general proxy for the different kinds of insolvency events which might occur.

2. Master/Services Agreement: Termination Triggers

It is common for the occurrence of an insolvency event to act as a termination trigger in the master outsourcing agreement and ancillary agreements. For example, a archetypal termination trigger might be drafted as follows:

> If an "Insolvency Proceeding" has been commenced against a Party and an order approving the Insolvency Proceeding is entered, and such Insolvency Proceeding has remained undischarged for period of sixty (60) days or has not been stayed throughout such 60 day period.

In the case of many insolvency events, however, a jurisdiction's insolvency legislation will focus on maintaining the operational activity of the insolvent organization – in this case, the service provider - , which can lead to an effective freeze on the ability of other parties to terminate their contracts with the insolvent entity. As a result, a customer will often be prevented from terminating the outsourcing contract based on the grounds that the service provider has become insolvent. This can present the customer with a challenge. If the customer is fortunate enough to have a termination for convenience provision, it may seek to trigger it, but often the exercise of such a right will be conditional on the customer paying an "early termination fee". Where the customer does not have such a provision of which it can take advantage, the prudent customer will be reluctant to wait for the insolvent provider to start defaulting on its obligations due to a lack of resources.

One possible solution is to draft a "early warning" termination trigger in the master/services agreement is that will allow the customer to terminate the agreement *prior* to, but in anticipation of, the insolvency event. For examplem, such a termination trigger could read as follows:

> If either (i) Moody's Investors Service, Standard & Poors or Dun & Bradstreet lower Provider's credit rating from the rating as of the Effective Date by more than two (2) steps; or (ii) Customer otherwise has reasonable cause to doubt Provider's financial stability (including concerns over Provider's ability to perform its obligations under any Service Schedule consistently and in a sustained manner).

Settling such 'anticipatory' termination provisions raise its own challenges. Not all providers have been formally rated by credit agencies, and providers will object to less objective tests. However, having appropriate termination triggers is important since outsourcing agreements may otherwise contain significant early termination penalties for customers. For example, one study has noted that customers who used WorldCom as their service provider prior to its bankruptcy had penalties as high as half the costs of remaining with the contract, and only around 20% of customers were able to terminate their agreements cost-free with WorldCom in the event that WorldCom's financial ability feel below a certain level[1].

3. Master/Services Agreement: Provision of and Payment for Transition Services

Those provisions of outsourcing agreements which require that the provider provide certain post-termination/expiration transitional services form an important component of an outsourcing agreement. Conceptually, transition services could be said to have two elements: (a) the provision of 'ordinary course' services (e.g. in the case of an outsourcing of technology services, the provision of desktop computing services, or help desk services); and (b) the provision of 'special' transition services, the focus of which is on knowledge transfer and consulting services from the provider. In the case where the customer is seeking to terminate the agreement based on the material breach of the service provider, the customer may argue that as one means of seeking to mitigate its damages it should not need to pay for these transition services, particularly these 'special' transition services.

However, if the customer manages to successfully argue that it should also not have to pay for 'special' transition services in the case of an insolvency event, the customer may have won the battle but lost the war. More specifically, where the service provider suffers an insolvency event, the trustee in bankruptcy (or depending the nature of the insolvency event, their equivalent) will be unlikely to agree to perform the requires services where there is no compensatory revenue which accompanies such an obligation to perform. In short, the absence of a requirement to pay fees for the provision of transition assistance could very well increase the likelihood that the trustee will disclaim the transition services performance obligation. As such, in the case of an insolvency event, it appears beneficial for the customer to agree in the outsourcing agreement to pay the service provider for the provision of the transition services.

4. Other Issues

Other issues which the customer's counsel will also need to examine, in thecontext of each insolvency event, are:

(a)the extent to which a trustee in bankruptcy, or its equivalent, can disclaim a customer's right to use any licensed IP;

(b) challenges to the effective operation of an escrow agreement in the case of an insolvency event;

(c) how to address employees post-termination/expiration;

(d) if the customer so wishes, how to repurchase assets from the supplier; and

(e) if the customer so wishes, how to repurchase/re-lease real estate using in the outsourcing arrangement, from the supplier; and

(e) the role of parental guarantees, performance bonds and other measures in mitigating the risks of provider bankruptcy.

5. Conclusion

As we note above, this article is only a brief excerpt from a more comprehensive, forthcoming paper which will review each of the above issues in detail. However, the excerpt nevertheless serves to reemphasize the importance of the outsourcing practitioner's much stated refrain that the parties should spend just as much time focusing on the issues where the outsourcing transaction goes wrong, as they do focusing on the issues where the transaction goes right.

[1] Ann H. Spiotto & James E. Spiotto, "The Ultimate Downside of Outsourcing: Bankruptcy of the Service Provider" (2003) 11 Am. Bankr. Inst. L. Rev. 47 at 62.

(*) John P. Beardwood is a partner with the law firm of Fasken Martineau DuMoulin LLP, practicing in the Toronto office. John is engaged in a corporate/commercial practice, with an emphasis on outsourcing, information technology and privacy law related matters. John is listed among the world's pre-eminent Internet and e-commerce lawyers in Who's Who Legal - The International Who's Who of Business Lawyers. He is recognized in The Best Lawyers in Canada in information technology law and is 'highly recommended' as a leading outsourcing practitioner in the PLC Which lawyer? Yearbook 2008 and in the PLC Outsourcing Handbook. John is co-editor and contributing author of the industry-leading text Outsourcing Transactions: A Practical Guide, now in its 3rd Edition.

Monopoles d'Etat et Jeux d'Argent en Ligne
Les Jeux sont-il faits ?

Par Michel Béjot et Caroline Bouvier [1]
Bernard – Hertz – Béjot, Paris

*Le marché mondial des jeux d'argent en ligne a généré en 2003 un chiffre d'affaire annuel brut d'environ 5,7 milliards d'euros, la part du marché européen représentant environ 1,63 milliards d'euros. En 2010, ce chiffre mondial devrait atteindre environ 16,26 milliards d'euros (25 milliards de dollars).**[2]***

Les jeux d'argent - La notion de « *jeux d'argent* » peut être diversement appréciée selon les pays.

Au niveau européen, il peut être utile de se reporter à la définition des jeux d'argent contenue dans la directive du 8 juin 2000 qui dispose « *que l'exclusion des jeux d'argent couvre uniquement les jeux de hasard, les loteries et les transactions portant sur les paris, qui supposent des enjeux de valeur monétaire*».[3]
Ainsi, la notion de jeux d'argent ne couvre pas « *les concours ou jeux promotionnels qui ont pour but d'encourager la vente de biens ou de services et pour lesquels les paiements, s'ils ont lieu, ne servent qu'à acquérir les biens ou les services en promotion* ».
La directive européenne du 12 décembre 2006 reprend la même définition des jeux d'argent.[4]
Il est à noter que l'exclusion des jeux d'argent du champ d'application de ces directives tient compte « *de la spécificité de ces activités qui entraînent de la part des Etats membres la mise en œuvre de politiques touchant à l'ordre public visant à protéger le consommateur* ». [5]
L'étude effectuée par l'Institut suisse de droit comparé sur les services des jeux d'argent au sein de l'Union Européenne distingue également (**i**) les services de jeux d'argent et (**ii**) les jeux promotionnels les premiers étant définis comme « *tout service, y compris tout service de la société de l'information, impliquant des mises ayant une valeur monétaire dans des jeux de hasard, y compris les loteries et les transactions portant sur des paris* ».[6]

Les jeux d'argent en ligne – L'apparition des nouvelles techniques de communication a élargi considérablement le marché des jeux d'argent et a généré de nouvelles problématiques dépassant le carcan des législations nationales.
Ainsi, comment concilier l'internationalisation des services de jeux d'argent et l'hétérogénéité des législations nationales dans un domaine aussi sensible moralement et économiquement ?

L'Union Européenne face à des conceptions nationales divergentes – Au sein même de l'Union Européenne les législations nationales sont diverses.

Alors que Malte et le Royaume-Uni tentent de concilier l'ouverture du marché des jeux d'argent avec un contrôle des opérateurs, d'autres pays européens ont instauré un régime de monopole sur l'ensemble des segments de jeux (Finlande et Suède, notamment) ; d'autres encore combinent un régime de monopole et d'autorisations (Italie, Allemagne et France, notamment)[7].
La diversité des législations nationales s'explique par la spécificité du secteur des jeux d'argent, d'ailleurs admise tant par certaines directives européennes[8] que par la Cour de Justice des Communautés Européennes (CJCE) dans un arrêt *Schindler* du 24 mars 1994 [9].

La CJCE a ainsi reconnu que les considérations d'ordre moral, religieux ou culturel liées au jeux d'argent justifient que les autorités nationales disposent d'un pouvoir d'appréciation suffisant pour déterminer les exigences que comportent la protection des joueurs, et plus généralement la protection de l'ordre social.

[1] Michel Béjot est avocat associé du cabinet Bernard - Hertz - Béjot. Il peut être joint par e-mail à l'adresse mbejot@bhbfrance.com. Il est membre du comité éditorial du "*Journal of Internet Law*" et préside la section Europe ("*EMEA Region*") de la "*Global Advertising Lawyers Alliance*" (GALA). Il intervient plus particulièrement dans les domaines de compétence suivants : Propriété intellectuelle, Droit de l'informatique, Droit des technologies de l'information et des nouvelles technologies, Droit de la publicité, Droit de la distribution, Fusions et acquisitions, Contentieux international.
Caroline Bouvier est avocat au cabinet Bernard - Hertz - Béjot. Elle est titulaire d'un DEA de Droit Privé (Université de Paris I Sorbonne) et d'un DESS de Droit du Multimédia et de l'Informatique (Université de Paris II Assas). Elle intervient plus particulièrement dans les domaines de compétence suivants : Propriété intellectuelle, Droit de l'informatique, Droit des technologies de l'information et des nouvelles technologies, Droit de la publicité.
Carole Bui, stagiaire, est également remerciée pour sa participation à la préparation de cet article.
[2] "*Study of Gambling in the Internal Market of the European Union*", Rapport final de l'Institut suisse de droit comparé, 14 juin 2006, page xl.
[3] Directive 2000/31 du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (considérant 16 et article 1er paragraphe 5, alinéa d).
[4] Directive 2006/123 du 12 décembre 2006 relative aux services dans le marché intérieur, et plus particulièrement l'article 2, paragraphe 2, alinéa h.
[5] Notamment le considérant 25 de la directive 2006/123 précitée.
[6] "*Study of Gambling in the Internal Market of the European Union*", page V précité op. cit. note 2.
[7] "*Rapport d'information sur le monopole des jeux d'argent au regard des règles communautaires*", Rapport enregistré à la Présidence de l'Assemblée Nationale le 6 février 2008 et présenté par Messieurs Blessig et Myard, p. 30 à 52.
[8] Directives précitées op. cit. notes 3, 4 et 5.
[9] CJCE, 24 mars 1994, Aff. C-275/92, Schindler, Rec. 1994, I p.1039.

State Monopolies and Gambling
Les Jeux sont-ils faits? Is the Betting Closed ?

By Michel Béjot et Caroline Bouvier [1]
Bernard – Hertz – Béjot, Paris

The worldwide online gambling market currently provides a GGR (Gross Gaming Revenue) of about €5,700 million per annum as of 2003, with the EU share being about €1,630 million. Such revenue should reach approximately €16.26 million (US$25,000 million) by 2010.[2]

The "gambling" concept – The definition of *"gambling"* may vary from one country to another.

For the European perspective, one can refer to the definition of gambling activities given by the European directive of June 8, 2000 where it states that *"the exclusion of gambling activities from the scope of application of this Directive covers only games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value".*[3]
Thus, the gambling concept does not cover *"promotional competitions or games where the purpose is to encourage the sale of goods or services and where payments, if they arise, serve only to acquire the promoted goods or services".*
The European directive of December 12, 2006 uses the same definition.[4]
It should be noted that the exclusion of the gambling services from the scope of the European directives is due to "*the specific nature of these activities, which entail implementation by Member States of policies relating to public policy and consumer protection".*[5]
The study prepared by the Swiss Institute of Comparative Law on gambling services in the European Union makes a distinction between (i) the "*gambling services*" and (ii) the "*promotional games*", and defines the first as *"any service, including any information society service, which involves wagering a stake with monetary value in games of chance, including lotteries and betting transactions".*[6]

On-line gambling services – The appearance of new communication technologies has vastly extended the gambling market and has raised new issues which are going far beyond domestic laws.

In light of the above, how can the internationalization of gambling services be made compatible with the heterogeneous domestic legislations in such a morally and economically delicate field?

The European Union faced with divergent perceptions – Within the European Union, domestic laws vary from one Member State to another.

Whereas Malta and United Kingdom attempt to reconcile the opening of the gambling market with regulators' control, other Members States establish a monopoly in the whole gambling and betting market (notably Finland and Sweden); others combine such monopoly with a system of authorizations (*e.g.*, Italy, Germany and France).[7]
The variety of domestic laws can be explained by the specificity of the gambling sector, which has been acknowledged by the European directives[8] as well as the European Court of Justice (ECJ) in the Schindler case of March 24, 1994.[9]

The ECJ admitted that the moral, religious or cultural considerations, with relation to gambling services, justify the sufficient and discretionary power granted to the national authorities, allowing them to determine the criteria necessary to protect gamblers, and more generally, to protect the social order.

[1] Michel Béjot is a partner of the Paris-based firm Bernard - Hertz - Béjot. He can be reached by email at mbejot@bhbfrance.com. He is on the Editorial Board of the Journal of Internet Law and chairs the EMEA Region of the Global Advertising Lawyers Alliance (GALA). His practice's areas are notably the following : Intellectual Property; Computer Law; Information Technology and New Technologies; Advertising Law; Trade Regulation; Mergers and acquisitions, International Litigation.
Caroline Bouvier is an associate at the Paris-based firm Bernard - Hertz - Béjot. She is graduated from the University of Paris I Sorbonne (Master Private Law, contract and torts) and from the University of Paris II Assas (Master Media and Information Technology Law). Her practice's areas are notably the following : Intellectual Property; Computer Law; Information Technology and New Technologies; Advertising Law.
Also thanked is Carole Bui, a trainee at Bernard - Hertz - Béjot for her help in the research of this article.
[2] « *Study of Gambling in the Internal Market of the European Union* », Final Report of the Swiss Institute of Comparative Law, June 14, 2006, p. XI.
[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (recital 16 and article 1, subsection 5, indent d)
[4] Directive 2006/123 of 12 December 2006 on services in internal market, and in particular article 2, subsection 2, indent h.
[5] See notably recital 25 of the aforementioned Directive 2006/123.
[6] « *Study of Gambling in the Internal Market of the European Union* », p. V, see aforesaid note 2.
[7] "*Rapport d'information sur le monopole des jeux d'argent au regard des règles communautaires*" (Report related to the gambling monopoly in light of the European rules), Report filed with the Presidency of the French National Assembly on February 6, 2008 and presented by Mr. Blessig and Mr. Myard, p. 30 to 52.
[8] See the aforesaid directives and notes 3,4 and 5.
[9] ECJ, March 24, 1994, C-275/92, Schindler, ECR I-1039.

Dans ce même arrêt, elle a également qualifié de « *service* », au sens de l'article 49 du Traité CE, l'activité d'organisation de loteries.
Par la suite, elle a adopté la même qualification s'agissant de paris d'événements sportifs en considérant que « *l'activité qui consiste à permettre à des utilisateurs de participer, contre rémunération, à un jeu d'argent* », constitue un service au sens du Traité CE et que les particularités étatiques relevées dans l'arrêt *Schindler* s'appliquent « *pour les autres jeux d'argent qui présentent des caractéristiques comparables* » [10].

Ainsi, les services de jeux d'argent, soumis au principe de libre prestation de services de l'article 49 du Traité CE, ne peuvent faire l'objet de mesures discriminatoires à l'égard des autres Etats membres de la Communauté que si ces mesures sont justifiées par l'exercice de l'autorité publique (article 45 du Traité CE) ou par des raisons d'ordre public, de sécurité publique et de santé publique (article 46 du Traité CE) ou encore par « *des raisons impérieuses d'intérêt général* », telle que cette notion a été développée par la jurisprudence de la CJCE.

La jurisprudence de la CJCE en évolution - Dans les années 90, la CJCE a reconnu la licéité de certaines législations européennes restreignant l'offre de services de jeux d'argent et, par la même, a posé le cadre des restrictions transfrontalières autorisées.

L'arrêt *Schindler* a pris en considération les objectifs de la législation britannique en cause comme destinée à « *prévenir les délits et garantir que les participants aux jeux d'argent seront traités honnêtement ; éviter de stimuler la demande dans le secteur des jeux d'argent dont les excès ont des conséquences sociales dommageables ; veiller à ce que les loteries ne puissent pas être organisées en vue d'un profit personnel et commercial mais seulement à des fins caritatives, sportives ou culturelles* ». Sur la base d'une étude d'ensemble de ces motifs, la CJCE a considéré qu'ils étaient de nature à justifier une restriction à la libre prestation de services.[11]

De la même manière, le fait de confier à un seul organisme des droits exclusifs pour l'offre de jeux d'argent peut être justifié au regard des principes du droit communautaire en ce qu'une telle restriction « *présente l'avantage de canaliser l'envie de jouer et l'exploitation des jeux dans un circuit contrôlé, de prévenir les risques d'une telle exploitation à des fins frauduleuses et criminelles et d'utiliser les bénéfices qui en découlent à des fins d'utilité publique* ».[12]
En revanche, de telles restrictions à la libre prestation de services ne peuvent être acceptées que si ces mesures sont justifiées par des raisons impérieuses d'intérêt général, si elles sont propres à garantir la réalisation de l'objectif qu'elles visent et si elles ne vont pas au-delà de ce qui est nécessaire pour l'atteindre. [13]

La CJCE a également conditionné l'existence de mesures restrictives à l'offre transfrontalière de jeux d'argent à la nécessité que leurs « ***modalités concrètes d'application*** » répondent « ***véritablement*** *aux objectifs susceptibles de* [les] *justifier et si les restrictions* [qu'elles] *imposent n'apparaissent pas disproportionnées au regard de* [leurs] *objectifs* ».[14]
Au début des années 2000, la CJCE a poursuivi ce mouvement de rationalisation des restrictions à la libre prestation des services de jeu d'argent en exigeant qu'elles soient « *propres à garantir la réalisation desdits objectifs* [raisons impérieuses d'intérêt général] *en ce sens que ces restrictions doivent contribuer à limiter les activités de paris de manière* ***cohérente*** *et* ***systématique*** ».
Par conséquent, si un Etat mène une politique d'incitation des consommateurs pour qu'ils participent à des jeux d'argent et qu'il en retire des bénéfices sur le plan financier, il ne saurait invoquer l'ordre public social pour justifier des mesures jugées restrictives.[15]

Plus récemment, dans l'arrêt *Placanica*, la CJCE a considéré « *qu'il convient d'analyser* ***séparément****, pour chacune des restrictions imposées par la législation nationale, notamment si elle est propre à garantir la réalisation du ou des objectifs invoqués par l'État membre en cause et si elle ne va pas au-delà de ce qui est nécessaire pour l'atteindre* » [16], ce qui diffère de la position initiale posée dans l'arrêt *Schindler* précité (analyse « *d'ensemble* » des motifs d'intérêt général). L'analyse de la licéité des restrictions posées par un Etat membre semble ainsi plus affinée.

[10] CJCE, 21 octobre 1999, Aff. C-67/98, Zenatti, Rec. 1999, I p.7289.
[11] CJCE, 24 mars 1994, arrêt Schindler, précité op. cit. note 9.
[12] CJCE, 21 septembre 1999, Aff.C-124/97 Läärä, Rec. CJCE, I p.6067.
[13] CJCE, 25 juillet 1991, Aff. C-288/89 Collective Antennevoorziening Gouda , Rec. P. I-4007, points 13 à 15 et repris dans l'arrêt Zenatti précité op. cit. note 10 (point 29).
[14] Arrêt Zenatti précité op. cit. note 10 point 37.
[15] CJCE, 6 novembre 2003, Aff. C-243/01, Gambelli, Rec. CJCE, I p.13031.

In the same decision, the ECJ also defined the activity consisting of the organization of lotteries as a "*service*" according to article 49 of the Treaty establishing the European Community.
Later on, the ECJ adopted the same qualification for sport betting by considering that *"the activity which allows the users to participate, upon payment, to a gambling service*" is deemed a service according to the European Treaty and that the national specificities highlighted in the Schindler case apply *"to the other games which present the same characteristics".[10]*

Thus the gambling services, which are submitted to the principle of the freedom to provide services as stated in article 49 of the Treaty establishing the European Community, should not be subject to discriminatory measures towards other Member States, except where these measures are justified by the exercise of official authority (article 45 of the Treaty), by public policy, public security or public health (article 46 of the Treaty), or by the "*overriding reasons relating to the public interest"*, as developed by the ECJ decisions.

The evolution of the ECJ's position – In the 90's, the ECJ recognized the legality of some European legislations restraining the offer of gambling services and thereby created the framework of authorized cross-border restrictions.

The Schindler case took into account the goals of the British legislation as it aims *"to prevent crime and to ensure that gamblers would be treated honestly; to avoid stimulating demand in the gambling sector which has damaging social consequences when taken to excess; and to ensure that lotteries could not be operated for personal and commercial profit but solely for charitable, sporting or cultural purposes".* Based on a global analysis of these factors, the ECJ admitted that they could justify a restriction to the freedom to provide services.[11]

Similarly, granting to a single organization the exclusive rights to provide gambling services can be justified under European principles, by the fact that such restriction *"… has the advantage of confining the desire to gamble and the exploitation of gambling within controlled channels, of preventing the risk of fraud or crime in the context of such exploitation, and of using the resulting profits for public interest purposes, likewise falls within the ambit of those objectives*".[12]
However, such restrictions to the freedom to provide services shall only be accepted if these measures are justified by overriding reasons relating to the public interest, if they are suitable in guaranteeing the achievement of the intended aim and do not go beyond that which is necessary in order to achieve such purpose.[13]

The ECJ also conditioned the existence of the measures restraining the cross-border gambling offer to the requirement that their "***concrete modalities*** *of* ***application*** *really correspond to the aims that are likely to justify these restraining measures and if these restrictions are not out of proportion as regards their objectives".*[14]
In 2003, the ECJ kept on rationalizing restrictions to the freedom to provide gambling services by requiring their suitability for *"achieving those objectives, inasmuch as they must serve to limit betting activities in a* ***consistent*** *and* ***systematic*** *manner".*
Consequently, if a Member State incites and encourages gambling and if profits are made from it, this Member State should not invoke public policy to justify restrictive measures[15].

More recently, in the Placanica case, the ECJ considered that *"the restrictive measures imposed by the national legislation should therefore be examined in turn in order to determine in each case in particular whether the measure is suitable for achieving the objective or objectives invoked by the Member State concerned and whether it does not go beyond what is necessary in order to achieve those objectives".[16]* This analysis is quite different from the one applied in the Schindler case (global analysis of the public policy considerations). The study of the legality of the restrictions imposed by a Member State seems more elaborated here.

[10] ECJ, October 21, 1999, C-67/98, Zenatti, ECR I- 7289.
[11] ECJ, March 24, 1994, C-275/92, Schindler, ECR I-1039 and aforesaid note 9.
[12] ECJ, September 21 1999, case C-124/97 Läärä, ECR I-6067.
[13] ECJ, July 25, 1991, C-228/89, Collective Antennevoorziening Gouda, I-4007 (recitals 13 to 15) and mentioned in the Zenatti judgement (recital 29), aforementioned in note 10.
[14] Zenatti judgement, aforementioned in note 10.
[15] ECJ, November 6, 2003, C-243/01, Gambelli : ECR I-13031.

La convergence de la position de l'Organisation Mondiale du Commerce (OMC) avec celle de la CJCE – Dans une affaire opposant Antigua-et-Barbuda et les Etats-Unis (en raison de l'interdiction faite à des opérateurs localisés à Antigua de proposer des services de paris et de jeux en ligne à des joueurs établis aux Etats-Unis), l'organe d'appel de l'OMC a rendu, le 7 avril 2005, une décision se fondant sur les dispositions de l'Accord Général sur le Commerce des Services (AGCS).[17]

L'organe d'appel a estimé que les lois fédérales américaines étaient contraires aux dispositions des articles XVI.1 et 2 de l'AGCS mais a toutefois considéré que ces mesures sont « *nécessaires à la protection de la moralité publique ou de l'ordre public* ».
Il a cependant constaté que ces mesures s'appliquent de manière différente aux fournisseurs de paris nationaux et étrangers et violent la règle du traitement national.
Ce raisonnement en deux temps est comparable à celui tenu par la CJCE sur le fondement de l'article 49 du Traité CE.

Les procédures lancées à l'encontre de certains Etats européens – L'affinement de la position de la CJCE s'est soldée par la mise en cause de certaines législations européennes. Ainsi, la Commission européenne a officiellement demandé notamment à la France, la Suède, la Grèce et aux Pays-Bas, sous la forme d'avis motivés[18], de modifier leurs législations.[19]

La mise en conformité de ces législations nationales sera cependant plus longue que le délai imparti par la Commission, tant les questions, notamment fiscales, sont nombreuses.
La France, qui a bénéficié d'un délai supplémentaire pour apporter ses propositions à la Commission, travaille actuellement à une « *ouverture maîtrisée* » du marché du jeu. Une commission gouvernementale[20] a ainsi été mise en place et devrait rendre son rapport prochainement.

* * *

[16] CJCE, 6 mars 2007, Aff. jointes C-338/04, C-359/04 et C-360/04, Placanica.
[17] Voir sur le site de l'OMC : http://www.wto.org/french/tratop_f/dispu_f/cases_f/ds285_f.htm et également l'article de A. Tenenbaum, « *les jeux d'argent sur l'Internet facilités dans le cadre de l'Organisation mondiale du commerce – réflexions à propos de la décision de l'organe d'appel de l'OMC du 7 avril 2005* », Comm. Com. Electr. 2005, étude 31.
[18] Il s'agit du préalable à la procédure d'infraction prévue à l'article 226 du Traité CE.
[19] Communiqués de presse des 27 juin 2007, 28 et 29 février 2008, disponibles sur le site Europa : http://europa.eu/index_fr.htm.
[20] Commission présidée par Monsieur Bruno Durieux, ancien ministre, inspecteur général des finances.

Similar position of the World Trade Organization (WTO) and the ECJ – In a case opposing Antigua-and-Barbuda and the United States (due to the prohibition preventing gambling and betting websites located in Antigua to supply gambling services to players living in United States), on April 7, 2005 the WTO Appellate Body rendered a decision based on the provisions of the General Agreement on Trade in Services (GATS)[17].

The WTO Appellate Body held that US federal laws are contrary to articles XVI.1 and 2 of the GATS. Nevertheless, it recognized that these laws are *"necessary to protect public morals or to maintain public order".*
The Appellate Body found, however, that these measures apply in a different manner to the domestic and foreign suppliers of gambling and betting services in a way that does infringe the national treatment principle.
This two-step analysis is similar to the position adopted by the ECJ on the basis of article 49 of the Treaty establishing the European Community.

Actions initiated against certain Members States – The refinement of the ECJ's position leads to the reconsideration of certain European legislations by the European Commission. Thus, the Commission officially sent notably to France, Sweden, Greece and The Netherlands reasoned opinions[18] in order to have them modify their legislations.[19]

However, the compliance of these domestic laws with the European principles will certainly exceed the time period allocated by the European Commission, insofar as the issues raised, notably the tax issues, are numerous.
France, which has been granted additional time to present to the European Commission suggestions to amend its legislation, is currently working on a *"controlled opening"* of its gambling market. A governmental commission[20] has been established and will be required to deliver its report in the near future.

* * *

[16] ECJ, March 6, 2007, C-338/04, C-359/04, C-360/04, Placanica.
[17] [See WTO's website] : http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm and the article from A. Tenebaum, "Les jeux d'argent sur l'Internet facilités dans le cadre de l'Organisation mondiale du commerce – réflexions à propos de la décision de l'organe d'appel de l'OMC du 7 avril 2005 » («the offer of online gambling services rendered more easy in the field of the World Trade Organization – analysis of the judgment of the WTO Appellate Body dated April 5, 2005"), Comm. Com. Electr. 2005, study 31.
[18] Prior to the procedure before the ECJ, as defined in article 226 of the Treaty establishing the European Community.
[19] Press releases of June 27, 2007 and February 28 and 29, 2008 : available on the website : http://europa.eu/.
[20] Mr. Bruno Durieux, past Secretary, Senior Treasury Official, is the chairman of this governmental commission.

Telecommunications and converging technologies: what's new?

By Bill Jones (*)
Wragge & Co LLP

I recall that when I first heard the term "convergence" used in an Information Technology context some years ago (probably the late 1990s), it meant the coming together of telecoms networks, software applications and media content. It was a fairly solid concept referring to discrete and what looking back today seem to have been relatively stable elements. Reference to the concept, and interest in it, were driven by increasing consumer access to the internet via basic dial up and telecoms facilities. In this way consumers in increasing numbers were taking advantage of the services of "new" Internet Service Providers such as AOL and "new" search engines such as AltaVista. That all seems such a long time ago!

The advent of broadband and of Web 2.0 technologies has changed the landscape dramatically. We now contemplate the distant past as Web 1.0, the recent past as Web 2.0 and the future as Web 3.0.

At the Technet Summit in November 2006, Reed Hastings, founder and CEO of Netflix, stated a simple formula for defining the phases of the Web:

> "Web 1.0 was dial-up, 50K average bandwidth, Web 2.0 is an average 1 megabit of bandwidth and Web 3.0 will be 10 megabits of bandwidth all the time, which will be the full video Web, and that will feel like Web 3.0."

So much for the networks; as for the applications, at the Seoul Digital Forum in May 2007, Eric Schmidt, CEO of Google, was asked to define Web 2.0 and Web 3.0. He responded:

> "Web 2.0 is a marketing term, and I think you've just invented Web 3.0.
> But if I were to guess what Web 3.0 is, I would tell you that it's a different way of building applications... My prediction would be that Web 3.0 will ultimately be seen as applications which are pieced together. There are a number of characteristics: the applications are relatively small, the data is in the cloud, the applications can run on any device, PC or mobile phone, the applications are very fast and they're very customizable. Furthermore, the applications are distributed virally: literally by social networks, by email. You won't go to the store and purchase them... That's a very different application model than we've ever seen in computing."

Applications which are pieced together are converging. If a phone is no longer just a phone, but a texting and email device, an MP3 player, and a means for browsing the internet, a relatively straightforward technological product has become many times functionally richer through convergence of the various applications now contained within this single but radically transformed entity.

Meanwhile producers of media content have adapted with speed and increasing flexibility to take advantage of the new technologies. When I watch a programme that I have missed as a live transmission later on the BBC's iPlayer, I lose the sense of formerly strict divisions between TV and Video. This recently introduced means of time-shifting activity is achieved by the convergence of formerly distinct technologies and devices.

The final twist in the content layer is the new found proactivity and power of the users. Armed with new tools and improved technology we have witnessed an explosion of user-generated content – text, photographs, film, video, music. Because it is no longer necessary to be a computer scientist to create a program, the distinction between professionals, semi-professionals, and consumers is becoming blurred. Content on the BBC website includes traditionally displayed news items written by professional journalists, alongside eye-witness pieces or extensions to those items "mailed" in by the man or woman in the street. Professional journalists morph into amateur, and amateur into professionals.

As lawyers we can only struggle to keep up! The objective of achieving "certainty under the law" is challenged by such periods of rapid change and transformation. New business models raise fresh business questions while new legal issues tend to emerge in tandem with them.

Privacy and Security of Personal Data

One major area of concern has been in respect of threats to the privacy and security of personal data. This has a number of contexts. First, a number of embarrassing incidents in respect of the loss personal data held by public sector organisations have drawn attention to the vulnerability of increasingly large databases held by such organisations. Chief amongst the many recent embarrassing incidents of this sort was the loss in the UK in late 2007 by HM Revenue and Customs of two discs containing personal data relating to 25 million individuals. There have been a dozen or more similar incidents in the UK within the last twelve months which is challenging public confidence in the handling of such data in both public and private sectors.

A second area of concern is the naivety and lack of education of the general public about their interaction with web-based services. Social networking sites and the lack of control over personal data posted by participants in particular have attracted attention and comment. Poor understanding of the available controls to determine how and where such data is posted, and the lack of use of such controls have led a number of experts to voice concern about the use that might be made by criminals and fraudsters of personal information such as names, addresses and dates of birth routinely posted on sites such as Facebook and MySpace[1].

Sir Tim Berners Lee has recently questioned proposed use of new software applications to track the websites consumers visit in order that web based adverts can be tailored to the individual concerned[2]. Berners Lee's view is that his data and his web history belong to him. He doesn't want use made of it without his express agreement, and he wants to know the precise nature of the actions and activities proposed before giving agreement: "I want to know if I look up a whole lot of books about some form of cancer that that's not going to get to my insurance company and I'm going to find my insurance premium is going to go up by 5% because they've figured I'm looking at those books," is how he expressed one of the concerns he has with such activities.

Intellectual Property

Another legal area challenged by convergence is Intellectual Property. Copyright has proved extraordinarily adaptable over several centuries of technological change but in an era of mash-ups and morphing, where do the rights in one work end and rights in a new work start? And when technology makes copying and reproduction ultra fast, easy, and user friendly, how do traditional rights owners control the use made of their assets in ways which are at the heart of their business models? Digital rights management has become a cause celebre for the owners of copyright in music, video, and film, but some artists have shown a refreshing willingness to adapt their business models and the management of their IPR in the light of these changes as witnessed by Radiohead leaving their record label, EMI, and releasing their seventh album, In Rainbows, last year through their website as a digital download for which customers selected their own price.

Regulation

Finally, the newly converged technologies challenge traditional models of regulation. Should internet video be subject to regulation based on the laws regulating television? The revised European TV Without Frontiers (TVWF) directive, renamed the Audiovisual Media Services (AVMS) directive, involves some extension of the regulatory regime to cover "TV-like" video-on-demand services. Convergence as an excuse for regulation of the internet has provoked strong emotions. Graham Smith has argued against such developments, seeing "broadcast content regulation (as) an anomalous relic of the old days of spectrum scarcity", and calling for vigilance to ensure that national implementations of the Directive in each EU Member State properly reflect the limited regulatory extension intended by the Directive's final form[3].

It is hard to be bored as an IT lawyer in these interesting times! I look forward to similar passions being reflected in the debate on these and related issues at our forthcoming Conference.

(*) Bill Jones is attorney-at-Law at Wragge & Co LLP. He is Chair of SCL, and is the Session Chair for the afternoon session on Friday 6th June which starts with the topic "Telecommunications and Converging Technologies". In this article he describes his thoughts in anticipation of this part of the Conference.

[1] "Social networkers warned of risk", bbc.co.uk, 12th November, 2007
[2] "Web creator rejects net tracking", bbc.co.uk, 17th March, 2008
[3] "Convergence is not an excuse to regulate the internet", Times Online, October 22nd, 2007[52] Ibid.

Regulating World IT Companies

By Clive Davies (*)
Fujitsu Services Limited

I have the privilege of moderating the session on "Should World IT Companies be Regulated?" at the IFCLA conference in Paris in June and am very much looking forward to exploring this fascinating subject which has become more and more topical in recent years. This may seem a bit paradoxical since it could be said that we live in an increasingly deregulated era with a plethora of delivery platforms as convergence becomes a reality. However if regulation is taken in a broader context then it rapidly becomes clear that it is an important topic for technology companies, especially if these are broadly defined.

I have worked in private practice and industry as an IT lawyer for many years. I currently work for Fujitsu Services Limited which was originally International Computers Limited (ICL). This company was formed in 1968 as a part of the Industrial Expansion Act of the UK Labour Government to create a British computer industry that could compete with major world manufacturers like IBM. Computer companies were seen as national assets. Those days are of course long gone. Fujitsu Services Limited is now part of a worldwide group which is a leading provider of customer focused IT and communications solutions for the global market place owned by Fujitsu Limited in Japan. Interestingly there are relatively recent vestiges of national interest such as the French government's support for Groupe Bull which was only re-privatised in 1994.
Communications companies have of course been subject to regulation, traditionally because of a shortage of available spectrum or networks, or because telecommunication capability was seen as a national asset of public importance. However with the expansion of broadband capacity and the relative surfeit of capacity we now have, coupled with the international deregulation of telecommunication services, regulation now has a much lighter touch.
However what interests me now is that the issue of regulation has moved on from wanting to establish and control IT or telecommunications companies to concerns about their ability to influence so much of what happens in our interconnected globe, dependent as it is on technology and data. IT companies can no longer be considered as just hardware vendors or software licensors. They are now the suppliers of the digital products and services that enable the converged web 2.0 world where computing and distributed services are provided through service oriented architecture across national boundaries. In this sense the regulation or potential regulation of multinational IT companies manifests itself in a number of ways.
Regulation under competition law
Microsoft has been fined 899 million Euros in February 2008 by the European Commission for failure to comply with a 2004 decision that it had abused its dominant position in the software market (for which it had already been fined 497 million Euros).
Outsourcing to offshore locations
The outsourcing of government functions with loss of local jobs was a huge issue at the time of the last US presidential election. Barack Obama, the likely Democratic presidential candidate in the current presidential campaign, has proposed tax breaks for US corporations that invest at home rather than abroad.

Financial regulation of outsourcing
The Financial Services Authority (FSA) in the UK regulates outsourcing of financial services in order to assist in the management of risk. Although strictly more regulation of customers than IT outsourcing companies this guidance, which is really a distillation of good practice, is critical for compliance purposes.

Voice over IP (VoIP)
With the advent of VoIP IT companies have become telecoms companies. How if at all should this be regulated? From 8 September 2008, for example, the UK communications regulator OFCOM has required require certain categories of VoIP service to provide access to the emergency services.

Television and radio without frontiers
IT companies also now facilitate the provision of on line music and video content across national boundaries challenging the regulation of TV without frontiers. EU member states have 2 years from November 2007 to implement the Audiovisual Media Services (AVMS) Directive which will cover internet TV and on-demand services.

Data protection and transfer
To what extent should the storage and transmission of data by IT companies be controlled to protect the privacy of individuals? There are different regimes in the US and Europe and worldwide compliance by IT companies is more and more challenging.

Responsibility of ISP's
The existence of websites that support antisocial activities such as terrorism or pornography and are "permitted" by ISP's are often challenged in the court. But are ISP's not just innocent conduits?

Search engines and data
The amount of personal data available to or controlled by search engines is astonishing and can in theory be used for all manner of purposes. However should the providers of those search engines, which are providing a service we all use and benefit from, be subject to more regulation?

Virtual worlds
Should companies such as Linden Labs that run on line virtual communities like Second Life (where property has a real world value and avatars can suffer personal abuse) be regulated? This is important as virtual worlds move more into the business main stream.

Multinational "IT" companies have never been more at the forefront of business and social activities. Global compliance is a major issue and the regulation of IT companies is more and more of an issue when looked at in this wider context. Perhaps some of the issues are more to do with the services that IT companies in the converged world provide or facilitate. Some regulation as with outsourcing is aimed more at the customers for services. However it is likely in the next decade that multinational organisations providing IT and related communications and digital services generally will be affected by more regulation on a global scale than ever before. These and more issues will be explored at the IFCLA conference.

(*) Clive is Senior Counsel at Fujitsu Services Limited. He specialises in major IT and outsourcing project contracts. He has over a decade of experience advising customers and suppliers in the public and private sectors. He advises on all aspects of IT contracts including standard terms, software licences, development agreements, integration agreements and service contracts. He also advises on data protection and e-commerce.

Clive is a trustee of SCL and one of the editors of Communications Law. He participates in the activities of Intellect as a member of various industry working groups. He regularly writes articles and speaks on his subject at events.

The short but dense histoy of IT Law: to be followed...

By Antonio Millé (*)
Estudio Millé

The International Federation of Computer Law Associations is celebrating their twenty second year of life with a meeting that will join at Paris an important number of the lawyers that along the world make of the Information Technology the focus of their business and studies. It is without any doubt a good opportunity to reflect together about the past and future of our legal specialty.

As International President of the Latin American High Technology, Computers and Law Institute (ILATID in Spanish abbreviation) I had the opportunity of being one of the IFCLA initiators and to contribute to extend its international activities representing the Federation in international forums such as the World Intellectual Property Organization. Let me share with you my remembrances about these interesting initial times.
Those that the English legal jargon denominate "Computer Law" and the French nomenclature designate as "Droit de l´Informatique" born as legal specialty when an independent software industry begun to show the existence of novel and different legal problems asking for solutions in a legal framework devoid of any "digital" component. The appearance of a new variety of lawyers, able to understand a technology that was not at the reach of everybody at that time, was the natural consequence. Most of those lawyers came at that initial time from the fields of Patents, Licenses and Copyright, only later young lawyers who grown with a computer in their hands became "native" computer lawyers.

The first professional association of computer lawyers was probably the Computer Law Association, officially founded in USA in 1973. Different associations appeared in the course of the end of the years 70 and the beginning of the years 80 (among them ILATID, established in Buenos Aires in 1981). At that time, cohabited in the European and South American associations (there were not any one in Asia that I can remember) public officers and professors devoted to the applications of the Information Technology to legal purposes (case law databases, courts management, legal expert systems, etc.) as well as practitioners providing services to computer software companies and IT users. For the contrary the CLA was an association conformed almost exclusively by practitioners, not familiar with the themes of "Informatique Juridique/Computers and Law" (it is good to add that at that time the practitioners normally were also writers and professors on the matters of our branch of law).

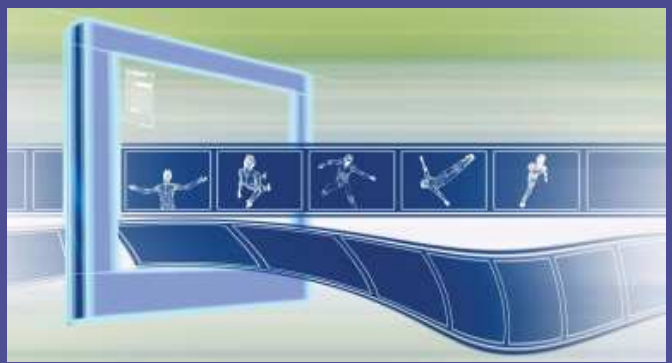
The seniority of CLA, it focalization in the computer software legal problems, and their competence with IBA for being the worldwide umbrella for the computer lawyers, kept this association apart from IFCLA. Many of the computer lawyers of that time were members both of a national association and of CLA, which with the course of the time becomes more and more international.
It is difficult to imagine at present how important was at that foundational time the personal contact between the lawyers specialized in the matter and the role of "virtual" (but "analogical") forums that accomplished reviews as the Californian *Software Protection* or the Parisian *Expertises*. It shall be a surprise to some of the readers to know that we communicated by post and that some Computer Law newsletters were typed at machine and then printed using Rotaprint stencils.

Beginning with the debates about the possibility to protect the computer software by patents, by copyright, or by a new ad-hoc regime and following by the recognition of the computer software legal nature as an artistic and literary work in the late 70´, with the subsequent apparition of Positive Law amendments in the first half of the 80´ (USA in 1980; France, Germany, Japan and UK in 1985) the Computer Law widen their index of matters.
Each progress of the Information Technology, each new business approach of the IT Industry was accompanied by the appearance of a new wave of juristic problems and solutions. We went from the "look and feel" interfaces conflicts to the reverse engineering and compatibility debate, in a way that included the software patents controversy. The convergence with the Communication business expanded the universe of the specialty and the Internet expansion carried us an array of digital problems which center progressively became distant from the pure computer programs issues. Personal data protection, EDI, electronic commerce, OSS, data security and retention, computer crime, electronic documents and signature, are some of the pieces of the big panoply that continued to grow.

Interim, the national, regional and international Law was creating a web of rules (with a notable compatibility) firmly supported by a growing Case Law. The impulse that coming from the WIPO documents and from the European Directives played an important role in the process of harmonization of the law on a matter that is of international application, and in a measure that no other law branches had.
The Internet bubble exploded, but the online Information Society continued and continues to solidify and grow. The field of the IT law received themes coming from the banking services, the music and movies exploitation, the journalism.. in a list that gets bigger daily. While practically all the humans becomes Internet users, legal problems related with the access to and sharing of digital content turn out to be matter of the IT law.
We arrived to the present among a promissory framework for the IT lawyers (that is the most current denomination for the former "computer lawyers"). All the activities are going digital, and the problems consequent to their entering in the digital environment comes to our desks. Our daily work requires us (in words of my appreciate friend and colleague Mike Scott) to be the most specialized of the generalists and the most generalist of the specialists. Niches of specialization are borning in the bosom of those that a quarter of century ago was a new niche of specialization.

Be part of the IT Law history! Come to the Paris IFCLA Conference to meet a good number of Computer Law veterans, share good work with colleagues from the entire world and contribute to give impulse and substance to a new and exiting branch of the Law.

(*) Professor Antonio Millé, Senior Partner of Estudio Millé, Buenos Aires, an Argentinean legal firm mainly devoted to Intellectual Property Law and High Technology Law. Among other charges he is Computer Law and Copyright Law Professor in the Catholic University; Panelist of WIPO Arbitration and Mediation Center; International Chairman of the Latin American High Technology, Computers and Law Institute ILATID; and Member of the Board and Chairman of the Liaison Committee of ITechLaw Association.



Anti-Social Networking | Learning the Art of Making Enemies in Web 2.0

By Sajai Singh (*)
J. Sagar Associate

Background paper[1] for IFCLA 2008 Conference

In the last few years there has been a proliferation of social networking websites. Increasingly, people around the world are sharing very personal and sensitive information in the process of building both professional and personal relationships on websites such as Facebook and MySpace. There are numerous Internet dating, chat forums and blogs which Internet users use to expand their social networks. The convergence of mobile and Internet technologies will invariably enable people to remain virtually tethered to their online social networks 24 hours a day. There are numerous benefits of social networking websites as the legions of these websites' users would likely attest to. However, critics and detractors of these websites warn of the potential abuses including the loss of privacy and anonymity that result from using these sites. On the flipside of this global phenomenon of social networking on the Internet is the emergence of online anti-social networking. Anti-social networking on the Internet can range from harmless parodies of established online social networking sites to more potentially harmful email messages and postings on blogs and chat sites, cyber bullying and harassment and hate speech. This paper looks at the emergence and implications of anti-social networking on the Internet.

Online Social Networking: A New Forum
In order to place the discussion of anti-social networking on the Internet in context, it is necessary to briefly highlight a few prominent social networking websites. This list is not all inclusive, since new and varied social networking websites are continually emerging on the Internet. The main online social networking are: Facebook, Orkut, MySpace, Rediff iShare, Apna Circle, Bigadda, Flickr and Hi5.

Social Networking Websites: A Common Thread
The common thread among most social networking websites is that they combine email, instant messaging, blogs, personal profiles and photo galleries into one easily accessible interface.[2] Providing an online forum with so many features is one of the main advantages of online social networking websites. However, social networking websites also make personal information more available to individuals who may wish to use this information for anti-social activities. In some respects, social networking websites could be viewed as the impetus for the emergence of anti-social networking websites.

Anti-social Networking Websites: Moving from a Harmless Parody to a Dangerous Trend
Riding the wave the popularity of online social networking is a new crop of websites that are essentially the antithesis of their social networking counterparts. These so called "anti-social networking" websites provide an outlet for users to express their displeasure and dislikes on a variety of topics. Some of the more recent additions to the online anti-social networking space aim to lampoon the prominent social networking websites with a kind of tongue in cheek tone. The emergence of these websites likely reflects a growing sense of cynicism among some Internet users who perceive the relationships established on the large social networking websites such as Facebook and MySpace as artificial and baseless.

Online Anti-Social Networking: The humorous side
For instance: Snubster and Enemybook, Isolatr, Introvertster, Ruduzu, NoSo Project, Choad Network.

Online Anti-social Networking: Harmful messages
The anti-social websites mentioned above, are, for the most part, innocuous. However, of greater concern to governments, NGO's, corporations and individuals is online anti-social networking which defames, damages reputations or promotes hatred. Of particular concern to individuals is the advent of cyber bullying, cyber stalking, cyber harassment and hate speech.

Cyber-bullying
Cyber-bullying refers to willful and repetitive harm inflicted through the medium of electronic text.[3] The intent of cyber-bullying is to cause emotional distress and can include threats, sexual remarks, and hate speech.[4] Cyber-bullying has also been described as deliberate, repeated and hostile behavior by an individual or group that is intended to harm others.[5] Cyber-bullying has become particularly common in the blog world where bloggers have been known to use racist and vulgar language and threats of violence.[6] Cyber-bullying falls within the ambit of anti-social networking because it can often impact more than just the intended victim, especially when threatening messages are posted on widely read blogs and websites. Cyber-bullying is clearly a form of anti-social networking since threatening messages posted by cyber bullies can often intimidate people from otherwise engaging in their own online social networks.
The incidence of cyber-bullying is particularly troubling among youth. In a study by i-Safe America, over 42% of children aged 10-14 reported being bullied online.[7] This statistic is alarming given that 58% of these children did not report these incidents to their parents or guardians.[8]

Hate Speech
Hate speech is defined as speech intended to degrade, intimidate or incite violence against a person or group of people based on a range of criteria including: ethnicity, nationality, sexual orientation, political affiliations, gender and socio-economic class.[12]
The prevalence of hate speech on the Internet has been steadily rising since the mid 1990's. For example, the number of white supremacist websites increased from 1 in 1995 to approximately 4000 in 2001. Recent data indicates that this upward trend is continuing. In its 10th annual Digital Terrorism and Hate report, the Simon Wiesenthal Center identified over 7000 hate websites, a 17% increase from 2006.[13] Hate speech can easily be disseminated through other forums such as blogs, chat rooms and email distribution lists and online video games, all of which cannot easily be tracked and quantified.[14]

'Pro Choice' gets another meaning - *Suicide Assistance!*
Sites are mushrooming all over Web 2.0 providing step-by-step guidance, including via chatrooms, on how to commit suicide. Cause for concern for parents and governments? Indeed. The recent teen suicide wave in the UK, which police believe was prompted by messages on a social networking site. In India, a Grade XII student GN Vinay, from Delhi, hanged himself to death. Police and relatives believe this is the result of an online discussion on life after death! 'Pro Choice' is getting a dangerous connotation with 'freedom of expression' taking a life threatening turn.
So what do these sites advocate as facilitators for suicide? Rat Poison, cigarettes, Cyanide, etc. are some of the 100,000 ways of killing oneself or embracing death in all its glory! While there is lack of statistics on the 'success' of such sites, as most people sign on in an anonymous pseudonym or nick name, but police in high tech centres the world over, including Bangalore[15], are seriously considering the impact of such websites with regard to an increase in suicides.

(*) **Sajai Singh,** Partner & Head of Technology Practice at **J. Sagar Associates Advocates & Solicitors. His practice fucusses on the emerging technologies, VC/PE Investments and M&A.Sajai is also member of the board of ITechLaw.**
[1] The aim of this paper is to present the reader with information, material and some analysis on the 'other side' to the growth of social networking sites which are a major part of the Web 2.0 environment. It is by no means a comprehensive study on an ever-changing landscape. This paper may be read in the stated context and any questions, comments or further information may be sought from the author whose communication details have been provided at the end of this paper.
[2] Forsite Group, "MySpace: Safeguard Your Students, Protect Your Network", 2006.
[3] http://en.wikipedia.org/wiki/Cyber-bullying
[4] Ibid.
[5] http://www.cyberbullying.org/
[6] Supra note 27.
[7] http://www.thefreelibrary.com/Cyberbullying:+a+%22virtual%22+camp+nightmare%3F-a0165939091
[8] Ibid.
[9] http://en.wikipedia.org/wiki/Cyberstalking
[10] Ibid.
[11] Ibid.
[12] http://en.wikipedia.org/wiki/Hate_speech
[13] Licia Corbella, "Hatred weaves evil new web", The Calgary Sun, June 1, 2007.
[14] Jane Bailey, "Private Regulation and Public Policy: Toward Effective Restriction of Internet Hate Propoganda", (2004) McGill L.J, 59-103, para 5.
[15] National Crime Records Bureau, India, recorded 1470 suicides in Bangalore in 2005 and the figure went up by 36.6% to 2008 in 2006, which is the highest in the country.

Hate Speech
Hate speech is defined as speech intended to degrade, intimidate or incite violence against a person or group of people based on a range of criteria including: ethnicity, nationality, sexual orientation, political affiliations, gender and socio-economic class.[12]
The prevalence of hate speech on the Internet has been steadily rising since the mid 1990's. For example, the number of white supremacist websites increased from 1 in 1995 to approximately 4000 in 2001. Recent data indicates that this upward trend is continuing. In its 10th annual Digital Terrorism and Hate report, the Simon Wiesenthal Center identified over 7000 hate websites, a 17% increase from 2006.[13] Hate speech can easily be disseminated through other forums such as blogs, chat rooms and email distribution lists and online video games, all of which cannot easily be tracked and quantified.[14]

'Pro Choice' gets another meaning - *Suicide Assistance!*
Sites are mushrooming all over Web 2.0 providing step-by-step guidance, including via chatrooms, on how to commit suicide. Cause for concern for parents and governments? Indeed. The recent teen suicide wave in the UK, which police believe was prompted by messages on a social networking site. In India, a Grade XII student GN Vinay, from Delhi, hanged himself to death. Police and relatives believe this is the result of an online discussion on life after death! 'Pro Choice' is getting a dangerous connotation with 'freedom of expression' taking a life threatening turn.
So what do these sites advocate as facilitators for suicide? Rat Poison, cigarettes, Cyanide, etc. are some of the 100,000 ways of killing oneself or embracing death in all its glory! While there is lack of statistics on the 'success' of such sites, as most people sign on in an anonymous pseudonym or nick name, but police in high tech centres the world over, including Bangalore[15], are seriously considering the impact of such websites with regard to an increase in suicides.

Propagation of Anti-social Messages on Legitimate Social Networking Websites
There are some instances where a legitimate social networking website can be a conduit for anti-social messages. For example, there was an online community on Orkut that recently garnered the attention of the Indian legal system. On October 10, 2006, Mumbai's High Court's Aurangabad bench served notice on Google's social networking website, Orkut, for permitting a hate campaign against India.[16] The notice was in response to online community on Orkut called "We Hate India", set up by a Russian, Miraslov Stankovic,[17] which propagated anti-India content and displayed an Indian flag being burned.[18] The origin of the notice was a public-interest petition filed by an Aurangabad attorney.[19]
In another development, Subodh Balsaraf, a resident of the Indian State of Maharashtra, in his Public Interest Litigation in the court, contended that Orkut used "slang, rude and vulgar language" about the Maratha king Shivaji. The community had been blocked by the Pune police after a few violent incidents were reported in the city. Though the community was then made inaccessible, the petitioner's demand for banning Orkut continued.[20]
Only recently, Google was ordered by a Brazilian court to hand over data of specific users to Brazilian authorities, following allegations that Orkut was being used for illegal activities, including child pornography and hate speeches against various groups.[21]
Several nations in the Middle East including Iran, UAE and Saudi Arabia have blocked access to Orkut because of some its online communities, which they consider to be an affront to Islam.
The site was officially blocked on July 17, 2007, after the Telecommunications Regulatory Authority (TRA) issued a formal letter to the Etisalat (UAE's Internet service providers) to block the site, following reports that the site contained sexually explicit material and was being used for 'immoral activities'.[22] The UAE also has a ban on social networking websites flicker and Hi5, and only recently lifted a ban on MySpace and video-sharing site YouTube.[23]
In August 2007, voices were once again raised against Orkut for its easy accessibility and abuse after a 16 year teenager Adnan Patrawala, was murdered in Mumbai, India. Kidnappers used Orkut to communicate with Adnan, befriend him, exchange phone numbers and entice him with the possibility of a 'real-life' meeting.[24]

Combating Anti-Social Networking: Legal and Non Legal Remedies
There are legal and non legal remedies at the disposal of individuals, NGO's, governments and corporations should they wish to take action against online anti-social networking websites. The legal remedies, however, are somewhat tenuous given the infancy of laws governing the Internet. Furthermore, there are jurisdictional issues which may inhibit a party from bringing forth legal action. The interpretation and application of laws that pertain to the Internet in India is scant; a reflection of limited Indian case law involving the Internet. There are, however, two statutes that may have some relevance in mitigating online anti-social networking.

The Indian Penal Code
The Indian Penal Code contains provisions that may be useful in a legal action against an anti-social networking website or an individual who spreads anti-social messages on the Internet. For example, Section 509 of the Code, could potentially be relied on when the subject of antisocial networking is a woman; where *whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.*[25]
Section 509 could potentially be useful to a female plaintiff (or class of female plaintiffs) when she has a claim for cyber stalking or cyber harassment. However, Section 509 does not specifically address harassment in the context of the Internet.
The Indian Penal Code also has a provision which addresses defamatory behavior. Section 499 stipulates, w*hoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person*[26]
Section 501 of the Code stipulates a fine or punishment of up to two years (or both) for anyone who prints or engraves any matter which they have good reason to believe is defamatory to any person.[27]

---

[16] "Google's social networking site in trouble", The Times of India,. Oct 10, 2006.
[17] http://www.pcworld.in/news/index.jsp/artId=2209
[18] Ibid.
[19] Ibid.
[20] http://www.rediff.com/news/2006/nov/23orkut.htm
[21] http://www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090100608.html
[22] http://www.arabianbusiness.com/index.php?option=com_content&view=article&id=495784:uae-bans-orkutcom&Itemid=72
[23] Ibid.
[24] http://www.rediff.com/news/2007/aug/20adnan1.htm
[25] Indian Penal Code, Section 509.
[26] Indian Penal Code, Section 499.
[27] Indian Penal Code, Section 501.

Information Technology Act 2000

There are several provisions within the Information Technology Act, 2000 which may provide legal redress against online anti-social networking.

Section 67 of the Act makes publication or transmission of obscene material in an electronic form an offence punishable, on first conviction, with a prison term up to 5 years and fine up to 100,000 Rupees.[28] However, there is a high threshold that must be met in order for anti-social material to be classified as obscene.

Anti-social behavior like website hacking is emerging as a large problem for corporations and non-profit organizations. India's Computer Emergency Response Team (CERT-In) monitors all incidents of defacement[29] to know which are the targeted domains and exact vulnerabilities being exploited by hackers. CERT-In claims that the .com domain is the first point of attack followed by the .in domain. Hackers often alter websites by displaying politically motivated, satirical or hate filled messages. This can significantly damage a company's brand image and bottom line. In terms of the hacking incidents, the major part thereof were phishing[30], then unauthorized scanning and finally virus / worm attacks.

Sections 65 and 67 of the Act may be useful against hackers who deface websites and spread anti-social messages. Section 65 of the Act also penalizes someone who intentionally alters, conceals or destroys computer source code.[31] Section 66 of the Act clearly defines hacking and a corresponding punishment, providing that *whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to 200,000 Rupees, or with both*.[32] Therefore, there may be legal recourse for anti-social networking perpetrated by hackers as defined by Section 65 of the Act. However, these provisions will have no effect on users of legitimate social and anti-social networking websites and blogs who post anti-social messages.

The Indian Ministry of Information Technology's Computer Emergency Response Team (CERT) is another potential legal avenue to combat anti-social networking. Although CERT is not related or mandated by the Information Technology Act 2000, its authority and purpose extends to some of the main legal issues which the Act addresses. The Charter of the CERT states that *the purpose of the CERT-In is, to become the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur ; the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents*.[33]

Computer hacking incidents which include anti-social messages and behavior may fall within the investigation domain of CERT.

The Constitution of India: Inbuilt Restrictions on Freedom of Speech

Article 19(1) of the Constitution of India protects the right to free speech and expression.[34] However, the Constitution of India, unlike the Constitution of the United States of America has inbuilt restrictions on this free speech. Article 19(2) of the Constitution of India curtails free speech, specifically in deference to public standards of decency and morality.[35] Thus India expects restraint while expressing freedom of speech in any form.

Global Context

There have been some efforts, at the international level, to address the emergence of online anti-social networking. For example, a number of Council of Europe (COE) member states signed a protocol in 2001 to address racist and xenophobic acts on computer networks.[36] The COE is also actively pressing for a new global treaty to protect children against on-line child predators.[37] The European Union is particularly concerned about a form of online anti-social networking referred to as, sexual grooming. This term refers to pedophiles that lure young users on the Internet.[38] In response to this practice, the European Union has earmarked $60 million on a three year child Internet safety program.[39]

US Legislation

Although the anti-social networking and messages are not restricted to borders, the ISP's where they originate from are. The US has been relatively tempered in passing hate speech legislation when compared to other countries. This hesitation likely stems for the United States Constitution's First Amendment. The First Amendment states that C*ongress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances*[40]

Perhaps the most important element of the first amendment is the freedom that individuals have to express themselves without the interference of congress.[41] Restriction of anti-social networking in the US is quite onerous, given the enshrinement of free speech. It also invariably constricts other nations from restricting anti-social networking websites and messages emanating from the US ISP's. Although, foreign jurisdictions can mandate their own ISP's to block or filter certain websites, it is by no means a foolproof method.

The United States Congress passed the Children's Internet Protection Act (CIPA) in December, 2000 to address offensive content on the Internet in schools and libraries.[42] Another US Federal Law, 18 U.S.C. 2425, makes using any form of interstate foreign commerce (including the Internet) to knowingly communicate with a minor with the intention to solicit unlawful sexual activity.

A Sample of Global Anti-Hate Speech Legislation

A detailed overview and analysis of international anti-hate speech legislation would be voluminous and go beyond the scope of this paper. However a snapshot of a few forms of anti-hate speech legislation is useful for comparative purposes.

In the United Kingdom, public incitement to racial hatred is punishable up to 7 years of imprisonment under the Public Order Act 1986.[43] In the UK, sites that encourage suicide and discussions about taking your own life have become part of an official review on child safety on the web.

In Germany, incitement of hatred against a minority community (if it takes place within German territory) is punishable with up to 5 years imprisonment under the German Criminal Code.[44]

In Norway, the Norwegian Penal Code prohibits hate speech, which includes, publicly making statements that ridicule someone based on their skin colour, ethnic orientation, religion, sexual orientation and religion.[45]

In Australia, providing any information online on suicide is punishable by a heavy fine.

Defamation: The Common Law Approach

The wrong of lowering an individual in the estimation of others, causing him/her to be shunned or avoided, or exposing him/her to hatred, contempt or ridicule, through publishing demeaning statements or other matter, is referred to in English common law as defamation.[46] Because of the international connectivity of the Internet, its speedy transmission of huge amounts of data simultaneously to multiple destinations, and general lack of respect for national borders, it is extremely easy for an individual to make a defamatory comment via a computer situated in one place attached to the Internet, which can then be read by thousands if not millions of people similarly equipped in multiple other national jurisdictions, where the law of, and defences to, defamation may be very different than those found in the legal system of the place where the defamatory comment is made.[47]

---

[46] Anna Beyer, "Defamation on the Internet: Joseph Gutnick v Dow Jones". http://www.murdoch.edu.au/elaw/issues/v11n3/beyer113.html

[47] Lilian Edwards, "Defamation and the Internet: Name Calling in Cyberspace". http://www.law.ed.ac.uk/it&law/c10_main.htm

[29] From data available, in August 2007 over 345 Indian websites were defaced, in September the figure was 60 and in October 2007 the figure went up to 143. The major attacks happen in August, coinciding with India's Independence Day. 2008 started with 858 defacements in February 2008 and 738 in March 2008.

[30] Like the west India too is witnessing a major rise in phishing attacks. In 2006 they were 180% higher than in 2005 and the trend has continued thereafter.

[31] Ibid.

[32] Section 66, Information Technology Act 2000.

[33] http://www.cert.org.in/mission.htm

[34] Aditi Jha, "The Law of Obscenity in India: How obscene is my right to freedom of speech and expression?", pg 12. www.indlaw.com

[35] Ibid.

[36] Supra note 36, para 7.

[37] Doreen Carvajal, "Fighting anti-social behaviour on social networking sites". International Herald Tribune, August 2007. http://www.iht.com/articles/2007/08/19/business/social20.php

[38] Ibid.

[39] Ibid.

[40] http://www.law.cornell.edu/constitution/constitution.billofrights.html#amendmenti

[41] Ibid.

[42] http://www.fcc.gov/cgb/consumerfacts/cipa.html

[43] http://en.wikipedia.org/wiki/Hate_speech

[44] Ibid.

[45] Ibid.

Where defamatory statements cross national boundaries, inevitably problems of international private law are invoked, with difficult questions raised such as what country (or countries) will have jurisdiction to hear any action for damages raised, what country's law should govern the action and if a decree is obtained, how can it be enforced if the defender lives outside the jurisdiction of the court. Those defamed on the Internet may find then that their case is not the simplest to pursue. Internet defamation defenders can be sued in the courts of multiple countries to which they have little or no connection, and where the law applied is foreign to them in the extreme. There can be jurisdiction either in the court of the defender's domicile, or the place where the remark was originally made, or the place where the remark is published, that is, where it is made public and has an impact on the reputation of the person defamed. [48]

The ISP

The case law which has developed in both the US and the UK has tended to support the proposition that an Internet Service Provider (ISP) and/or web host will not be liable for third party content, provided that they do not perform any editorial function. If an ISP or web host seeks to monitor the content on their system with a view to removing unlawful material, then if it fails to remove some then it may be deemed to be a publisher of that material as it is performing an editorial function. An ISP or web host needs to react swiftly when someone makes a complaint in relation to third party material which they are hosting on their site. It is essential that an ISP or web host has in place proper procedures to ensure that if a complaint is received it is investigated immediately and, if the material is unlawful, that it is removed.[49]

Non Legal Remedies: Public Relations and Private Initiatives

Corporations, individuals, NGO's and governments probably need to consider non-legal remedies in order to effectively counteract the negative effects of anti-social networking. For profit and non-profit organizations have vested interests in protecting their brand identities and position in the market place. Therefore, given the relative uncertainty with the effectiveness of legal remedies, it is imperative that organizations explore all avenues when mitigating the harmful effects of anti-social networking.

Corporations and NGO's in particular can harness the power of public relations to bolster their image and rebut damaging claims and assertions made by anti-social networking websites and blogs. For example, an organization could designate an individual in their PR department to post messages in blogs in order to respond to anti-social messages. Another method which organizations could employ is to create websites which directly respond to anti-social messages on the Internet. Openly questioning the reputation and credibility of anti-social messengers may have the desired effect of mitigating anti-social messages, *the most basic social technique- often overlooked but highly effective- is bringing an offensive message to the attention of people who know the sender on-or off-line, causing him to suffer the social or professional consequences of his behavior.*[50]

It is also imperative that social networking websites devise and implement policies and procedures that address anti-social behavior. This may include new techniques to validate and periodically check the authenticity of their users.

MySpace, increasingly concerned about on-line predators, has taken the initiative to implement their own measures to combat anti-social networking. They have designated a position in the company to oversee education, privacy programs and enforcement issues.[51] They are also developing technology to augment the search engines, pattern matching algorithms and human operators that they use to identify fake profiles.[52]

Conclusion

Anti-social behavior and networking on the Internet ranges from harmless parodies and satire to more harmful forms such as cyber stalking and hate speech. Clearly, the online anti-social networking phenomenon presents significant challenges to policy makers and Internet users. Currently available legal mechanisms alone may not be enough remedy, given the restrictions and limitations of laws governing the Internet and the rapid growth of online anti-social networking. Self regulation online, by ISP's, websites and user groups is essential and call of the day. Without these actions combating the ills of anti-social networking sites may not be possible.

---

[48] Ibid.
[49] http://www.out-law.com/page-488. For a amore detailed account of law governing liability of ISP in UK, USA and Australia , refer to http://www.efa.org.au/Issues/Censor/defamation.html and Lilian Edwards, "Defamation and the Internet: Name Calling in Cyberspace". http://www.law.ed.ac.uk/it&law/c10_main.htm.
[50] Ellen Spertus, "Social and Technical Means for Fighting On-Line Harrassment" 1996. http://people.mills.edu/spertus/Gender/glc/glc.html
[51] "MySpace: Safeguard Your Students, Protect Your Network". The Forsite Group. Pg 4. www.8e6.com
[52] Ibid.

We are looking forward to welcoming you soon!

The IFCLA Members

www.ifcla.com