WORLD INTERNET LAW REPORT

Volume 3, Issue 10 October 2002

Monthly News & Comment on Internet Law and Regulation from Around the World

HIGHLIGHTS

NEWS

THE FRENCH GOVERNMENT-owned postal monopoly, La Poste, has announced plans to launch an electronic version of the old-fashioned registered letter. The new e-letter will be accorded the same legal status as registered mail, giving Internet correspondence the same formal value and legal security until now reserved for physical exchanges. (Page 5)

THE NEW ZEALAND PARLIAMENTARY COUNSEL OFFICE has launched an interim website of New Zealand legislation. The website provides free public access to current versions of Acts of Parliament and Statutory Regulations and is part of the Public Access to Legislation Project. Report by Geoff Lawn, Deputy Chief Parliamentary Counsel and Project Director, Parliamentary Counsel Office, New Zealand. (Page 7)

CASE REPORTS

UNITED KINGDOM: Legitimacy of unofficial fan sites called into question: Hanna-Barbera Productions, Inc v. Graeme Hay. *Report by Katie Withers of Eversheds* (Page 10)

UNITED STATES: Cybersmearing: ZixIt Corp. v. Visa International. *Report by Jonathan Armstrong of Eversheds* (Page 11)

COMMENTARY

CHILE: Electronic Documents and Signature Law in Chile *by Fernando Castro and Cristóbal González, of Cruzat, Ortúzar & Mackenna (Baker & McKenzie – Santiago de Chile office)* (Page 14)

ITALY: Online Auctions in Italy: the Current Legal Framework in the Private and Public Sector *by Alessandro del Ninno, Studio Legale Tonucci* (Page 16)

INDIA: E-Business Regulation: Notes on Compliance Issues in the "Borderless Economy" *by Rodney D. Ryder of Anand & Anand* (Page 18)

HONG KONG: Defamation on the Internet *by Janine Canham of CMS Cameron McKenna* (Page 21)

Increasing use of the Internet has increased the risk of defamation lawsuits against companies which own websites and thereby either write or host messages of a potentially contentious nature. However, there are steps that website owners can take to limit their liability.

HONG KONG: The Gambling (Amendment) Ordinance: A Gamble or Not? *by Gabriela Kennedy and Vivian Lui of Lovells* (Page 24)

ROMANIA: An Overview of Romanian Telecommunications Legislation with reference to Internet Law Provisions *by Marius Petroiu of Baratz, Pachiu & Associates* (Page 26)

THAILAND: The Thai Electronic Transaction Act 2001: Recent Developments Surrounding IT Law in Thailand, *by Saravuth Pitiyasak, Lecturer in Law at Sukhothai Thammathirat Open University* (Page 28)

DOMAIN NAME DISPUTE RESOLUTION REPORTS

Listings of recent UDRP decisions (Page 31)

INTERNATIONAL DEVELOPMENTS

Internet Governance: ICANN under review *by Kate Ellis of Eversheds* (Page 33)

In recent months, the Internet Corporation for Assigned Names and Numbers - ICANN - has been the subject of intense scrutiny and its role, performance and future has been under review. The reform of ICANN has now reached a critical stage and whilst ICANN itself may be unknown to all but a small minority of Internet users, the outcome of the review will directly or indirectly affect all Internet users.

IN THIS REPORT

NEWS

CASE REPORTS

COMMENTARY

DOMAIN NAME DISPUTE RESOLUTION REPORTS

INTERNATIONAL DEVELOPMENTS

FORTHCOMING EVENTS

Submissions by Authors: The editors of *World Internet Law Report* invite readers to submit for publication articles that address issues arising out of the regulation of the Internet and e-commerce, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Nichola Dawson, World Internet Law Report, c/o BNA International Inc, Heron House, 10 Dean Farrar Street, London SW1H 0DX; tel. (+44) (0)20 7559 4807; fax (+44) (0)20 7233 2313; or e-mail: nicholad@bna.com.

WORLD INTERNET LAW REPORT

WORLD INTERNET LAW REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: Heron House, 10 Dean Farrar Street London SW1H 0DX, England. Tel. (+44) (0)20-7559 4801; Fax (+44) (0)20-7222-5550; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116. Subscription price: U.S. and Canada U.S.$925/U.K. and rest of world £550. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.

Website: *www.worldtaxandlaw.com* *ISSN 1468-4438*

Publishing Director: **Deborah Hicks** *Editorial Director:* **Joel Kolko** *Editor:* **Nichola Dawson** *Production Manager:* **Nitesh Vaghadia**

Correspondents: *Paris:* Lawrence Speer

NEWS FROM AROUND THE WORLD

AUSTRALIA

ABA and ACA to Merge

Australia's specialist broadcasting regulator, the Australian Broadcasting Authority (ABA), is to merge with the Australian Communications Authority (ACA) to create a single, unified agency with responsibility for radiocommunications, telecommunications and electronic media content issues.

It is envisaged that a multi-use spectrum and content regulator will increase efficiency and is the best way to deal with the future demands of Australia's communications environment.

Acting ABA Chair Lyn Maddock commented:

> "While substantial policy and governance issues need to be addressed, a properly designed, converged regulator would integrate and enhance current capacities".

The ABA has detailed its views on how the merger should be conducted in a submission to the Department of Communications, Information Technology and the Arts (DCITA). The overriding view is that spectrum management reform would be best dealt with as part of a broader process of media and communications policy development.

The ABA has been keen to highlight that it does not favour one of the options raised in the DCITA Discussion Paper, "Option for Structural Reform in Spectrum" (published in August of this year), whereby all or part of its spectrum management functions would simply be transferred to the ACA. The broadcasting authority rejected such an option as inefficient and detrimental to regulation and policy in a key area. The fact that such a move would fail to offer any significant benefits to end users or spectrum licensees, or help to finance the costs of the administrative restructuring, is something the ABA has also been quick to point out.

The ABA has stressed that in its own view "it is most important that spectrum management is not seen in isolation from the larger aim of ensuring a successful and timely transition to digital broadcasting".

DCITA Discussion Paper

The DCITA Discussion Paper put forward three options for re-arranging the spectrum management responsibilities of the ABA and ACA:

- combine the ABA and ACA in a single organisation;
- transfer the planning, licence allocation and enforcement functions of the ABA to the ACA; and
- transfer the broadcasting planning functions of the ABA to the ACA.

The full text of the Discussion Paper is available on the DCITA website (*www.dcita.gov.au/Article/0,,0_1-2_1-4_111029,00.html*), along with the ABA's submission, which can also be found in pdf format on the ABA website at: *www.aba.gov.au/abanews/news_releases/2002/pdf/NR92-02_ABA_submission.pdf*

AUSTRALIA

New Laws on Computer Crime

The Victorian Parliament is debating a bill designed to target hackers and individuals who intentionally spread computer viruses.

The Crimes (Property Damage and Computer Offences Bill), which will amend the 1958 Crimes Act, contains a range of new offences, created to deal with the type of twenty-first century crimes that are being perpetrated in light of the latest developments in computer technology, such as hacking, cyber-stalking, *etc.*

The new legislation repeals Section 9A of the Summary Offences Act, under which the maximum penalty enforceable for computer trespass offences was six months. The new Act carries a maximum penalty of ten years imprisonment.

Victorian Attorney-General, Rob Hulls has commented that the new laws are necessary to protect against the negative economic and social impacts that hacking and network sabotaging can cause and are in line with current public expectations in this area.

Cyber-Stalking Laws

The State Government has also sort comment from the legal community on proposals to make online stalking an offence. Electronic mediums, such as the Internet and e-mail are increasingly being used as methods of harassment, with victims being sent obscene and threatening messages and pictures.

The Law Institute has given its full support to the proposals and has endorsed the extra-territorial operation of cyber-stalking laws to deal with cross-border offences. It has advised however, that the requirement upon which current stalking legislation hinges, that harm, apprehension or fear actually occur, is not removed from any future law.

The Crimes Act, which underpins Victoria's present stalking laws (established as they were in 1995), defines stalking as a "course of conduct" intended to cause physical or mental harm to the victim or arouse fear or apprehension in the victim.

BELGIUM

New Legislation to Protect Electronic Transfers of Funds

On August 17, 2002, the Act of July 17, 2002 on transactions performed with instruments for the elec-

tronic transfer of funds was published in the Belgian Official Journal.

This new Act transposes the European Commission's non-binding Recommendation 97/489/EC of July 30, 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder. The Act aims to provide users of instruments for the electronic transfer of funds with a high level of protection in order to increase the users' confidence and thus support the development of e-commerce.

In general, the Act applies to transfers of funds via credit cards, phone banking, computer banking, the Internet, a device supplied by the issuer, sales outlet terminals, automatic distributors, *etc.*

However, rechargeable instruments that do not give direct access to a bank account and that a holder uses in his relationship with one specific issuer only, such as rechargeable telephone cards and photocopy cards, are excluded from the field of application. As companies using such instruments in principle have a better bargaining position with issuers, the Act only protects holders that are individuals.

The Act imposes some specific minimum pre-contractual and periodic information obligations on the issuer. It prescribes nine items that henceforth must be included in the issuer's general terms and conditions.

Furthermore, the Act sets out the obligations and liabilities of both the issuer and the holder. For instance, in case the instrument for the electronic transfer of funds is lost or stolen, then the holder is, as a rule, liable for an amount of EUR150 until he gives notice of the loss or theft to the issuer. However, if funds can be stored electronically on the instrument itself (*e.g.*, a Proton card), then the issuer is not liable in case of loss or theft of the instrument even when notice is given to the issuer, insofar as the amount that can be stored on the instrument is limited to EUR125. On the other hand, if the holder has used the instrument without having presented the instrument physically and without electronic identification (*e.g.*, by typing in his credit card number on a website), then the issuer is fully liable, even if the holder has not issued a notice.

Contractual provisions that deprive the holder from any of his rights or that relieve the issuer from any of his obligations set forth in the Act are legally void. The Act also provides the possibility to initiate a cease and desist action before the President of the Court of Commerce. In addition, a *mala fide* violation of the Act or the non-compliance with a judgment following a cease and desist action, can be sanctioned with a fine of between EUR500 and EUR20,000.

The Act enters into force on February 1, 2003, but some provisions become effective only on August 1, 2003.

Report by Erik Valgaeren and Frederic Debusseré of Stibbe, Brussels office; e-mail: erik.valgaeren@stibbe.be, frederic.debussere @stibbe.be.

COLOMBIA

Law Passed to Fight Online Paedophilia

A provision recently issued in Colombia obliges all information global network suppliers and administrators operating in the country to include a clause, expressly prohibiting the hosting of child pornography in all contracts entered into with content suppliers.

Indeed, Decree 1524 of July 24, 2002 prohibits suppliers, servers, administrators and users of information global networks from hosting any of the following on their sites:

- any image, text, document or audiovisual file showing, directly or indirectly, sexual activities involving minors;
- any pornographic material, especially in the form of images or videos if there are indications that the people who have been photographed or filmed are minors; and
- links to sites containing or distributing pornographic material involving minors.

Hence, suppliers, servers, administrators and users of information global networks operating in Colombia must:

- denounce before the competent authorities any criminal act performed against minors they may know of, including the dissemination of pornographic material involving minors;
- fight the dissemination of child pornography with all the means they may have available;
- refrain from using information global networks to disseminate unlawful material involving minors; and
- establish blocking mechanisms with which users can protect themselves and their children from unlawful, offensive or undesirable material involving minors.

In addition, all Internet service providers who may get to know about the existence of this type of content in their infrastructure must denounce it before the competent authority and remove it from the network.

The Ministry of Communications will sanction any suppliers, servers, administrators and users who violate these provisions, by imposing any of the following penalties:

- fines of up to one hundred monthly legal minimum salaries (approximately $11,500 dollars);
- suspension of the website; or
- closure of the website.

The Decree is a part of a general strategy devised by the government to prevent sex exploitation, pornography and sexual tourism using minors, who under Colombian legislation are all children and adolescents under 18 years of age.

Also as a part of the strategy, a government website, *www.dignidadinfantil.gov.co*, and a toll-free telephone

number, have been opened to receive the reports of unlawful material logged by service providers.

The Ministry of Communications has issued the decree in response to a recent report by UNICEF that there are some 10,000 sites on the net showing child pornography. Most of these children are given away to abusers by their own families who live in extreme poverty, in countries such as Colombia, Brazil, the Dominican Republic, Panama and Venezuela.

It is very difficult however, to fight online paedophilia. Studies have shown that 90 percent of web pages showing such content are designed to last just 24 hours, so it is almost impossible to access them once they have been denounced.

Additionally, the "chat rooms", access to which is free of charge and simply requires visitors to connect to the Internet and adopt a username (real or fictitious), are yet another problem that makes it difficult to identify the perpetrators of these crimes.

Report by Natalia Tóbon of Cavelier Abogados, Bogotá; e-mail: nataliatobon@cavelier.com.

EUROPEAN UNION

Website for Applications to Register E.U. Quality Products Launched

Applications for registration of a product as a Protected Designation of Origin ("PDO"), a Protected Geographical Indication ("PGI") or a Traditional Speciality Guaranteed ("TSG") can now be consulted on the website of the Directorate-General for Agriculture.

This new service, recently launched by the E.U. Commission, is aimed at simplifying the consultation procedure prior to registration of a PDO, PGI or TSG.

The current rules on the protection of geographical indications and designations of origin of agricultural products and foodstuffs, and the rules on certificates of specific character for agricultural products and foodstuffs, stipulate the Commission must publish the main characteristics of the application request in the Official Journal of the European Communities, at least six months before finally registering a product.

The publication of the application for registration confers the right to object to this request. Consequently, a transparent registration procedure is the pre-requisite for other parties concerned to exercise their right of objection. In order to facilitate the consultation of the requests published in the various issues of the Official Journal, all pending registrations can now be consulted online at: *www.europa.eu.int/comm/agriculture/foodqual/protec/firstpub/index_en.htm*.

The European Union created the PDO, PGI and TSG identification systems in 1992 to promote and protect food products from the unfair competition which can occur when a product's favourable reputation extends beyond national borders. This brings the original product into potential conflict with other products, passing themselves off as the genuine article and taking the same name as the original, which can discourage producers and mislead consumers.

Detailed information on products already registered as PDO, PGI or TSG can be found at: *www.europa.eu.int/comm./agriculture/foodqual/quali1_en.htm*.

FRANCE

French Postal Authorities Announce Offering of Electronic Register Letter

PARIS—French government-owned postal monopoly *La Poste* has announced plans to launch an electronic version of the old-fashioned registered letter later this year.

The new e-letter, to be accorded the same legal status as registered mail, will be phased-in over a trial period beginning in November 2002, according to *La Poste.*

The first stage will see the launch of a semi-electronic "hybrid" registered letter. This embryonic form – initially limited to corporate clients – will allow senders to file mail and pay electronically, after which *La Poste* will guarantee physical delivery.

A second stage, proposed for the first or second quarter of 2003, will open the semi-electronic registered letter to individuals, alongside a fully electronic letter – to be both filed and delivered electronically.

Marketing of the new electronic registered letter will take place at Internet sites run by *La Poste*: *www.laposte.fr* and *www.laposte.net*.

Product Enabled by E-Signature Law

While *La Poste* will guarantee delivery of this all-electronic registered letter, postal authorities will have no access to the contents of correspondence. Instead, *La Poste* will act as a trusted third party, ensuring the existence of content through the imprint of a coded algorithm and confirming reception through an automatic response mechanism.

In a statement announcing the electronic registered letter, *La Poste* said it was seeking to give Internet correspondence "the same formal value and legal security until now reserved for physical exchanges".

The new e-letter – made possible by recent legislation that legalised the electronic signature – will satisfy legal requirements for nearly all of the 217 million registered letters mailed in France each year, about 85 percent of which are filed by companies or the government (See *WILR Vol. 3, Issue 8, August 2002, "Electronic Signatures in France"*).

A survey by *La Poste* officials uncovered more than 2,400 specific acts that require a registered letter.

The e-letter will serve as proof in most all of these cases of a physical relay of information and content, offer a time/date stamp certifying when a transaction took place, and will eventually offer digital signature capacities, according to *La Poste*.

Further information on the new digital registered letter to be marketed by *La Poste*, is available in French at *www.laposte.fr*.

GERMANY

Amendment to the Broadcast State Treaty

On July 1 2002, the 6th Amendment of the Broadcast State Treaty (Rundfunkänderungsstaatsvertrag) came into force. It amends the Broadcast State Treaty (Rundfunkstaatsvertrag), the State Treaty of the Financing of Broadcasting (Rundfunkfinanzierungsstaatsvertrag) and the State Treaty of Media Services (Mediendienste-Staatsvertrag) ("MDStV"). The latter implements Directive 2000/31/EC on Electronic Commerce.

The major amendments that have been made to the MDStV are to the provisions concerning:

- liability for content (Articles 6–9);
- duty to supply information (Article 10);
- data protection (Articles 16–21); and
- sanctions for violation of the MDStV.

The provisions regarding liability for content are now more precise. In general, providers are liable for their own content and the content of third parties, if they have adopted the latter as their own. Providers, who either have a passive role as a "mere transmitter" of information obtained from third parties, or who grant access to the use of stored information, are only liable for the content if they have initiated the transfer, chosen the addressee of the transmitted information and chosen or changed the information (Article 7). The provider is also liable where he collaborates with the user to commit an offence. The newly inserted Article 8 limits providers' liability so that they are, in principle, not liable if they save information in cache memories to allow accelerated transfer. Those who store information of third parties, the so-called host-providers, are not liable for stored information unless they have knowledge of prohibited content or illegal use, or have knowledge of facts and circumstances, which indicate illegal content or use.

The amended Article 10 requires that all providers of media services supply mandatory information, including the name and address of the provider, which is to be made available in an easily accessible and permanent form. Furthermore, Article 10 requires that commercial media service providers supply information concerning their activities, such as their number on the commercial register, professional authorisation, VAT number, *etc.* It is important to provide the information requested, since otherwise competitors can serve letters of warning on the offending media service provider with an obligation on the media service provider to pay the costs.

With respect to data protection, the only substantial amendment is the newly inserted Article 19, Section 9, which permits providers of media services to process users' data and make use of it, or to forward it to third persons if they have an indication that the user is not willing to pay for the services.

Report by Brigitte Joppich, a partner with Linklaters.

INDIA

TRAI Recommends Establishment Of a National Internet Exchange

The Telecom Regulatory Authority of India (TRAI) has recommended that the government set up Internet exchange points (IXPs) across the country to increase the data access speed.

Concerned about the insufficient growth of Internet services in the country, the TRAI conducted an in-house study to determine the various barriers impeding Internet growth and also the main drivers of it. Following the study, TRAI assembled a multi-disciplinary Task Force to suggest the steps needed to trigger a faster growth of the Internet in the country.

The Task Force comprised a panel of experts from various government agencies, including the Ministry of Communication and Information Technology, the Centre for Development of Telematics, the Telecom Engineering Centre, the Indian Institute of Technology-Delhi and the TRAI. The brief for the Task Force was to prepare an action plan, aimed at fostering a higher rate of growth of the Internet in the country and to suggest plans for the setting up of Internet Exchange Points (IXPs).

The Task Force submitted its report at the end of August and the TRAI has since made its recommendations to the government. The key recommendation is for an implementable methodology to establish IXPs in the country.

Under the recommendation, the proposed exchanged, to be named the "National Internet Exchange of India" (or NIXI), would route the domestic traffic within the country to avoid its carriage abroad and back to India. Four initial IXP nodes, to be interconnected in ring architecture, have been proposed at Delhi, Mumbai, Kolkatta and Chennai.

It is hoped that NIXI would result in various tangible benefits for Internet users, as well as for the country as a whole, bringing down the cost of Internet connections and bandwidth, while improving the quality of the service and widening Internet use across India.

NIXI would also provide the country with an improved Internet infrastructure and save on foreign exchange on international bandwidth, boosting the economy and helping the local development of e-commerce.

Other recommendations by the Task Force included increased availability to cheaper access devices for Internet use, such as low cost indigenous PCs and Internet enabled second-hand PCs.

The government should also take steps to bring Internet service provider (ISP) services under the telecom infrastructure category, in order to decrease capital and operational costs for ISPs, the Task Force said.

Support for ISPs could also be provided by the government through the development of policy initiatives for the de-licensing of 2.4 GHz (ISM Band) for low power outdoor usage for last mile Internet Access, and for permitting the usage of Receive Only Satellite access by ISPs.

The Task Force also recommended that the government take steps to encourage the usage of alternative access technologies, such as Cable TV networks and W-LANs as well as the simultaneous provision of Internet access, along with voice in the local loop. It also highlighted the importance of implementing e-governance applications to enable citizens to access services online.

NEW ZEALAND

Legislation Online

The New Zealand Parliamentary Counsel Office (PCO), in association with legal publisher Brookers, has launched a new interim website of New Zealand legislation at *www.legislation.govt.nz*. The website provides free public access to current versions (with amendments incorporated) of New Zealand Acts of Parliament and Statutory Regulations.

The website is hosted and maintained by Brookers, and is updated monthly. The material on the interim website is unofficial, and is sourced from Brookers' own commercial product. Officially printed copies of legislation remain the only official versions of legislation.

The interim website is part of the Public Access to Legislation (PAL) Project, being undertaken by the Parliamentary Counsel Office with Unisys New Zealand Ltd. as its implementation partner. The aim of the project is to provide public access to up-to-date official legislation in both printed and electronic formats.

The interim website will be replaced in early 2003 with an official PCO website, providing free public access to up-to-date versions of New Zealand legislation, including Acts of Parliament, Statutory Regulations, and Bills before the New Zealand Parliament. Superseded versions of current Acts and Statutory Regulations will be retained on the site, to enable users to see what the law was at a certain point in time. Repealed Acts, revoked regulations, and superseded versions of Bills will also be retained on the site so that a collection of historical material is built up over time.

The material on the official PCO website will initially be unofficial, but it is intended that the website will eventually become the official source of New Zealand legislation. The PCO will "officialise" the material, and this is expected to take at least three years. This process includes the exercise of powers to make editorial changes so that the format and style of the legislative material is consistent with current legislative drafting practice.

Users of the official PCO website will be able to print copies of legislation from the website, as well as order online.

Further information about the PAL Project is available on the PCO website at *www.pco.parliament.govt.nz/pal*.

Report by Geoff Lawn, Deputy Chief Parliamentary Counsel and Project Director, Parliamentary Counsel Office, New Zealand; e-mail: geoff.lawn@parliament.govt.nz

PAKISTAN

Electronic Signatures Law Approved

The President of Pakistan, Pervez Musharraf approved the new Electronic Transactions Ordinance on September 11, 2002, providing Pakistan with a law that the government hopes will support and encourage the growth of e-commerce in Pakistan. The e-commerce industry has already expanded rapidly in the country and reports have estimated that around 10 per cent of all business-to-business transactions in Pakistan will be carried out electronically by the year 2004.

Dr Attaur Rehman, Minister for Science and Technology has referred to the new law as "a landmark decision for the IT development of the country" and an achievement for the incumbent government.

The new law provides legal recognition to electronic documents, records, information, communications and transactions, as well as recognising electronic signatures, which will facilitate electronic trading by providing protection for both buyers and sellers.

SWEDEN

New Regulations on E-Commerce

The Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the "Directive") has been implemented in Sweden, principally by the

enactment of the new Act on electronic commerce and other information society services (the "Act"). Further, a new provision regarding unsolicited commercial communication by electronic mail has been incorporated in the Swedish Marketing Practices Act ("SMPA"). The Act and the additional provisions in the SMPA came into force on July 1, 2002.

The Act includes, amongst other things, provisions regarding the free movement of information society services and that Swedish law is to be applicable when the services are provided by a service provider established in Sweden. Further, the Act lays down certain requirements regarding the information that must be provided in connection with the supply of services by electronic means, for example, general information about the service provider and clear and unambiguous price information. The Act also makes clear under which circumstances, service providers that act only as intermediaries shall be free from liability.

The Directive has also resulted in a new provision in the SMPA regarding unsolicited commercial communication by electronic mail. As the Directive does not deal with the question as to whether commercial advertising by electronic mail should be allowed or not, the Swedish opt-out solution will remain in force (*i.e.*, that entities are allowed to send unsolicited commercial advertising communications as long as the recipient has not explicitly refused such advertising). The new provision stipulates that service providers undertaking unsolicited commercial communications by electronic mail must consult regularly and respect opt-out registers in which people not wishing to receive commercial communications can register themselves.

Report by Malin Peterson of Linklaters

UNITED STATES

ICANN Alleges Verisign Engaged in Pattern of Inaccurate Domain Name Data Violations

The Internet's governing body on September 3, 2002 gave domain name registrar Verisign Inc. 15 working days to correct a "pattern of persistent violations" related to its failure to correct inaccurate data, or face possible termination of its right to sell .com domain name registrations.

The governing body, the Internet Corporation for Assigned Names and Numbers, said Verisign, headquartered in Mountain View, Calif., breached its Registrar Accreditation Agreement with ICANN 17 times in the past 18 months by failing to correct reported inaccuracies despite repeated requests by ICANN.

In response to the allegations, a Verisign spokesman said characterising 17 instances of inaccurate data and calling it a pattern is "somewhat specious" given the 10.3 million active domain names in Verisign's registrar.

ICANN made the allegations in both a formal notice on its website and in a letter from Louis Touton, ICANN's vice president and general counsel, to Verisign's Bruce Beckwith.

In that letter, Touton said Verisign had agreed to investigate and correct whois data in response to any reported inaccuracies.

Touton said, however, that it appeared that Verisign frequently publishes incomplete whois data, ignoring reports of inaccurate and incomplete contact information in its whois database.

Whois data gives the public information about domain name registrants, administrative contacts, technical contacts, and nameservers associated with each Internet domain name.

The data are useful for identifying and verifying online merchants, for investigations by consumer protection and law enforcement authorities, and for determining whether a domain name is available for registration, among other purposes, ICANN said.

The announcement about Verisign is the first formal notice issued by ICANN for any registrar on the accuracy of whois data, ICANN spokeswoman, Mary Hewitt told *WILR*.

Until 1999, Network Solutions Inc. – which was later merged into Verisign – had a government-sanctioned monopoly on the domain name registration market. One of ICANN's major roles after its creation in 1998 was to help introduce competition.

According to ICANN, in a May 2001 accreditation agreement, Verisign agreed to publish complete Whois data, to undertake reasonable efforts to investigate notifications of whois data inaccuracies, and to correct any inaccuracies found.

Verisign to "Immediately Correct" Discrepancies

Verisign spokesman Brian O'Shaughnessy said on September 3, that the company has always taken all of its obligations under its Registrar Accreditation Agreement seriously.

Verisign will immediately correct the 17 cases ICANN has pointed out, he said.

Verisign currently, and has for some time, taken steps to remind its customers of the need to maintain accurate whois data, O'Shaughnessy said. The company works with the law enforcement and intellectual property communities on a daily basis to correct inaccurate data, he added.

Among the discrepancies cited by ICANN are:

- failure to correct a whois entry showing a domain name registered to "Toto" with the address of "the yellow brick road" in "Oz, Kan.";
- failure to contact a registrant to correct data for six months after being notified of the incomplete data; and

- "numerous instances" of invalid telephone numbers or e-mail addresses for many months.

If ICANN does provide notice of termination of Verisign's agreement, Verisign may enter arbitration on whether the termination is appropriate, ICANN said.

Steps to Improve Whois Data Accuracy

Simultaneously to the announcement on Verisign, ICANN announced additional steps to improve the accuracy of Whois data.

In their original contracts with ICANN, 150 registrars that sell domain name registrations to consumers agreed to publish whois data about the domain names they register.

The new steps will include improved facilities for receiving and handling reports from the public about incomplete and inaccurate data, ICANN said.

Specifically, ICANN said it is implementing tools to streamline the process for receiving and tracking complaints about inaccurate and incomplete whois data, including a new, centralised online form available at ICANN's Internet website, *www.internic.net*, for reports on data for domain names in the gTLDs of .com, .net, and .org.

The form will be implemented soon for .biz, .info, and .name, ICANN said.

Reports received through the system will be forwarded to responsible registrars, and a tracking mechanism will inform registrars through periodic updates on outstanding reports of inaccuracies, ICANN said.

More information is available at the website of the Internet Corporation for Assigned Names and Numbers, *www.icann.org*.

UNITED STATES

Council of Europe Committee Push For Crime of Unlawful Website Hosting

A recent draft report by a committee of the Council of Europe's Parliamentary Assembly is trying to reintroduce the idea of "unlawful hosting" into the hate speech protocol to the Cybercrime Convention.

This concept has already been rejected during the negotiation stage, according to *WILR* sources, and it is unlikely to find its way back into the protocol.

The hate speech protocol – fully titled the Draft additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems – was itself created as a way of making the Cybercrime Convention palatable to the United States.

So as to avoid First Amendment problems, the hate speech protocol was created as an optional addendum for states that preferred to include prohibitions on racist and xenophobic speech on the Internet. This compromise resulted in a convention that the United States could sign; thus, the United States never planned to sign on to the protocol.

The body that drafted the protocol – the Committee of Experts on the Criminalization of Acts of a Racist or Xenophobic Nature committed through Computer networks – already considered the issue of requiring signatory states to shut down websites that direct hate speech towards a state where such speech is illegal, according to Jonathan Band of Morrison & Foerster, Washington, D.C.

Given that the issues have been fully hashed out by the delegations at the Council of Europe, it is highly unlikely that this concept will be re-introduced at this stage, in spite of the September 2 draft report of the Committee on Legal Affairs and Human Rights.

The draft report characterises the compromise that rejected inclusion of unlawful hosting as a bowing to the interests of one state, the United States, and strenuously argues for its inclusion in the hope that it would create a means for the United States to sign on.

First Amendment Not Fathomed

According to Band, those arguing for reconsideration have a fundamental misconception about the constitutional problem in the United States. They seem to believe that the U.S. government can ban websites that direct hate speech toward non-U.S. Internet users. However, the speaker's as well as U.S. users' rights would be unlawfully infringed by such action.

The interests in favor of the change seem to be upset by what they see as a loose hate speech protocol that does not mandate that signatory states criminalise any particular behavior.

> "They're concerned that the way the convention is drafted now, there's so many reservations that you could be a signatory and in essence agree to nothing", Band said.

Furthermore, according to Jeffrey F. Pryce of Steptoe & Johnson, Washington, D.C., since the United States has no intention of subjecting itself to the protocol, the current disagreement is really between two camps of Europeans.

On the one hand are continental European states such as Germany and France, which are interested in removing any access to sites that violate their hate speech laws. On the other hand are the English-speaking and Scandinavian states in northern Europe that are more concerned with preserving free speech rights.

Pryce also said he thought it was very unlikely that unlawful hosting could be re-introduced into the protocol, but if it were, it would be a concern to the United States even as a non-signatory because of the possibility of extra-territorial prosecution, such as in the Yahoo! France case.

UNITED KINGDOM

LEGITIMACY OF UNOFFICIAL FAN SITES CALLED INTO QUESTION

Hanna-Barbera Productions, Inc v. Graeme Hay

Nominet UK Dispute Resolution Service – DRS 00389, August 23, 2002

A recent decision of Nominet's Appeal Panel, reversing an earlier decision under the ".uk" Dispute Resolution Service Policy ("DRS"), has questioned the legitimacy of registering domain names which are, or incorporate, trademarks, even where they are legitimately used as tribute sites, with little evidence of bad faith. In spite of an earlier decision finding in favour of the fan site owner, Nominet's Appeal Panel has stated that *"honest intentions are not enough"*. The decision may open the floodgates for other brand owners to procure a transfer of domain names which they previously considered irrecoverable, on the basis that they were being put to "fair use" by third parties as tribute sites. The implications of that decision for fan sites operating under the *".uk"* tld are considered below.

Background

Graeme Hay had registered *scoobydoo.co.uk* and operated a Scooby fan site at that address. He used various metatags to attract visitors to his site, including "Shaggy" and "Scoobygang". Mr Hay offered a free e-mail address incorporating *scoobydoo.co.uk,* although claimed to make no profit from this. Mr Hay sold Scooby-Doo merchandise through the site, for which he received commission.

Hanna-Barbera Productions Inc ("Hanna-Barbera"), which owns various trademarks in the name "Scooby-Doo" as well as other Scooby-Doo characters (including certain names used as Mr Hay's metatags) brought DRS proceedings against Mr Hay in an attempt to have the domain name transferred.

Hanna-Barbera submitted, amongst other things, that the registration and use of the name was "Abusive" within the meaning of the DRS because Mr Hay was misrepresenting that he was connected with Hanna-Barbera, and his site was unfairly disrupting Hanna-Barbera's business and/or was unfairly detrimental to its rights. Hanna-Barbera also argued that Mr Hay had sought payment from Hanna-Barbera for a sum which exceeded his costs associated with the domain name.

In response, Mr Hay claimed, amongst other matters, that the name was registered in good faith as a legitimate fan site and included a disclaimer stating that it was an unofficial site. After he was contacted by Hanna-Barbera, Mr Hay also removed his online store saying that if he could not reach agreement with Hanna-Barbera, he would cease selling merchandise.

The Sole Panellist's Decision

Hanna-Barbera's claim that Mr Hay was misrepresenting to people consulting the whois database that he was the owner or licensee of goodwill in the mark, and connected with the Complainant was rejected, on the grounds that if this were correct, the additional requirement in the DRS for the registration to be "Abusive" would be otiose, and each domain name which was identical to a registered trademark – no matter how generic – could be transferred.

Hanna-Barbera noted that Mr Hay offered to sell the domain name for £3,000, a sum which both parties acknowledged exceeded his costs associated with the domain name. This sum included compensation for three years of Mr Hay's time and work. However, a mere offer for sale was not sufficient to succeed under the DRS; in order to show that the registration was Abusive, Hanna-Barbera still needed to show that Mr Hay's *primary purpose* in registering the name was for onward sale to Hanna-Barbera. To find otherwise would outlaw the buying and selling of domain names.

The Expert found that the onus was on Mr Hay to prove that his registration of the domain name was not Abusive. He referred to the example of a "sham" fan site, which in spite of ostensibly being a tribute site, would still constitute an Abusive Registration. An earlier Nominet decision concerning DISNEY demonstrated that a person wishing to re-sell domain names to brand owners at profit may use the "ruse" of a fan site in an attempt to prevent them from being recovered. However, in respect of *scoobydoo.co.uk*, the Expert found that selling the name was not Mr Hay's primary purpose.

Finally, the Expert considered whether Mr Hay's use of the site otherwise took unfair advantage of/caused unfair detriment to Hanna-Barbera. The changes made to Mr Hay's site over time were examined. Prior to being contacted by Hanna-Barbera, Mr Hay had sold merchandise through his site, but stopped shortly after being contacted by Hanna-Barbera. Mr Hay also inserted a disclaimer on his site confirming that the site was unofficial and was unconnected with Hanna-Barbera. A link to the "official" site was provided. Significantly, the Expert considered that the site's appearance should be judged at the time Hanna-Barbera filed its complaint, *i.e.* when Mr Hay had stopped selling merchandise, and the disclaimer was visible.

In his concluding remarks, however, whilst finding that Mr Hay's use of *scoobydoo.co.uk* was not Abusive, the Expert noted that if Mr Hay were still selling merchandise from the site, or if he had profited from the e-mail service, then his decision may have been different. He also said that Hanna-Barbera could file a fresh

Complaint if the sale of merchandise continued without agreement being reached or if other material changes to the site were made. Hanna-Barbera appealed.

The Appeal Panel's Decision

Like the Expert, the Panel accepted that Mr Hay's motive at the time of registration was to set up a tribute site. The subsequent offer to sell was merely a response to Hanna-Barbera's complaint, not an indication of bad faith. Accordingly, the Panel considered whether Mr Hay's *use* of the domain name was Abusive.

The panel noted that some of the site's reported 37,00 visitors may mistakenly have believed that the site was official. This was less significant if the Expert was correct, and the site should be judged at the date on which the complaint was filed. However, the Panel did not think this approach was correct. Instead, all use of the domain name – from its registration onwards – should be considered. This included use of the site before the disclaimer was inserted. The previous lack of a disclaimer exacerbated the mistaken impression that the site was official.

The Panel noted that commercial activity was not necessarily incompatible with tribute sites. The intention of the DRS was that a registration for the purposes of a tribute site would be Abusive, unless the owner of the domain name could prove otherwise. The sale of merchandise though the site did not prevent it from being "solely" in tribute to Scooby-Doo; rather, the trading was a reasonable ancillary activity.

The Panel decided to evaluate the purposes for which the domain name had been used as whole. It considered that the disclaimer was ineffective because by the time it was seen, Mr Hay had obtained a business opportunity that he would not otherwise have had. The choice of name was very significant; it was unnecessary for a tribute site's address to be identical to a mark. This arguably amounted to impersonating the brand owner, and this impression would be exacerbated by Mr Hay's sale of official merchandise. The Panel considered that Mr Hay had impersonated Hanna-Barbera and thereby secured an advantage (whether financial or otherwise), and that this was unfair.

Mr Hay's use of the domain name had exposed Hanna-Barbera to risk because its name, mark and goodwill were outside its control and the distinctiveness of its trademark rights was being diluted. As a result, the Panel considered that Mr Hay's use of the domain name took unfair advantage of or was unfairly detrimental to Hanna-Barbera, and directed that the name should be transferred.

Comment

It remains the case that, in domain name disputes, where there is evidence of cybersquatting, which necessarily involves an element of bad faith on the part of the domain name owner, it is more expedient for an aggrieved rights owner to invoke the relevant DRS, rather than commence lengthy and expensive litigation. However, this decision indicates that a dispute involving an unofficial fan site, particularly where the owner is engaged in certain activities (whether commercial or otherwise) which may arguably be at the expense of the brand owner, is also likely to be resolved in favour of the brand owner.

Similarly, it appears that the circumstances in which a site will be regarded as denigrating or operating at the expense of a brand owner will not just be, for example, in the context of "sucks" sites. The Panel attached considerable significance to the dilution of Hanna-Barbera's trademark rights by the network of users who obtained a *scoobydoo.co.uk* e-mail address, and the fact that Hanna-Barbera's goodwill was outside its control. While the Panel differed as to the significance of Mr Hay trading through the site, it was acknowledged that by selling official merchandise, Mr Hay may have encouraged visitors to believe they were visiting an official site.

The decision also raises some interesting issues about the meaning of "fair use". Those wishing to operate tribute sites would be well advised to be circumspect and register domain names that are not identical to trademarks, such as *ilovescoobydoo.co.uk*. This means that a Complainant would need to show, first, that the domain name was similar to its mark, and second, it would find it more difficult to argue that there had been a misrepresentation, which had confused Internet users as to the origins of the site.

The considerable debate about the date on which the site should be assessed also raises interesting issues; it is likely that changes will be made to a site during the course of a dispute. This illustrates the importance for those aggrieved by a third party's use of a site to ensure that evidence of the changing appearance of the site is kept. In this regard, the view of the Appeal Panel seems correct. The DRS requires the manner in which the domain name has been used to be considered, and it seems implicit that this requires all use of the domain name to date to be looked at, rather than a "snapshot" of its appearance at a particular date.

The decision of the Appeal Panel was given on August 23, 2002, and interestingly, at the time of writing, Mr Hay's site is still live and contains links to the official site, the site connected to the recent "Scooby-Doo" movie, as well as the opportunity to acquire a *scoobydoo.co.uk* e-mail address. It remains to be seen whether Hanna-Barbera has learnt to live with unofficial sites…..

Report by Katie Withers, a solicitor in the Intellectual Property department of Eversheds; e-mail: katie.withers@eversheds.com

UNITED STATES

CYBERSMEARING

ZixIt Corp. v. Visa International

District Court, Dallas, July 31 2002

The Dallas-based ZixIt Corporation (now known as Zix) announced at the end of July 2002 that they had lost their long awaited action against Visa USA, Inc. and Visa International Service Association, which had been

proceeding in the courts in Texas since 1999. The case, decided by a judge and jury, is probably the biggest cybersmearing case to date with a claim against Visa of $699 million.

The case concerned an allegation by Zix (an Internet start up credit-card processor), against Visa, over 437 message board postings made by one of Visa's Vice Presidents on a Yahoo! message board, relating to Zix's stock.

The postings dated back to 1999 when Zix was trying to raise funding. When proceedings were issued, Zix alleged that they had met with credit card executives on May 17, 1999 to discuss their plans and that just two days later, the smearing campaign began.

The court heard how Visa's executive, Paul Guthrie, "set out on a mission" to undermine the company challenging Zix's own information and urging those who had already bought stock to sell "before it's too late". Guthrie had posted 437 messages before being caught. Zix alleged that he used at least seven different aliases and that the day Visa were warned about the messages, the postings ceased. Zix said that the messages included such defamatory comments as:

> "[ZixIt] is the result of a big April fools joke…. or perhaps the outcome of a three day tequila binge and drunken-bet payoff…."
>
> "…none of these financial institutions who [ZixIt] is so dependent on will touch them."
>
> "Everything [ZixIt] has presented has been done well by someone else, and in many cases for years by strong consortiums…of industry players."

Zix alleged that Visa used Guthrie as its agent in its online campaign and then started an offline campaign against it using other employees.

Zix sued Visa (but not Guthrie) for $699 million in damages. Visa argued that Guthrie had not acted as their agent and called him to give evidence on their behalf. He said that he had acted alone and according to Visa's counsel, "The jurors concluded that he really was off in his own world". Visa said that whilst they had moved Guthrie within Visa after the incident, they could not sack him because of First Amendment issues unique to California.

Zix's Vice President testified that Guthrie's postings contained 592 lies. Visa analysed the postings and in court argued that of those, 20 were true or had been taken out of context. In addition Visa introduced expert testimony with poster-sized charts and graphs to try and persuade the jury that the postings had not had an adverse affect on Zix's share price.

The trial lasted three weeks with jury deliberations of two and a half days before the case against Visa was dismissed. The jurors found that Guthrie was not acting in the scope of his employment.

Whatever the result of the case, the tale is a sorry one for all three parties. We do not know whether separate proceedings will now take place against Guthrie. We do know however, that harmful allegations were made in court about both companies and that each of them will have significant irrecoverable costs.

Whilst this case is maybe the highest profile case of its type to date, we are seeing an increasing number of cybersmearing cases come to court, and an even higher number reach the desks of lawyers. Cybersmearing is not confined to technology companies or those who are publicly quoted, although clearly both are more vulnerable. Cybersmearers can on occasion do more damage with companies whose profile is lower than it should be on the Internet – this can happen as the company concerned will not rate highly in search engine rankings and as a result is easy prey for a cybersmearer with even limited technical ability.

To avoid similar incidents happening to them, companies need to nip this type of activity in the bud. To protect their online reputation, organisations need to monitor what is being said about them online and act where appropriate. Executives in an organisation also need to be reminded via a company's acceptable use policy that disparaging rivals, however well intentioned, will not be tolerated.

Report by Jonathan Armstrong, Eversheds; e-mail: jonathanarmstrong@eversheds.com

UNITED STATES

ISPS' HTML AND INTERNET HYPERLINKING DO NOT AS A MATTER OF LAW, INFRINGE ON BT PATENT

British Telecommunications PLC v. Prodigy Communications Corp., S.D.N.Y., (Docket No. 00 Civ. 9451 (CM), 8/22/02)

U.S. District Court for the Southern District of New York, August 22, 2002

An Internet service provider that gives users access to web pages that incorporate hypertext markup language and hyperlinking, does not, as a matter of law, infringe on a patent for an information retrieval system, the U.S. District Court for the Southern District of New York has ruled.

In comparing the Internet to the patent claims as constructed previously, the court found that web servers are not "central computers", that HTML files are not "blocks of information" and that uniform resource locator addresses are not "complete addresses".

The plaintiff, British Telecommunications PLC, had filed a patent infringement suit, alleging that a patent awarded to it in 1989 was being infringed by Internet service provider, Prodigy Communications Corp.

The patent in question (U.S. Patent No. 4,873,662) – originally filed in 1976 in the United Kingdom – describes a

> "digital information, storage, retrieval and display system comprising: a central computer means in which plural blocks of information are stored at respectively corresponding locations, each of which is designated by a pre-determined address".

In executing the two-step inquiry for analyzing a patent infringement claim, the court first held a hearing pursuant to *Markman v. Westview Instruments Inc.*, 52 F.3d 967 (Fed. Cir. 1995), to construe the claims to determine their scope and meaning.

Turning to the next step of the inquiry, Judge Colleen McMahon proceeded to compare the allegedly infringing device against the claims as construed previously, and determined that as a matter of law, no jury could find that the defendant's device was infringing.

In order to infringe on a patent, a device must "embody every limitation of the asserted claims". The court examined, in particular, three aspects of Internet access that British Telecommunications claimed showed that it was encompassed by its patent.

Servers Not "Central Computers"

First, the court rejected the plaintiff's argument that "[e]ach web server on the Internet is a 'central computer' " as defined by the patent.

There is no central computer that stores information for access through terminals on the Internet, the court said. Information is stored on a multitude of servers and Internet users may access information from any of those sources. The court rejected the plaintiff's argument that under its patent, there could be several central computers from which information could be accessed.

> "The patent claims as construed clearly provide that the central computer is one device, in one location", the court said. "Just as a circle has but one center, hub-and-spoke networks have only a single hub."

This fact makes the Internet basically different from the device described in the plaintiff's patent, the court said, rejecting the plaintiff's characterisation of this as merely an "addition" to the patent.

Furthermore, the Internet could not be characterised as a functional equivalent of the patented device, the court said. In the patented system, all users are connected to a central computer; in the Internet, users are not all connected to Prodigy's server.

> "Indeed, the Internet is the very antithesis of a digital information storage system having a central computer", the court said. "The opposite of a claim limitation cannot be considered its equivalent."

Information Storage System Differs

Next, the court found that the Internet is not comprised of blocks of information as described by the patent. In the patented storage retrieval system, all information is neatly collected into two-part blocks, the first portion containing information for visual display and the second portion containing complete addresses for other blocks of information referenced in the first block.

A page of HTML data does not work like this, the court said. One Web page is a hodge-podge of various kinds of data, including information meant to be displayed and links to other pages referenced in the text.

> "Unlike the blocks of information required by the ... patent, HTML code, which is the primary language of the World Wide Web and of the Prodigy Internet Service, does not use blocks", the court said. "HTML code does not separate displayed information into a first sub-unit, and non-displayed information in a contiguous, separable second sub-unit. Rather, HTML code contains information to be displayed intermingled with other information concerning formatting and liking, such as URLs and anchors."

The court rejected the plaintiff's argument that the patent could be read to extend to this manner of storage. It was a basic characteristic of the patent that the information be neatly separated in pairs.

In rejecting the plaintiff's argument that a web page could be constructed in such a way as to meet this definition, the court cited from case law the principle that just because a device could be used in such a way as to infringe did not raise a genuine issue of material fact upon which a jury could rule.

The court further pointed to the fact that the plaintiff was not able to enter into evidence any page other than one constructed by its expert specifically for this action that was written in such a paired manner.

URLs Not Actual Addresses for Data

Finally, the court determined that URLs were not "complete addresses", such as those used in the pairs of information described by the patent.

In coming to this conclusion, the court focused on the fact that a URL does not describe the actual physical location of a piece of information. It merely references the information in such a way that it can be found by looking up references on databases:

"A URL contains names – or virtual addresses. It then points to several other sources of information that must be obtained to determine a complete address:

- the user's computer must first attempt to translate the URL server name into an IP address, by reference to other information in the form of either the external DNS service or locally-cached DNS information;
- when communication with a content server is achieved, the relative path contained in the URL must be translated using other information in the form of the configuration file of the content server to identify an actual path; and
- the actual path must be referred to other information in the form of a lookup table on the operating system's file system to determine a physical address for the requested information."

British Telecommunications was represented by Albert J. Breneisen, Benjamin Hershkowitz, Edward J. Handler, and Robert F. Perry of Kenyon & Kenyon, New York. Prodigy was represented by James I. Serota of Vinson & Elkins, New York; and Willem G. Schuurman, Andrew G. DiNovo, David B. Weaver, Avelyn Ross, and David E. Killough of Vinson & Elkins, Austin, Texas.

The text of the court's opinion is available at http://pub.bna.com/eclr/009451.pdf.

COMMENTARY

CHILE

Electronic Documents and Signature Law in Chile

By Fernando Castro and Cristóbal González, of Cruzat, Ortúzar & Mackenna (Baker & McKenzie – Santiago de Chile office); e-mail: fernando.castro@bakernet.com; cristobal.gonzalez @bakernet.com

As the use of the Internet for business has steadily grown, various legal concerns have arisen regarding the negotiation and execution of documents in electronic or digital format. In connection with electronic transactions and electronic data interchange ("EDI"), issues have arisen with respect to parties' identities, document security, transaction enforceability, *etc.*

Chile, like many countries around the world, has passed legislation to address these issues. In April 2002, the Chilean Congress enacted a law regarding "Electronic Documents, Electronic Signature and Certification Services of such Signatures". This law is based on similar legislation in other countries, such as: the United Nations Commission on International Trade Law's (UNCITRAL) model law; Spain's Real Decree 14/1999; the German Digital Signature Law; the United States law regarding Electronic Signatures in Global and National Commerce; and various European Union Directives. As with other jurisdictions, the purpose of the Chilean law is to guarantee the authenticity, integrity, non-repudiation, and confidentiality of the electronic document.

In addition to this legislation, there are other special laws in Chile, which address electronic issues, such as the use of electronic evidence in criminal procedure contained in the Criminal Procedure Code and in connection with the filing of income tax returns (Resolution N°09 of 2001, Internal Revenue Service).

The Chilean Law

On April 12, 2002, after several years of discussions, parliamentary negotiations, definition of technologies and development of regulations, Law No. 19,799 regarding "Electronic Documents, Electronic Signature and Certification Services of such Signatures" (the "Law") was published in the Official Gazette. With the purpose of providing legal certainty in electronic transactions and to update Chilean legislation with technological developments, the Law regulates the legal effects of electronic documents, the use of electronic signatures, both in the public and private sectors, as well as the certification of these signatures.

In order to implement the Law, on August 17, 2002, the Regulations promulgated with respect to the Law were published in the Official Gazette, giving full force and effect to the latter. The Regulations refer, amongst other issues, to:

- the requirements necessary to become a certification service entity, as well as the requirements that such entity shall be required to adopt in order to be accredited as such by the corresponding authorities;
- the requirements and procedures necessary to authenticate advanced electronic signatures certificates issued by non-resident entities; and
- the form, contents and effects of suspended or revoked electronic signature certificates.

The following are brief descriptions of the main issues regulated by the Law:

The Electronic Document and Signature: Technological Neutrality Principle

An "electronic document" is any representation of a fact, image or idea whether created, sent, communicated or received by technological means and stored in a proper way in order to allow its future use. On the other hand, an "electronic signature" is defined as any sound, symbol or electronic process, which allows the recipient of an electronic document to formally identify its author. If the electronic signature is:

- certified by an accredited certification entity; and
- if it has been created by using technologies under the exclusive control of the user in such a manner that the signature can only be linked with the latter, allowing the detection of any subsequent amendment, verifying the identity of its signatory and preventing the lack of recognition of the authenticity of the document or its author,

the electronic signature is deemed as "advanced".

Authorities have considered that the Law is not limited to a specific technology, allowing the same to keep its full force and effect before new technology developments. Notwithstanding the foregoing, it appears that the Law has restricted itself to the digital signature and *PKI* or *cryptographic* system (Public Key Infrastructure) and does not utilise a much more secure and reliable system, which is based in the retina or fingerprint identification (the *biometric* system).

Validity of Documents Executed by Electronic Signature

Documents and contracts executed by means of electronic signatures are fully valid and produce the same effects as and are the "functional equivalent" of those

executed on paper. Consequently, electronic documents are deemed as written and electronic signatures as hand-written for any legal purpose. The aforementioned does not apply to those acts subject to formalities that cannot be accomplished by an electronic document, to those acts where personal appearance of one or both of the parties is required by law, and to acts concerning family law.

Regarding public electronic documents, they must be executed by means of an advanced electronic signature in order to guaranty the integrity and authenticity of said document.

Evidentiary Value of Electronic Documents and Signatures

One of the main aims of the Law was to permit electronic documents to be submitted as evidence in a trial and, although it specifies the different value that different electronic documents shall have as evidence in court, the Law does not provide clear regulations on the means by which these documents may be submitted before a judge. This is a vague area that practice and jurisprudence should resolve with time.

According to the Law, documents executed with advanced electronic signatures, whether public or private, are deemed as a mater of law to have been executed without requiring any further evidentiary showing. On the other hand, private electronic documents executed with simple electronic signatures shall have such evidentiary value as provided by general rules of evidence. Accordingly, the importance of the advanced electronic signature contained in a document basically lies on the evidentiary value attributed to said document in a trial.

Electronic Signature Certification Services

As mentioned above, in order for an electronic signature to be qualified as "advanced", it must be certified by an accredited certification entity. Only legal entities, whether national or foreign, public or private, may perform electronic signature certification services. Additionally, in order to be an "accredited" certification entity, it must:

- be domiciled in Chile;
- evidence, before the relevant authorities, the possession of the necessary means and resources to grant electronic signature certificates under the terms and conditions provided by Law; and
- hire and maintain an insurance policy for damages based on any civil responsibility that may arise, the minimum amount for which is approximately of US$115,000.

Accredited certification entities must be registered in a public registry kept for such purposes by the Economy, Development and Reconstruction Ministry and are subject to its surveillance faculties.

Regarding public entities, certification of advanced electronic signatures of the authorities and officials shall be performed by the person qualified by law to perform such certification, notwithstanding the possibility that accredited certification entities may render such services when deemed convenient by the relevant public entity.

Certification service entities must respect and fulfil the obligations established in the Chilean Consumer Protection Law N°19,496, and Personal Data Law 19,628.

Limitations on Electronic Signature Certification

Electronic signature certificates granted by a certification entity may contain limitations regarding the use of the certificate, provided that said limitations may be recognised by third parties. Additionally, electronic signature certificates are only valid for a limited period of time, which shall not exceed three years from the issuance date of the certificate.

Certification Services Liability

Certification services entities are liable for damages caused in the performance of their services, and accordingly must use proper care in connection with such performance. Notwithstanding the aforementioned, certification entities are not responsible for damages arising from misuse or fraudulent use of an electronic signature certificate and, in no case, the liability of an accredited certification entity shall compromise the pecuniary responsibility of the State.

Electronic Signature Users' Rights

The Law grants the following main rights to the electronic signature users:

- the right to be informed (of the terms and conditions of the certification services, of the specific conditions and limitations in the use of an electronic signature certificate, of the cessation of the services rendered by the certification entity, to access by electronic means to the public registry of accredited certification entities, of claims procedures, *etc.*);
- the right to confidential treatment of information provided by electronic signature users to certification entities;
- the right to convey their data to another certification entity; and

the right to be indemnified in case of damages.

■ ITALY

Online Auctions in Italy: The Current Legal Framework in the Private and Public Sector

By Alessandro del Ninno, Studio Legale Tonucci, Rome; e-mail: adelninno@tonucci.it

Introduction

In Italy there is a particular situation with regard to online auctions. Article 18, para 5 of the Legislative Decree of March 31, 1998 No. 114 "Reform of the discipline of Commerce" provides that

> "… selling auctions operations carried out by means of television or other means of communications are prohibited".

The expression " other means of communications " also includes the Internet.

The violation of Article 18 L.D. 114/98 is sanctioned by a penalty fine of between EUR2,582 and EUR15,493.

The reason for the prohibition is that in Italy, the legal framework related to "auctions" considers this kind of operation as involving public interests (*i.e.*, the protection of the socio-economic contest and guarantees for the participants).

So, the compulsory general requirements underpinning the hosting of auctions are:

- the physical localisation of the auction operations (*i.e.*, the establishment/licensing of a physical place where the auction is held); and
- the concomitance of the auction operations (*i.e*, the concurrent physical presence of both the auctioneer and the subjects attending the auction).

These requirements are not directly provided for by specific legal provisions, but they can be clearly deduced in Article 534 and the following articles of the Italian Civil procedure Code and in Articles 72 and 79 of the Regulation of State Accounting – Law of May 24, 1924 No. 827 (which provides for the physical presence of the auctioneer in the operations).

It is clear that these requirements cannot be fulfilled if an auction is carried out online, being almost impossible to establish the localisation of the physical place where the operation is conducted.

It must be highlighted however, that these rules apply only to public auctions and not to private ones (private online auctions included).

Moreover, the "Consolidation Act containing rules for Public Security" (Law of June 18, 1931 No. 773, Article 115 and its Regulation of execution of May 6, 1940 No. 635, Article 205) provides that a public security licence is required to conduct both public and private auction operations. Such a licence can be granted by the Police Superintendent but only if it is possible to carry out both a preventive control and a successive control on the place where the auction operations are conducted and on the operations themselves (again, such a licence could not be granted for private online auctions, given the presuppositions).

In spite of this legal framework in Italy, there are several auction websites. The subjects who manage these websites try to get round the legal prohibitions by means of the following considerations and interpretations of the law, which mean that from a legal point of view, there is no organised "auction" by the manager of the site and thus no breach of Article 18 of Legislative Decree 114/1998):

- the website is only a web space placed at the disposal of users to conduct auction operations by themselves;
- the auction website is only a means through which to carry out selling operations on behalf of Third Parties;
- the manager of the website is not an auctioneer but only a mediator who puts Third Parties in contact;
- the website is only the online seat for a telematic service within a relationship qualified as contract of services.

Hosts of such sites also choose to interpret that Article 2 of the Legislative Decree of May 22, 1999 "Implementation of Directive 97/7/CE related to the protection of consumers in the field of distance contracts" clearly provides that its discipline shall not apply to distance contracts concluded in occasion of an auction. It can be deduced therefore, that distance contracts (including those conducted via the Internet) concluded in occasion of an auction, are licit and provided for under Italian law.

It should be pointed out however, that the above considerations have not been deemed acceptable by the public authorities. Indeed, the government has recently imposed heavy financial penalties on some of the well-known auction websites for violating the laws on conducting online auctions (Article 18 L.D. 114/1998).

New Rules for Online Auctions

On June 17, 2002, the Minister of Productive Activities enacted the important Circular No. 3547, containing clarifications about the discipline introduced by the Legislative Decree of March 31, 1998 No. 114 with regard to online auctions.

Article 18 of LD 114/1998 provides that:

> "The operations of selling carried out by means of TV systems or by means of other communication systems [including the Internet] are prohibited".

According to this rule, online auctions in Italy are now considered absolutely forbidden.

The introduction of Circular 3547 (available at *www.minindustria.it/pdf_upload/documenti/phpwFwVat.pdf*) has provided clarification that the prohibition regards the "special kind of selling by retail" (including by websites). This means that all the subjects that do not fall within

the definition of "commerce by retail" provided by Article 4, para 1 (b) of LD 114/1998, are exempt from the prohibition.

So the prohibition to organise and manage online auctions as a special kind of selling, shall not apply to:

- wholesalers;
- any other operator who does not sell to final consumers; and
- subjects selling goods to final consumers, but not by carrying out "*commerce by retail*" activity: *e.g.*, farmers and sellers of agricultural products, craftsmen, *etc.*

With regard to the subjective and objective requirements (for the subjects mentioned in the points above) related to selling activities by means of online auctions, the Consolidation Act on Public Security Laws shall apply.

With regard to the carrying out of online auctions, the Ministry of Productive Activity Circular No. 3547 of June 17, 2002, contains some rules about the fulfilments and information to be indicated on the related website.

Information to be Displayed for the Purpose of an Online Auction Procedure

According to Article 5 of E.U. Directive 2000/31, the Auctioneer must indicate on the website:

- the business name of the company;
- the geographical address of the office;
- the number of registration to the Chamber of Commerce (including the place where the related Chamber of Commerce is located);VAT number and fiscal code;
- an indication related to the protocol number (or similar) of all the authorisations, communications, licences and similar necessary to carry on the activity, including the indication of the Body who has enacted the mentioned acts;
- evidence of enrolment in professional Registries or Listings (only if a subjective legitimation aimed at carrying on the related activity is compulsory), including the name of the enrolling Body;
- contact information for the site operators, including e-mail addresses.

Subjects interested in participating in the online auction must be previously and exactly informed about the following:

- the type of auction it is (see para 3.3 of Circular 3547);
- specific procedures of the auction;
- the process of determination of the price;
- rules related to the adjudication and the related communications;
- information about the delivery and the payment of the goods; and
- time limits of the auction and its result.

Requirement for Indication of Prices in Online Auctions

The Ministry of Productive Activity Circular No. 3547 of June 17, 2002, has established some fulfilments and indications related to the prices of the good or services sold in online auctions.

First of all, para 5.1 (c) of Circular 3547 provides that participants to the auction (both sellers or buyers) must be clearly informed about the specific process of determination of the price (para 3.3 of the Circular mentions five modalities according to which the price can be determined, subject to the different kind of auction being carried out).

Secondly, it is provided that all the participants are prohibited from behaving in such a way as to alter the process of determination of the price (*i.e.*, behaving in such a way as to alter the selling prices or simply to try to alter the selling prices or the other contractual conditions related to the offer).

Furthermore, the auctioneer must provide a specific insurance coverage related to the price of the item or service sold by means of an online auction, so that the buyer can be reimbursed if the item/service purchased is lacking in the characteristics presented on the website.

All the operations must be recorded by the auctioneer in specific logs, including the information related to the final price paid by the buyer.

Finally, with regard to the determination of prices, the Circular provides that e-commerce operations (including online auctions) are excluded from the prohibition of underselling set forth in the Ministry of Productive Activities Circular of October 24, 2001 No. 3528/C.

Online Auctions in the Italian Public Administration

With regard to online auctions as a means to the purchasing of goods and services by the Italian Public Administration, a Regulation for e-procurement procedures in Public Administration entered into force on May 30, 2002 (Regulation No. 101 of April 4, 2002, published in the Italian Official Journal of May 30, 2002 No. 125 (see *www.innovazione.gov.it/ita/intervento/normativa/dpr_020404.shtml*).

The Regulation sets out the criteria for the carrying out of online auctions (e-procurement) by the Public Administrations. Until recently, online auctions – for a comprehensive economic value lower than the E.U. limit of EUR200,000 – have been informally carried out. According to the new Regulation, it shall now be possible to proceed beyond the current experimental phase, exploiting all the advantages of the purchasing of goods and/or services by means of telematic devices.

The Regulation aims to achieve a sensitive reduction of costs, expand the market to several players (*i.e.* all the companies or other entities able to provide goods and services to the Public Administrations) and establish transparency of the bids. Furthermore, the Regulation introduces the so-called "electronic market", a kind of supermarket where qualified suppliers may display their catalogue, determining an irrevocable offer to sell. The interested Administration shall evaluate the most advantageous offer and shall immediately sign the supplying contract online, by means of a specific procedure based on the use of an electronic signature.

With the introduction of these new measures, savings of more than EUR2.5 billion on the costs of the procedures employed by the Public Administrations in purchasing goods and services have been estimated by 2005.

INDIA

E-Business Regulation: Notes on Compliance Issues in the "Borderless Economy"

Rodney D. Ryder, a Senior Consultant with the IT, Media and Telecommunications Law Division of Anand & Anand in New Delhi; e-mail: rodney@anandandanand.com

Achieving legal and business order in cyberspace is another development that has been made possible by increasingly sophisticated technological advances.[1] For businesses keen to gain ground in this new environment, the Internet can be intimidating; it is also an indispensable tool and one that is essential for business success.

The issue of regulation is replete with unanswered e-business issues that need to be clarified as companies operate electronically across the globe. Some of the regulatory issues facing businesses are as follows:

- Whose law governs contracts that are formed online? Are contracts valid without a physical signature? Do the same laws apply to both consumers and businesses?
- Can the actual electronic transmission between countries be subject to taxes or tariffs? Are product and service sales treated the same under local law? Who decides?
- What are acceptable forms of online promotion? Are firms with websites that link to other sites using questionable tactics, putting themselves at risk?
- When the buyer sends his address and phone number to the seller, whose laws determine the restrictions on the use of that data? How is the seller's credit card number protected? Who is empowered to address disagreements that might arise?
- What tariffs and taxes are due? How are they accounted for and paid?
- What transaction crosses a border, what consumer protection is available? What additional risks do sellers assume?
- What happens if the seller does not get paid? Where do consumers return damaged goods purchased online? Does business-to-business commerce operate predictably across all trading jurisdictions?
- How can buyers and sellers enforce their rights in foreign countries? What international treaties apply? Does enforcement differ geographically? By product or service type?
- Many laws applicable to global e-business are not yet clear. Does it make sense to move aggressively to gain first mover advantage, or wait? How can an individual company protect its interests?

Business in the new economy will mean that traditional business approaches do not necessarily apply when viewed through the lens of the digital environmental. E-business is a completely different way to transact ordinary business. Since new, unfamiliar business practices are routinely scrutinised by governments and regulatory organisations, one can expect continued regulatory review, especially where consumer protection and economic welfare are at stake.

E-business shrinks the optimal regulatory action. New business arrangements with wide-ranging impact can now take effect in months, not years. This rapid change means that regulatory issues must be addressed early on to avoid overly "reactive" responses that can be counterproductive.

E-business effectiveness depends on a regulatory environment that is both supportive and predictable. While onerous rules can be stifling to business interests, regulatory indecision can be similarly disruptive. In order for e-business to work best, business must accept equal responsibility with governments to point the way.

Companies, Industry 'Vigilance' and Audits

Companies must remain vigilant, both to protect their business interests and ensure that they can proceed securely in uncharted territory. While some maintain it is unrealistic to have no restriction whatsoever on e-business, others oppose the restrictions various bureaucracies might place upon business conducted via the Internet. Most are hopeful that industry, driven by market forces, will ultimately regulate itself. If that fails, however, a wide range of regulators can be expected to step in forcefully.

Perhaps industry groups could identify potential and real 'hurdles' and attempt a solution. The vast majority of regulatory hurdles facing Internet businesses today relate to traditional considerations, whose scope and application are transformed by the global character of the electronic market. The industry needs to examine and be aware of key international issues, such as:

- international trade and tariffs;
- data security;
- encryption;
- infrastructure and access;
- intellectual property rights;
- liability: choice of law and jurisdiction;
- content;
- competition law;
- self-regulation; and
- privacy

and identify the major international institutions that are addressing them.

Web Audits and Commercial Strategy: an Advantage

According to Internet surveys, the fastest growing websites are those that provide a place for personal expression, such as chat rooms, message boards, e-mail

and personal web pages.[2] In addition, "e-tailing", or retail sales over the web have far exceeded industry expectations. Not surprisingly, many companies are launching websites to establish their presence on the Internet and to introduce themselves to the emerging online consumer market.

In so doing, many of these companies enter into new businesses, and some may enter into regulated industries. Each of these website owners – whether they are software vendors, search engines, banks or auction houses – becomes a publisher, in addition to their original core business. And, because of the competition to offer more and better services on the web, Internet companies frequently move from their core business to entirely new ventures as sales agents, financial information providers, mail providers, and more. This article outlines some of the issues arising from operating a website in India and offers some suggestions to minimise legal risk.

For a variety of reasons, initial and periodic legal audits for content liability issues on a website play an important role in managing a company's risk on the Internet. First, for website operators located in India, there are a number of constitutional and statutory protections for these "New Media" publishers, similar to the protections long enjoyed by traditional publishers, such as newspapers, magazines and television or radio broadcasters. The same probably applies for new media laws worldwide. Indeed, the U.S. Supreme Court determined that, online "speech", or content, should enjoy the highest level of constitutional protection.[2] As part of the audit, websites should also be reviewed for compliance with legislation regulating Internet content, commerce and conduct.

Secondly, websites generally contain a mixture of content – some of which may be generated by the site owner, but often, is not. An audit identifies the different types of content and the different risks associated with each type, and creates risk management strategies to protect the company.

Finally, the most successful websites are highly dynamic; that is, the content is not only interactive but constantly growing, and therefore changing. A good audit identifies "hot spots" on a site that are more likely to draw complaints or have greater exposure. Given the uncertainty of the law with regard to the Internet, a primary objective of risk management is to "marginalise" the potential plaintiff's success. An audit may provide guidelines for dealing with particularly complex areas, such as chat rooms or message boards, e-commerce transactions and user privacy. A great deal of thought and practical judgement are necessary to conduct a legal audit of website content.

Where to Begin: the First Steps

A website audit begins with a survey of the site – identifying the types of content and services provided on the site, the types of terms of service or legal disclaimers needed, the intellectual property rights, and the potential hot spots that are likely to give rise to liability. Typically, this phase of the audit requires discussions with the staff responsible for the site's content to determine how content is generated, which areas are the subject of complaints and what policies exist to handle complaints.

Depending upon the company, websites fulfil different and often multiple functions. Some sites are essentially advertisements that bolster brand identity, describe the company's product or services and provide investors or shareholders with information. Others fulfill traditional media functions of providing news, entertainment or other content (such as financial information or classified ads). Many of the largest sites have moved toward building online communities – sites that draw users back again and again. These sites offer a variety of services, including search engines, e-mail, chat, message boards, and commercial services – such as travel, brokerage and retail. The breadth of an audit depends to a large extent on the complexity of the site.

Content and Control: a Guide for Businesses

Original Content

Website content which is entirely or mostly generated by the website owner often presents the least complex liability issues. These issues are substantially similar to liability issues that a newspaper publisher has when publishing its daily paper or that a company has when publishing its prospectus or retail catalogue. Like their traditional media counterparts, website owners in India enjoy the significant legal protection available to publishers. Generally, website owners should review their content for accuracy, fair advertising practices, intellectual property rights and Securities Exchange Commission and other regulatory related issues.

Licensed Content

Many websites license content rather than create their own. An audit therefore, may also include a review of the licensing agreements to ensure that the website owner has the rights it needs to distribute, alter, republish or otherwise use the licensed content. In addition, the audit should review all representations and warranties for the content and any appropriate indemnifications by the licensor.

Third Party Content

As interactivity becomes a primary draw for bringing back Internet users, more sites are including chat, message boards, e-commerce and e-mail at their site. As a result, much of the content in these areas is created by users of the site and cannot as a practical matter be reviewed or edited by the website owner. Not surprisingly, while user-created content draws the most interest, it also draws the most complaints.

Linking and Framing

The practice of linking to or framing other websites raises liability issues unique to the Internet. A website owner may be found liable for contributory infringement or vicarious liability for knowingly linking to another site that contains copyright infringing material or otherwise engages in infringing activity. In an interesting

claim arising from allegedly improper linking, Ticketmaster sued Microsoft for its use of hypertext links to bypass Ticketmaster's homepage and advertising.[3]

A website owner may also be found liable for trademark infringement or unfair competition for framing another site on its own site. For example, in *Washington Post, et al. v. TotalNEWS,*[4] a number of news media sued TotalNEWS, a website which aggregated the other news sites and "framed" those sites with their own ads, thus effectively deriving ad revenues based on others' content without their permission. Although that case settled out of court, the practice of framing should be carefully reviewed in an audit.

Content Liability Issues: a Checklist for Web Publishers

Copyright and Trademark

A content audit should include a review of the third-party content, and the corresponding licence agreements, to ensure that the website owner has acquired the appropriate rights for use on its site. This includes graphics, images, logos and text. Indeed, use of another's trademark as a link may give rise to liability if the manner in which one uses a trademark creates the false impression that the trademark owner is somehow affiliated with the website owner. In addition, the audit should review the owner's copyright and trademark notices to ensure that they are accurate and current.

Defamation

Under U.S. as well as Indian law, a website owner may be held liable for false statements of fact which are defamatory and published with fault. While the owner may not be liable for statements by third parties because of the statutory protections of the Communications Decency Act, statements originating with the owner may give rise to liability. Traditional publishers frequently have an attorney review sensitive articles prior to publication to identify troublesome statements and to set up the best possible legal defences for publication of the article. A similar practice may be appropriate for articles published on the Internet which are written by the website owner.

Invasion of Privacy

There are three types of privacy torts that may arise from statements made on websites:

- the public disclosure of private facts;
- statements which place the subject in a false and defamatory light; and
- the commercial use of another's image or likeness without their permission.

As in defamation, while the website owner in the United States may not be liable for state law invasion of privacy claims arising from third party statements, the owner should carefully review original content.

User Privacy

An audit should include a review of the website's collection of user information. This is usually done at the registration page, and may include name, address, e-mail address, telephone number and credit card number. In addition, most sites now monitor the pages viewed and services utilised by a user via "cookie" technology. Thus, sites may maintain and use personally identifiable information about its users for a wide range of purposes such as targeting banner advertisements, tailoring services to individual users and sending direct advertisements to individual users based on their demonstrated interests. What information is collected, how it is used and to whom it is disclosed should be carefully reviewed to ensure that the website owner is in compliance with applicable privacy statutes, Competition and MRTP regulations and the site's privacy policy.

Advertising and Promotions

As a growing number of websites move toward the advertising business model, a content audit should include a review of the site's guidelines for accepting advertising on its site, particularly banner ads which hyperlink to the advertiser's site. The guidelines should adhere to state and federal fair advertising laws, particularly in regard to minors. In addition, the audit should review the advertisement insertion orders to ensure that they include appropriate indemnifications and representations and warranties. Some websites also sponsor interactive contests or sweepstakes and an audit may include review for compliance with sweepstake and contest laws.

Sales

If the site includes commercial transactions, the audit should include a review of the online contracts and also the website owner's account procedures for creating and maintaining records of the transactions. In some cases, the owner may also need to obtain accounting, security or other professional advice.

Regulatory Compliance

If the business hosting the website is publicly traded or involved in a regulated industry, such as banking, real estate, utilities, pharmaceuticals, or alcoholic beverages, the audit should include a review of SEC compliance and the specific advertising, shipping or other regulations for such industries.

The Sphere of Audit

Specific components of a website are worth particular attention:

Disclaimers and Terms of Service

The disclaimers and terms of service are important in establishing the relationship between the website owner and its users. Generally, the comprehensiveness of a user agreement is determined by balancing the potential exposure created by site content and activities against the potentially intimidating impression a long agreement will make on the user. For example, relatively straightforward sites that provide information about a company, but have little user interactivity, may only require a short disclaimer. On the other hand, sites which host e-commerce, chat, e-mail, or message boards or provide sensitive information, such as financial

information and services, will likely require a more extensive user agreement.

Message Boards and Chat

Many websites now provide areas for users to interact with both the website owner and other users. These areas take the form of message boards (where users can post a message that can be read and responded to by other users) and chat rooms (where users can send eachother messages, or "chat", in real time).

Whilst user interaction is enjoyable and fun, it can also be highly inflammatory. Frequently, a user may make defamatory or otherwise objectionable statements about others. Users then tend to turn to the website owner to remedy the problem by removing the statements, correcting the statements or somehow punishing the author of the statements. An audit should include a review of how the owner responds to such demands and set up a policy for when, if ever, it is appropriate to either remove a post or provide information about the author.

User Information

The privacy and security of personal information on the Internet has become an increasing concern. A website audit should include review of the site's policies for disclosing user information and, in particular, policies for responding to subpoenas for user information. In the United States, responding to requests for either the content of communications (*i.e.*, e-mail messages) or user information is strictly limited by the [federal] Electronic Communications Privacy Act. Any policy should take into consideration privacy or procedural requirements and other duties arising from common law or the site's Terms of Service.

Finally, an audit should include a review of the site's privacy policy. In general, the policy should provide notice to users about the types of information collected, how such information is used and to whom it is disclosed. In addition, websites should provide their users with reasonable access to their personal information and the ability to update or remove such data as appropriate.

The legal audit provides some guidance for website owners by identifying areas of potential liability before litigation arises. In addition, further content liability counselling can be done to place the website owner in the best possible legal position – by posting proper disclaimers, establishing sensible complaint policies, *etc.* – should a legal demand be made.

1 For further information, please refer to the report of the American Bar Association (ABA) Jurisdiction in Cyberspace Project empanelled in 1998 under the title, "Trans-national Issues in Cyberspace: A project on the Law relating to Jurisdiction".
2 *Reno v. American Civil Liberties Union*, U.S., 117 S. Ct. 2329 (1997) (the Internet receives full First Amendment protection).
3 *Ticketmaster Corp. v. Microsoft Corp.*, No. 97–3055 DDP (C.D. Cal., filed April 29, 1997).
4 97 Civ. 1190 (PKL) (S.D.N.Y., filed Feb. 28, 1997).

HONG KONG

Defamation on the Internet

By Janine Canham, CMS Cameron McKenna; e-mail: janine.canham@cmck.com

Increasing use of the Internet has increased the risk of defamation lawsuits against companies which own websites and thereby either write or host messages of a potentially contentious nature. However, there are steps that website owners can take to limit their liability.

The growth in the use of the Internet in recent years has been lauded as a huge boost for freedom of speech on an international scale. The ability of users to post information on web pages and to communicate with others all over the world in chat rooms has been a major part of the Internet's popularity. The new technology does not mean, however, that users are now free to say whatever they wish without limitation. The increase in communication over the Internet has led to an increased potential for complaints of defamation against those parties who write or host messages that damage the reputations of others.

What Constitutes Defamation?

In Hong Kong, as in other jurisdictions, defamation on the Internet is regulated in the same way as defamation that occurs in other media. No new legislation has been introduced in relation to defamation occurring over the Internet. Instead, existing legal principles have been applied to defamation claims arising out of subject matter appearing on the Internet. In some instances, existing principles have been adapted or applied by analogy. Section 5 of the Defamation Ordinance (Cap.21 Laws of Hong Kong) provides that:

> "Any person who maliciously publishes any defamatory libel, knowing the same to be false, shall be liable to imprisonment for two years, and, in addition, to pay such fine as the court may award."

What is meant by "defamatory libel"? A "defamatory libel" is a statement which causes a person to be a focus of hatred, contempt, ridicule, avoidance or which lowers that person's reputation in the estimation of right-thinking people generally. A statement that affects the reputation of an individual within a specific section or class of society would not necessarily be deemed sufficient. The statement must affect the reputation of an individual in society generally.

Once a statement is found to be defamatory, in order to avoid liability for publishing the statement, a defendant must show either that it is true or that it is protected by one of the other defences available.

The most common defences to a defamation action are:

- justification - *i.e.* that the words were true in substance and in fact;

- fair comment – *i.e.* that the words were the defendant's honestly held opinion on a matter of public interest and were published without malice; and
- qualified privilege – *i.e.* that the statement was made by a person who had a duty to communicate the matter in question to a person with a corresponding interest in receiving the communication. (This defence may be difficult to use in respect of Internet publications because of the potentially limitless audience available.)

Publication and Jurisdictional Issues

A defamatory statement is only actionable if it is published to a third party. With statements made in newspapers and magazines, the place of publication is clear. The position is more problematic with statements published on the Internet. Initial debate centred around whether defamatory statements were libels (*i.e.* a defamation in a permanent form) or slanders (*i.e.* a defamation in a transitory (traditionally spoken) form) because of the different types of damages available depending on this classification. Courts in both England and the United States have decided that defamatory Internet postings are libels because they are stored on a server somewhere and may be accessed repeatedly from that server, making them relatively permanent. The debate now is whether publication takes place at the point at which the statements are uploaded to the server or at the point at which they are accessed by a reader, because the uploading and accessing may take place in different jurisdictions under different laws.

The English courts have ruled that publication takes place at the point of access by the reader of the statements, meaning that an English court would have jurisdiction in a case involving defamatory statements posted anywhere in the world provided that at least one reader had accessed them in England. It is by no means certain, however, that courts in other countries will follow this approach.

Therefore site owners should be aware, when uploading information on to their sites that they could potentially become liable under the laws of any country where the site has been accessed. As a result website owners could realistically face liability under laws they do not know exist or with which they are unfamiliar. In order to minimise difficulties over the law governing the contents of their sites and potential claims, site owners and ISPs are recommended to post a clear statement of the countries to which the site and its contents are directed and the law which they consider applies to the site.

Site owners should also consider asking users to confirm that they are not located in jurisdictions that the site owner has determined to have onerous defamation laws.

There is no absolute guarantee that these measures will be effective, however. Courts in some jurisdictions have shown a willingness to accept jurisdiction and/or apply their own law to actions based on information appearing on the Internet simply because the claimant is located in the same jurisdiction as the court.

Information Published on Websites

Site owners who review, edit and publish articles written by third parties will be liable for defamatory statements made in those articles in the same way as they would if the statements were made in a newspaper. It is unlikely that a disclaimer would be successful in limiting the site owners' responsibility in this respect.

Messages Posted in Chat Rooms

Despite their popularity with Internet users, chat rooms are hazardous from a defamation perspective. If, as is common practice, site owners or ISPs do not screen the content of the messages in chat rooms, Hong Kong laws provide that no liability will attach to the site owners or ISPs as a "publishers" of any defamatory statements. However, the site owner may risk liability as a "disseminator" of the material.

At common law, site owners and ISPs, who face liability as disseminators of information, may be able to

avail themselves of the defence of "innocent dissemination" as a defence against a defamation action.

This defence is available if the site owner or ISP can establish that:

- they did not know the publication contained a libelous statement;
- they did not know the publication was of a character likely to contain libelous material; and
- their lack of knowledge was not due to their own negligence.

The type of material often found in chat rooms may, however, mean that the second limb of this test is difficult to satisfy.

Site owners and ISPs are therefore advised to monitor their chat rooms for offensive statements and to act quickly on complaints from third parties about material not already identified as defamatory. In most cases acting quickly will mean rapidly taking action to remove the potentially offending material from the site.

Law in Jurisdictions Outside Hong Kong

Since no Internet defamation cases have been tried in Hong Kong so far, there has been much interest in recent developments in the law in other jurisdictions. These developments have unfortunately not been consistent, which means that there are still unanswered questions regarding the approach to ISP liability which will be adopted in Hong Kong.

In England, the Defamation Act 1996 provides a defence in Section 1 for ISPs who merely host defamatory material without exercising any editorial control over it. The defence is available to a person who can show that:

- he is not the author, editor or publisher of the statement complained of;

- he took reasonable care in relation to its publication; and
- he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

Before the introduction of the Defamation Act, ISPs' only defence was at common law, with the criteria discussed above.

A recent English case has illustrated a limitation of the new statutory defence. In *Godfrey v Demon Internet*, Demon hosted a series of Usenet sites that allowed users to post comments in a bulletin board format. Defamatory comments about Mr Godfrey were posted to one of the groups. Demon sought to rely on Section 1 of the Defamation Act by arguing that it was not the author, editor or publisher of the material in question, and was not responsible for its appearance on the bulletin board. However, Mr Godfrey had complained to Demon about the messages, and asked for them to be removed. Demon had declined to do so. It could not therefore satisfy the requirement in Section 1(c) and it settled with Mr Godfrey by paying him £15,000 in damages and his legal costs, estimated at some £230,000.

In comparison, in *Lunney v Prodigy*, a case heard in the United States, the court held that an ISP could not be held responsible for defamatory postings on its sites, as its role is analogous to that of a telecommunications carrier.

These cases demonstrate that an entirely different approach to defamation claims on the Internet is being adopted in different jurisdictions. This means that certain publications may attract liability in one jurisdiction but not another, which is an unsatisfactory situation for ISPs whose operations take place on a global scale.

The English position is particularly unsatisfactory because there is no definition of what constitutes adequate notice to an ISP of the presence of defamatory material on a website. At present, sites are being shut down on the basis of a single complaint alone, as ISPs fear becoming the next Demon and facing massive legal bills from disgruntled claimants.

Despite all of these issues and problems which site owners face there are steps which website owners can take to limit their liability to defamation claims. Some of these steps are preventative measures, which may stop actions arising in the first place and others may aid a site owner's defence to a defamation action.

The Use of Disclaimers

As mentioned, the adoption of disclaimers and user policies to prohibit the posting of defamatory materials on the site may not give a site owner or ISP a watertight defence. However, the use of such precautions does at least show that the companies are taking their responsibilities seriously and may encourage leniency by those adjudicating defamation claims.

For a list of areas that may be included in disclaimers, see Figure 1:

Figure 1

- the users of the website or chat room agree not to post or publish any offensive, defamatory or unlawful materials that could encourage or constitute a criminal offence, civil liability or violate any law;
- the opinions posted on the websites are those of the authors and do not represent the views of the ISP or site owner;
- the ISP or site owner exercises no editorial control over the material being posted on the site or in the chat room and shall not be deemed to be the author, editor or publisher of the material;
- the ISP or site owner reserves the right to monitor or review the contents of the website or chat room, but is not obliged to do so and assumes no liability or responsibility for the contents therein;
- the ISP or site owner may change or remove any materials being posted which are regarded as offensive or defamatory, or which violate the user policy of the site;
- the ISP or site owner may, upon request, disclose the identities of those who have violated the law to
- relevant parties to aid investigation.

The location of disclaimers is important. Users should have to pass through a gateway so that the disclaimers can be read and acknowledged by the user each time the site is accessed. In addition, users should have to click the "I accept the terms" button before access is permitted so that it is clear that the disclaimer applies to all parts of the site. Further to this, when anything is downloaded from the site, the disclaimers should again appear on the downloaded text in a prominent position.

If the website is to contain any links/hyper-links to other sites, responsibility for the information on those sites should also be specifically disclaimed so that the ISP or site operator is not held responsible for any materials or information deemed offensive, defamatory or inappropriate in third party sites.

Indemnities

Site owners and ISPs are advised to include an indemnity, by which users of the chat room or site agree to indemnify the website owner against any claims made against the website owner by third parties as a result of the use of the chat room or site by the user. To some extent this will shield website owners from the expense of claims arising from defamatory material posted, especially via chat rooms, on their sites.

Privacy Policy

Site owners should consider including a privacy policy on their site. Under Hong Kong law, the position is governed by the Personal Data (Privacy) Ordinance, one of the principles of which requires you to inform readers of privacy policies. For example, a privacy policy should include a statement that if a person participates in a chat room, they may be prompted to submit their name and the statement should inform the user for what purpose their name may be used.

Education of Staff

Site owners or ISPs should educate their staff about the dangers of publishing defamatory material and implement a process to monitor the contents of chat rooms to avoid claims of negligence. Journalists or

regular contributors to a site should be given guidelines as to the type of statements that could be viewed as defamatory.

Editorial Role

Site owners and ISPs should not edit any messages in chat rooms, as by doing so they may be deemed a publisher of the defamatory information and as a publisher they would not be able to avail themselves of the defence of innocent dissemination. Instead, site owners and ISPs are advised to remove immediately statements that are obviously defamatory. If a site owner or ISP is unsure as to whether the contents of a posting are potentially defamatory, legal advice should be sought immediately.

Complaints

Site owners and ISPs are recommended to remove any potentially defamatory material upon receipt of a complaint. Websites should contain clear details of the person and/or e-mail address to whom complaints should be directed.

In addition to disclaimers allowing a site owner to withdraw material, contracts with journalists, freelance writers or other contributors to a site should include terms which grant site owners and ISPs total discretion to withdraw any material that they consider may give rise to a defamation action.

Insurance

It is possible to obtain specific insurance to cover defamation claims that might arise as a result of the conduct of a site owner's or ISP's business. Two or three of the big insurance companies in Hong Kong provide such cover as part of their "Internet Liability Package".

Warranties and Indemnities

Consideration could be given to obtaining warranties and indemnities from all contributors to the site to the effect that their materials are not defamatory in any way, and do not breach any third party intellectual property rights. For example, companies that employ journalists to write articles for their websites could make it a term of the journalists' employment contract that the deliberate use of defamatory material in an article is an action for which they could be dismissed.

Limited Liability Company

Finally, site owners are advised to conduct their publishing activities through an entity separate from their operating vehicle in order to ring fence any liabilities which they may incur through defamation claims.

Summary

The Internet is an exciting new medium with enormous potential for increased worldwide communication. This does not mean, however, that users are free to publish statements that harm the reputations of others. Defamatory statements on the Internet will be governed by existing principles from the law of tort, including relevant statutory provisions and case law. Interesting legal questions are already arising as a result of the multi-jurisdictional nature of Internet communications. Until these questions are resolved, caution is necessary on the part of site owners and ISPs, who should ensure that they take all reasonable steps to avoid contributing to the publication or dissemination of defamatory material. They should also ensure that they respond quickly to any complaints that are received about materials that appear on their sites.

Janine Canham may be contacted at janine.canham@cmck.com or on tel: (+852) 2846 9100.

HONG KONG

The Gambling (Amendment) Ordinance: A Gamble or Not?

By Gabriela Kennedy and Vivian Lui, Consultant and Assistant Solicitor respectively, working in the Technology, Media and Telecoms Group of Lovells in Hong Kong; e-mail: gabriela.kennedy@lovells.com; and/or: vivian.lui@lovells.com.

Background

In May 2002, the Hong Kong government enacted the Gambling (Amendment) Ordinance ("The Amendment Ordinance") amending certain provisions in the Gambling Ordinance (Cap. 148 of Laws of Hong Kong) regarding bookmaking and placing bets with overseas bookmakers and promoting or facilitating such bookmaking. The amendments widen the scope of gambling offences to cover offshore bookmakers who accept bets from Hong Kong. Anyone in Hong Kong who places bets with offshore bookmakers will also be committing an offence. Persons operating premises which promote and facilitate such gambling will also be liable under the new legislation.

The Amendment Ordinance in effect prohibits computer users from placing bets over the Internet with bookmakers not licensed in Hong Kong, whether or not the website taking the bets is hosted in Hong Kong or offshore. The Amendment Ordinance also imposes criminal liability on operators of online gambling websites who accept bets from within Hong Kong.

Bookmaking Offence

Prior to the Amendment Ordinance, the Gambling Ordinance contained a provision that made it a criminal offence to engage in "bookmaking". This was defined as soliciting, receiving, negotiating or settling a bet by way of trade or business, by letter, telephone, telegram,

10/02 Copyright © 2002 The Bureau of National Affairs, Inc. WILR ISSN 1468-4438

or by any other means. For a while it was unclear whether this meant that it was an offence under the law to engage in bookmaking activities outside Hong Kong (for example, by running a gambling website from outside Hong Kong, with an Internet server outside Hong Kong but to which Internet users within Hong Kong could have access).

In a recent Hong Kong case, *Hong Kong v Chu Kam Yiu and Others* [2002] HKCU 107, the Court of Appeal held that under the pre-amendment Gambling Ordinance, "where the bookmaker is outside Hong Kong, no offence is committed in Hong Kong". Prior to the Amendment Ordinance, only bookmaking activities carried out in Hong Kong were illegal. Bookmakers physically located outside Hong Kong could avoid being caught by the pre-amendment Ordinance.

The Amendment Ordinance changes this position. Under the Amendment Ordinance, the definition of "bookmaking" has been revised to include "receiving, negotiating or settling of a bet which is either placed from Hong Kong or placed by a person in Hong Kong". Section 7 of the Amendment Ordinance makes it clear that overseas bookmakers commit a criminal offence in Hong Kong when they accept a bet placed from Hong Kong. They cannot avoid criminal liability by placing their "base" outside Hong Kong.

The definition of "bookmaking" has been further amended to include soliciting, receiving, negotiating or settling of a bet by way of trade or business "by means of an online medium". Section 7 of the Amendment Ordinance makes it clear that it is a criminal offence to accept bets placed over the Internet, even though the operator or the server for the website taking the bets are located outside Hong Kong. The maximum penalty for illegal bookmaking is a fine of HK$5 million and imprisonment for seven years.

Offence of Betting with an Unlicensed Bookmaker

The pre-amendment Ordinance contained a provision whereby betting with an unlicensed bookmaker constituted a criminal offence. It was unclear however, whether it was illegal to bet with a bookmaker located outside Hong Kong. The Amendment Ordinance has now clarified that anyone who bets with a bookmaker, whether the bookmaker is in or outside of Hong Kong, commits a criminal offence and may be liable to a maximum penalty of a fine of HK$30,000 and imprisonment for nine months.

Issues Arising from the New Definition of "Bookmaking"

There are several issues that have arisen from the changes brought about by the Amendment Ordinance:

Gambling May be Legal in the bookmaker's own country

The Amendment Ordinance imposes criminal liability on bookmakers located outside Hong Kong, even though such bookmakers may be properly licensed and their activities may be lawful in their home jurisdiction. Furthermore, it is arguably difficult for offshore bookmakers to screen out bets placed from Hong Kong. While it appears from the Amendment Ordinance that the burden remains on the prosecution to prove the criminal intent of the offence, it is not yet clear how much will need to be proved by the prosecution. Does the prosecution have to show positive evidence that the offshore bookmaker knew that the bet was placed from Hong Kong? This question is yet to be answered by the court when the first prosecution is brought under the Amendment Ordinance. In any event, computer savvy users may "daisy-chain" their connections and make offshore bookmakers believe that the bet is being placed from anywhere else but Hong Kong.

Extra-territorial Enforcement

As the Amendment Ordinance seeks to impose criminal liability on offshore bookmakers, the enforcement of the new provisions will involve extra-territorial elements. In practice, the Ordinance can only be enforced against offshore bookmakers when they arrive in Hong Kong. Otherwise enforcement agencies will need assistance from their counterparts in overseas jurisdictions but if the bookmakers' activities are legitimate in such a jurisdiction, it is hard to see how forthcoming that help might be.

Privacy Rights

Under the Amendment Ordinance, any person who bets with a bookmaker commits an offence, whether the bet is received within or outside of Hong Kong. One problem with this amendment lies in the fact that some infringement of privacy rights will be inevitable during enforcement by government enforcement agencies. So far, the government has refused to disclose the extent of interception of communications that took place in the past and will take place in future. The government, however, has claimed that it would not conduct real-time monitoring of online communications.

At present, the interception of communications is regulated by the Telecommunications Ordinance and the Post Office Ordinance. These Ordinances provide sweeping powers of interception upon public interest grounds and on the part of enforcement agencies. No warrant is needed in order to monitor or intercept communications under these ordinances. Another Ordinance, the Interception of Communications Ordinance, which was enacted in 1997 but has yet to come into force, may change this situation. This Ordinance requires law enforcement agencies to obtain and renew warrants for interceptions of communications. Warrants for interceptions of communications are renewable only once, with the renewal being valid for only 90 days.

Offences for Facilitating Betting or Bookmaking

The Amendment Ordinance also includes new provisions that make it an offence to promote and facilitate illegal gambling activities. Under the amended Ordinance, a person who knowingly operates, manages,

or otherwise has control of any premises that promote or facilitate bookmaking or betting with an overseas bookmaker (*i.e.*, an unlicensed bookmaker under the Ordinance) commits an offence. A person who knowingly promotes or facilitates illegal bookmaking or betting with an unlicensed bookmaker is also criminally liable. The maximum penalty for these offences are a fine of up to HK$5 million and imprisonment for seven years.

Effects of the Amendment Ordinance

The Amendment Ordinance places an added risk on Internet Cafés' operators of being found liable for illegal online gambling activities committed by customers of the cafés. If an owner or operator of an Internet Café knows that a customer is placing a bet on a gambling website within the café and does nothing to stop that customer from doing so, he or she may run the risk of being found liable under the Amendment Ordinance.

Although the new provision requires the prosecution to prove that the owners or operators of Internet Cafés "knew" about the illegal gambling activities on their premises, owners or operators of Internet Cafés may be well advised to take active steps to ensure that their customers do not engage in illegal online gambling on their premises. As a minimum, notices should be displayed at the premises warning customers not to commit such actions. Website filters may also be used to block access to gambling websites using the cafés' computers, though the efficacy of such filters is debatable.

Internet Services Providers

During the legislative process, there were numerous discussions as to whether Internet Services Providers ("ISPs") should be empowered to block access to gambling websites. The legislature recognised that most of the gambling websites are offshore and maintained on servers outside Hong Kong. It was concluded therefore, that empowering local ISPs to block access would not be of much help or have much use in practice. Further, if any gambling website is hosted on a local server, government enforcement agencies will be able to track down the operator of the website and take enforcement action without the involvement of the local ISP concerned.

All this seems to imply is that, in the absence of the required *mens rea*, ISPs are unlikely to be found guilty under the Amendment Ordinance of promoting or facilitating illegal bookmaking or betting with a bookmaker, simply because they provide access to bookmaking websites.

The situation is different for content providers, who will be responsible for all content they post on websites. Advertising banners or any kind of advertisements relating to unlicensed bookmakers will attract liability for promoting or facilitating illegal bookmaking under the Amendment Ordinance.

Conclusion

The Amendment Ordinance has been enacted to stop Hong Kong residents from placing bets with offshore bookmakers. While the Amendment Ordinance clarifies that online gambling is illegal, even where the gambling websites are located outside Hong Kong, and it imposes obligations on operators of Internet Cafés to prevent online gambling activities by customers, in practice, the Amendment Ordinance may be difficult to enforce.

■ ROMANIA

An Overview of Romanian Telecommunications Legislation with reference to Internet Law Provisions

By Marius Petroiu, attorney at law, member of the Bucharest Bar and an associate with Baratz, Pachiu & Associates, Bucharest; e-mail: m.petroiu@bar-law.com

Applicable Law

Following the conclusion in 1993 of an Association Treaty with the European Communities, the Romanian government agreed to restructure its domestic regulations in order to comply with European Union legislation.

With reference to the field of Internet law, certain regulations referring to online commercial transactions were enacted, such as Law No. 455/2001 on electronic signature,[1] Government Ordinance No. 20/2002 concerning online public acquisitions, as amended,[2] Government Ordinance No. 24/2002 on rules regarding online tax payments, as amended,[3] and Law No. 365/2002 on e-commerce rules.[4]

Furthermore, certain laws were passed in the telecommunication field, establishing a National Surveillance Authority on Telecommunications (hereinafter the "Authority") and the basic terms and conditions to be followed for further investments in the area. In this respect, the Emergency Government Ordinance No. 79 on the legal telecommunications framework (hereinafter the "Ordinance") was published in the Official Gazette No. 457 of June 27, 2002 and is scheduled to enter into force on September 27, 2002.

The new telecommunication legislation also makes reference to Government Ordinance No. 34/2002 on access to electronic communication networks and infrastructures, as amended,[5] Law No. 676/2001 on protection of individuals as regards processing of individual's data in the telecommunication field[6] and Government Ordinance No. 31/2002 on postal services, as amended.[7]

Scope of the Ordinance

According to the provisions of Article 1, the Ordinance establishes the attributions of the Authority as a government commissioner in the field of telecommunications and postal services and lists the applicable unfair competition rules.

Furthermore, the Ordinance underlines the principles for authorising entities to provide third parties with access to electronic communication networks,[8] such as the access to networks using radio frequencies for transferring data to various clients through the Internet.

Access to Electronic Communication Networks

Pursuant to the provisions of Article 4 of the Ordinance, entities intending to provide third parties with access to electronic communication networks using radio frequencies for transferring data through the Internet, must previously notify their intentions with the Authority. The notification shall include information as to the entity identification's co-ordinates, network's technical requirements and estimated date of commencing the activities.

Following the notification, the Authority shall issue a general authorisation, (hereinafter the "Authorisation") stating the terms and conditions under which the entity may provide services to the consumers. Such Authorisation is issued on a temporary basis and may be amended or canceled in case the original information is changed or new technical requirements are requested under international agreements. However, amendment or cancellation of the Authorisation must follow a consultation procedure with the Authority, as provided by Articles 49 and 50 of the Ordinance.

Basically, once authorised, the entity shall be entitled to have access to private or public properties, in order to establish electronic communication networks, subsequent to an agreement concluded between the entity and the property's owner. Furthermore, the authorised entity shall be able to enter into various access and inter-connection agreements with similar authorised providers.

In all cases, the operational use of radio frequencies for transfer of data via the Internet is subject to a license permit issued by the General Authority for Communications and Information Technology (hereinafter the "Technical Authority"), established under the control of the Ministry of Telecommunications and Technology.

Transparency Procedures

According to the provisions of Article 49 and 50 of the Ordinance, the Authority must maintain a public information website, available both in Romanian and a widely spoken "international" language, such as English. Such information shall refer to the Authority structure and attributions, pertaining also to the Authority's decisions and the regulations applicable in the telecommunications field.

All-significant measures referring to the telecommunication market (*i.e.* the amendment or modification of the Authorisation of an Internet service provider) shall be taken following a website consultation procedure. In this respect, the Authority shall establish a discussion forum list, open to all interested parties, who may register their e-mail address to receive further information. Presently, the website is available at *www.anrc.ro*, both in Romanian and English.

As to the applicable procedure, the draft concerning the measures to be taken by the Authority shall be published on the Authority's website. All persons registered with the discussion forum list shall be informed by e-mail as to the object of the proposals and to the applicable delay for posting suggestions (as a rule, the delay shall vary from 10 to 30 days, starting with the date when the Authority's draft was published on the website). Finally, the Authority shall issue a decision, together with a synthesis of the suggestions received.

Conclusion

At present, in accordance with the provisions of Article 61 of the Ordinance, until December 31, 2002, the National Telecommunications Company (Romtelecom SA) has the exclusive right to lease the phone lines necessary for the transfer of data via the Internet to various consumers. However, starting from January 1, 2003, it is expected that such market will be liberalised and opened to competition.

Moreover, until December 31, 2002, the National Radio-Communications Company shall be the sole entity authorised to provide for transfer of data via the Internet, using leased radio frequency lines, with a capacity of more that 2 Mbits/s (*i.e.* radio lines providing a very fast transfer of data on the Internet). After January 1, 2003 such market is also expected to be liberalised, in order to allow private corporations to provide with access to different technologies, by renting on a temporary basis certain radio frequencies, under a license permit issued by the Technical Authority, the special authority in the field, and following the authorisation issued by the National Surveillance Authority on Telecommunications.

1 Published in the Official Gazette No. 429 of July 31, 2001.
2 Published in the Official Gazette No. 86 of February 1, 2002.
3 Published in the Official Gazette No. 81 of February 1, 2002.
4 Published in the Official Gazette No. 483 of July 5, 2002.
5 Published in the Official Gazette No. 88 of February 2, 2002.
6 Published in the Official Gazette No. 800 of December 14, 2001.
7 Published in the Official Gazette No. 87 of February 1, 2002.
8 In accordance with the provisions of Article 2 (a) of Government Ordinance No. 34/2002, the term "electronic communication networks" includes all systems, equipments and installations allowing the transfer of information by radio, telegraph or optic wire or any other electromagnetic means, including satellite communications networks, fixed networks, Internet connected networks, mobile networks, energy transfer networks if such networks are used for transfer of data, TV cable and audio-video networks, irrespective of the type of information subject to be transferred.

THAILAND

The Thai Electronic Transaction Act 2001: Recent Developments Surrounding IT Law in Thailand

Saravuth Pitiyasak, Lecturer in Law at the Sukhothai Thammathirat Open University; e-mail: lwaspsar@hotmail.com

Introduction

Digital information technology may present the most significant challenge in recent legal history to existing law in all countries worldwide. This new technology has lead to the development of electronic commerce, in which transactions that traditionally occurred by letter, fax, or even aurally, now take place over the Internet.

In late 1998, the National Information Technology Committee (NITC), in recognising this new challenge, empowered six sub-committees to study and draft six Information Technology related pieces of law (IT law) (The original six pieces of law are now five – because of their related contents, the draft Electronic Transaction Law and the draft Electronic Signatures Law were later merged into the Thai Electronic Transaction Act 2001). The IT law development project is carried out by NECTEC, which is the secretariat office for the six drafting committees. Each subcommittee is chaired by a prominent legal expert and is comprised of representatives from the agencies concerned.

The five pieces of IT law are intended to serve as an infrastructure for individuals and organisations conducting e-commerce within Thailand and increase confidence in this area. The new laws aim to enhance Thailand's competitiveness and its reputation as a country in which to conduct e-business.

The five pieces of IT legislation include the following:

- Thai Electronic Transaction Act 2001 (to be discussed in further detail below);
- Electronic Funds Transfer (EFT) Law;
- Data Protection Law;
- Computer Crime law; and
- National Information Infrastructure Law.

Electronic Funds Transfer (EFT) Law

The Electronic Funds Transfer (EFT) Law seeks to provide consumer protection, establish security procedures in electronic funds transfer and allocate the liability incurred from the technological risks. The content of the EFT Law is currently at draft stage. The draft law will be forwarded to the Thai Cabinet for approval in the first quarter of 2003.

Data Protection Law

The Data Protection Law is intended to protect the right to privacy regarding personal data. Its present draft is similar to the laws of many European countries in this respect, particularly that of Italy. According to the draft Data Protection Law, the data subject shall be protected from unauthorised use of his/her personal data through the electronic processing of such data. The draft law also seeks to provide a balance between the privacy rights of the individual and the freedom to exploit information technology; attempting not to jeopardise the former in the development of the latter. Personal data must not be disclosed, made available or used for purposes other than those specified at the time of data collection, except by consent of the data subject or the authority of law. The draft Data Protection Law was approved by the NITC on October 3, 2001 and is currently under consideration by the Thai Cabinet.

Computer Crime Law

The Computer Crime Law is aimed at clarifying and criminalising the new type of criminal offences that may occur in the borderless virtual world or "cyberspace" created by the Internet. The draft Computer Crime Law was approved by the NITC on May 2, 2002. At present, the draft Computer Crime Law is under the consideration of the Thai Cabinet.

National Information Infrastructure Law (By Law of Section 78 of the Thai Constitution 1997)

The National Information Infrastructure Law is aimed at creating an equitable information society by promoting universal access in the National Information Infrastructure, pursuant to Section 78 of the 1997 Thai Constitution. The draft National Information Infrastructure Law was approved by the Thai Cabinet on November 7, 2000, then forwarded to the State of Council for examination and is awaiting submission to Parliament in early 2002. However, with the plans to set up an Information and Communications Technology Ministry in October 2002 as part of the public sector reform, the draft law as a related legislation will require some amendments in order to accommodate the functions of the new Ministry. At present, the draft law is under the reconsideration of the Ministry of Science, Technology and Environment.

Electronic Transaction Act 2001

The Thai Electronic Transaction Act 2001 (Thai ETA 2001) was first drafted as two pieces of legislation, namely the draft Electronic Transaction Law and the draft Electronic Signatures Law. The two drafts were approved by the Thai Cabinet on March 14, 2000 and then forwarded to the Council of State for examination. The Council suggested that the two drafts be merged. On July 25, 2000, the Cabinet endorsed this suggestion. The law then progressed to Parliament and was promulgated in December 4, 2001 and came into force in April 3, 2002.

The Thai ETA 2001 has brought Thailand into line with what are becoming international norms with regard to electronic transaction legislation. It is based very much on the relevant UNCITRAL Model Law on

E-Commerce[1] and similar legislation passed in Singapore and Malaysia. It contains six Chapters including Chapter I – Electronic Transactions; Chapter II – Electronic Signatures; Chapter III – Service Providers for Electronic Transactions; Chapter IV – Electronic Transactions in the Government Services; Chapter V – Electronic Signatures Commission and Chapter VI – Penalties.

The Act has two main objectives:

- to establish the legal framework necessary to support electronic contracts; and
- to recognise the legal validity of electronic signatures.

Setting the Legal Framework to Support Electronic Contracts

A Data Message has Legal Validity Equal to a Message Written on Paper

Where data messages are used to form a contract, the question arises as to whether such data messages have legal validity equal to messages written on paper. In this regard, Section 8 of the Thai ETA 2001 recognises data messages as the functional equivalent of those executed on paper by providing that:

> "… in case where the law requires that any transaction be made in writing or evidenced in writing or supported by a document which must be produced, if the information is generated in the form of a data message, which is accessible by reading and convertible into the information usable for subsequent reference, it shall be deemed that such information is already made in writing, evidenced by writing or supported by the produced document".

A Data Message Can Constitute an Offer or Acceptance

Section 13 of the Thai ETA 2001 provides that:

> "An offer to make a contract and an acceptance may be expressed in the form of a data message and the contract shall not be denied legal effect on the sole ground that the offer or acceptance respect to that contract was made in the form of a data message".

Consequently, with the enactment of Section 13 of the Thai ETA 2001, there will be no doubt that a data message can constitute an offer or an acceptance in Thailand.

Clicking on an Icon can Constitute an Intention to be Legally Bound

"Click-wrap" or "web-wrap" contracts are contracts formed over the Internet by clicking on a button labeled "I agree" or something similar. For example, when a customer orders goods or services through the website of a business, the customer will be required to provide some information, and to agree to certain terms and conditions by clicking a button labeled "I agree" or "I accept". Usually, the terms and conditions exclude some liability of the business and prohibit commercial use of the customer. The crucial question is whether clicking on an "I agree" or "I accept" button can constitute an intention by the customer to be legally bound.

Section 15 of the Thai ETA 2001 also attributes the data message to the originator by providing an assumption that:

"When any person sent a data message by any means, it shall be deemed that such data message is that of that person."

Section 15 of the Thai ETA 2001 is considered to be broad enough to cover the click-wrap contracts where the originator clicks an "I accept" or "I agree" button on a website. By clicking the button the originator is sending the data message. Section 15 assumes that the data message is that of the originator. If the originator would like to reject it, he/she has the burden to prove it.

Electronic Records Generated by Autonomous Computers Without Immediate Human Intervention can Create Binding Contracts

Whether autonomous computers can make a contract is a very important question. Section 4 of the Thai ETA 2001 deals with this uncertainty by giving the broad definition of "originator" as follows:

"Originator" means a person who is a sender or generator of the data message prior to its storage for transmission in accordance with the method designated by such person, whether the data message is sent or generated by such person or is sent or generated on such person's behalf, but does not include an intermediary with respect to that data message.

The definition of "originator" in the Thai ETA 2001 does no way intend to attribute the data message to the computer, which generates the data message. In fact, it intends to attribute the data message generated automatically by the computer to the person who designates the computer to operate (*i.e.*, the sender or the originator of the data message).

How to Determine the Time and Place of Formation of Electronic contracts

Time and Place of Dispatch of Data Message

Sections 22 and 24 of the Thai ETA 2001 deal respectively with matters of time and place of dispatch of data messages by providing:

> "It shall be deemed that the dispatch of a data message occurs when it enters an information system outside the control of the originator"; and
>
> "A data message shall be deemed to be dispatched at the place of business of the originator.
>
> "In the case where the originator has more than one place of business, reference shall be made, for the purpose of the place of business under paragraph 1, to the place of business which has the closest relationship to the underlying transaction. But, if it cannot be determined which place of business has the closest relationship to such transaction, the principal place of business shall be treated as the place where such data message is received or dispatched."

In the case where the place of business of the originator or the addressee does not exist, its habitual residence shall be treated as the place of dispatch or receipt of the data message.

According to Sections 22 and 24 of the Thai ETA 2001, an offer or an acceptance made in the form of a data message is deemed to be sent when it enters an information system outside the control of the originator and at the place of business of the originator.

If the originator has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction. But if it cannot be determined the place that has closest relationship to the underlying transaction, the principal place of business is the place of dispatch of data message.

If the originator does not have a place of business, its habitual residence is the place of dispatch of the data message.

Time and Place of Receipt of the Data Message

Time of receipt of data message in case that the addressee has designated an information system

Section 23 para 2 of the Thai ETA 2001 deals with time of receipt of data messages in case that the addressee has designated an information system.

According to Section 23 para 2 of the Thai ETA 2001, if the addressee has designated a particular information system for the purpose of receiving data messages, it shall be deemed that receipt of a data message occurs as from the time when the data message enters the information system designated by the addressee. But, if the data message is sent to another information system of the addressee that is not the information system designated by the addressee, it shall be deemed that receipt of the data message occurs as from the time when the data message is retrieved from that information system.

Time of receipt of data message in case that the addressee has not *designated an information system*

Section 23 para 1 of the Thai ETA 2001 deals with time of receipt of data message in case that the addressee has *not* designated an information system.

According to Section 23 para 1 of the Thai ETA 2001, if the addressee has not designated the information system, the data message is deemed to be received when it enters an information system of the addressee.

Place of Receipt of the Data Message

Similar to the place of dispatch of the data message mentioned earlier, place of receipt of the data message under Thai ETA 2001, is the place where the addressee has its place of business.

If the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business.

If the addressee does not have a place of business, its habitual residence shall be treated as the place of receipt of the data message.

Recognizing Legal Validity of Electronic Signatures

Thai Electronic Signatures

According to Section 4 of the Thai ETA 2001, electronic signature means

> "letters, characters, numbers, sound or any other symbols created by an electronic means and attached to a data message for establishing the association of a particular person with the data message for the purposes of identifying the signatory and indicating that such person has approved and agreed to be bound by that data message".

Under the Thai ETA 2001, electronic signature is given to include sound and any other symbols created by electronic means. Section 4 of the Thai ETA 2001, nonetheless, must be read alongside Section 9 of the Thai ETA 2001, which provides that:

> "In the case where a person is to enter a signature in any writing, it shall be deemed that a data message bears a signature if:
>
> 1. a method is used which is capable of identifying the signatory and indicating that the signatory has approved the information contained in the data message as being his or her own; and
>
> 2. such method is as reliable as was appropriate for the purpose for which the data message was generated or sent, having regard to surrounding circumstances or an agreement between the parties".

Under Section 9, a data message bears an electronic signature only if it is created by a capable and reliable method. At the moment, the only method that is accepted under the Thai ETA 2001 is the use of a public and private key pair or "digital signature". As a result, simply clicking on an "I accept" or similar icon on a website, typing one's name or even an "X" at the end of an e-mail, use of passwords or credit card number, or even complex techniques through biometrics authentication are not currently regarded as an electronic signature under the Thai ETA 2001.

Foreign Electronic Signatures

According to Section 31 para 3 of the Thai ETA 2001, an electronic signature created or used in a foreign country shall be deemed to have the same effect as an electronic signature created or used in Thailand, provided that a trustworthy system which is no less reliable than the trustworthy system under the Act is used in its creation. This means that all foreign digital signatures created by the use of private and public key technology are well accepted as electronic signatures in Thailand. This provision makes the contracts between the Thai contracting party and the foreign contracting party that require signatures to be enforceable in Thailand.

Summary and Comment

As discussed earlier, to a large degree the Thai ETA Act 2001 is able to fulfill its main objectives – to establish the legal framework necessary to support electronic contracts and to recognise the legal validity of electronic signatures. Nonetheless, since a number of provisions in the Thai ETA 2001 have been translated from the UNCITRAL Model Law on E-Commerce which deals with technology whose terms are very new and unfamiliar to the Thai language. Some technical phrases and words in the UNCITRAL Model Law on E-Commerce could not be translated properly into the Thai language. Thus, the Thai ETA 2001 is quite difficult to

read and comprehend and will ultimately lead to problems of interpretation.[2]

The best way to clarify the ambiguity of the Thai ETA 2001 is to look at the relevant provisions in the UNCITRAL Model Law on E-Commerce when interpreting the Thai ETA 2001. Ideally, there should be a reference in each section of the Thai ETA 2001, pointing to the relevant provisions of the Model Law. Such a provision could assist judges and attorneys who have to deal with the ambiguity of the Thai ETA 2001.

The author would like to thank Dr. Kevin K H Pun, Associate Professor of Computer Science and Honorary Associate Professor of Law at the University of Hong Kong for his invaluable comments on this paper.

1 UNCITRAL, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, Part I, Resolution 51/162 adopted by the General Assembly 85th at plenary meeting (December 16, 1996) (UNCITRAL Model Law on E-Commerce): *www.uncitral.org/en-index.htm*

2 Nanakorn, Pinai cited in Kanjanatawe, Kanjana, "Thailand's New E-Transaction Law raises Concerns", *Bangkok Post*, January 23, 2002.

DOMAIN NAME DISPUTE RESOLUTIONS

In this column, the World Internet Law Report *provides details of recent domain name dispute resolution rulings by ICANN-accredited institutions. The information is provided by* Riccardo Roversi, Studio Legale Abbatescianni, Milan & Rome, *with contributions from* Judith Paine *and* Yee Mun Loh. *Mr. Roversi may be contacted by e-mail at* rroversi@sla.it*; tel. (+39-25) 413-1722; fax: (+39-25) 501-4830; web page: www.sla.it*

Yahoo! Inc. v. Seocho

Domain names: auctionyahoo.com, cyahoo.com, emailyahoo.com, eyahoo.com, mapyahoo.com, ryahoo.com, wwwyahoogames.com, yahoochatrooms.com, yahooco.com, yahoodirectory.com, yahoolove.com, yahoon.com, yahooooo.com, yahoopersonal.com, yahooquote.com, yahooquotes.com, yahoor.com, yahoosearchengine.com, yahoospades.com, yahooxxx.com, yahooyahoo.com

Dispute resolution provider: National Arbitration Forum (Case no. FA0204000109050)

Panel: James P. Buchele

Identity or confusing similarity: (i) registered trademark; (ii) addition of minor differences and generic terms; (iii) repetition of domain names

Rights or legitimate interests: (i) linking of domain names to competing websites; (ii) world-wide fame of trademark

Bad faith: constructive knowledge

Process: no Response was filed

Result: the domain names were ordered to be transferred

Decision date: May 13, 2002

The Napoleon Hill Foundation v. Thinkandgrowrich.com

Domain name: thinkandgrowrich.com

Dispute resolution provider: WIPO (Case no. D2002-0228)

Panel: D. Brian King

Identity or confusing similarity: (i) registered trademark; (ii) total incorporation of trademark

Rights or legitimate interests: disclaimer is not always an effective defense

Bad faith: (i) proof of bad-faith registration and use is conjunctive; (ii) circumstances of bad faith listed in the Policy are not exclusive

Process: no Response was filed

Result: the domain name was ordered to be transferred

Decision date: May 14, 2002

Eastbay Corporation v. VerandaGlobal.com, Inc.

Domain name: finalscore.com

Dispute resolution provider: National Arbitration Forum (Case No. FA 0203000105983)

Panel: Richard Page, Esq., Alan Limbury, Esq., Judge Karl Fink (Ret.)

Identity or confusing similarity: (i) registered trademark; (ii) removal of spaces; (iii) addition of generic top-level domain

Rights or legitimate interests: use of domain name as a portal

Bad faith: Complainant bears the burden of proving both bad-faith registration and bad-faith use

Result: the domain name was not transferred

Decision date: May 20, 2002

American Greetings Corporation & Those Characters from Cleveland, Inc. v. Richard Mackessy

Domain names: popples.com, popples.net

Dispute resolution provider: National Arbitration Forum (Case no. FA0204000109374)

Panel: Alan L. Limbury

Rights or legitimate interests: burden of proof on Respondent if any of the circumstances listed in para. 4(c) of the Policy is present

Result: the domain name was not transferred

Decision date: May 22, 2002

The Leading Hotels of the World Ltd. v. Online Travel Group

Domain names: leadinghotelsworldwide.com, leadinghotels.com, leading-hotels-worldwide.com

Dispute resolution provider: WIPO (Case no. D2002-0241)

Panel: Andrew F. Christie

Identity or confusing similarity: (i) registered trademark; (ii) previous ICANN decisions; (iii) descriptive phrases give rise to distinctiveness

Rights or legitimate interests: (i) use of domain name (ii) knowledge of trademark

Bad faith: (i) descriptive domain name; (ii) registration after notice of dispute

Process: telephone conversation with case manager

Result: the domain name *leadinghotels.com* was not transferred but the domain names *leadinghotelsworldwide.com* and *leading-hotels-worldwide.com* were ordered to be transferred

Decision date: May 24, 2002

Richard Ravid, Inc. v. James Kang

Domain name: focus21.com

Dispute resolution provider: National Arbitration Forum (Case No. FA 0202000104997)

Panel: Moon Sung Lee

Identity or confusing similarity: (i) registered trademark; (ii) combination of common nouns and numbers can be registered as trademark

Bad faith: (i) list of examples of bad faith in the Policy is not exhaustive; (ii) Complainant bears the burden of proof and it is not reversible

Process: language of the proceeding is dependent on the language of the registration agreement

Result: the domain name was not transferred

Decision date: May 8, 2002

ChinaLucky Film Group v. Hu haobo

Domain name: luckyfilm.com

Dispute resolution provider: National Arbitration Forum (Case No. FA0204000109372)

Panel: Carolyn Marks Johnson

Identity or confusing similarity: (i) registered trademark; (ii) descriptive term does not always overcome confusing similarity

Rights or legitimate interests: inference to be drawn on message found on the site

Result: the domain name was ordered to be transferred

Decision date: May 28, 2002

INTERNET GOVERNANCE

ICANN Under Review

By Kate Ellis, a solicitor in the Intellectual Property Department of the Manchester office of Eversheds; e-mail: KateEllis@eversheds.com

Following the article "ICANN at a Crossroads" which appeared in the August 2002 edition of World Internet Law Report*, in the past month there have been significant developments in the process of reform that is taking place within ICANN.*

In recent months, the Internet Corporation for Assigned Names and Numbers – ICANN – has been the subject of intense scrutiny and its role, performance and future has been under review. The reform of ICANN has now reached a critical stage and whilst ICANN itself may be unknown to all but a small minority of Internet users, the outcome of the review will directly or indirectly affect all Internet users.

ICANN is the organisation responsible for the operation of the Internet and the co-ordination of the Domain Name System (or, "DNS"). ICANN was established in November 1998 as a not-for profit public benefit organisation, based in California and intended to assist the U.S. government in transferring its responsibility for the operation of the Internet to the private sector. In November 1998, the U.S. Department of Commerce entered into a Memorandum of Understanding ("MOU") with ICANN that effectively gave ICANN temporary authority for the technical and management responsibilities of the Internet.

The review of ICANN's activities has been on two fronts. First, the MOU was due to expire on September 30, 2002 and it has been the subject of discussion as to whether it would be renewed, renegotiated or replaced. Secondly, following the publication of a report – "ICANN, the Case for Reform" – by ICANN's president, Stuart Lynn, which identified ICANN's weaknesses, since July 2002 ICANN's Committee for Evolution and Reform has been involved in a consultation process with the Internet community to review ICANN's role and responsibilities. This consultation period is to be concluded in October 2002 and the future direction of ICANN – and, in turn, the future functioning of the Internet – will be determined. These two inextricably linked developments have provided a sharp focus to the debate about ICANN's future, which is due to culminate in October at ICANN's meeting in Shanghai.

The MOU – ICANN's authority to operate

Key to understanding the debate about ICANN is that it is a private organisation performing quasi-governmental roles. It decides which new Top Level Domains should be introduced and who will be in charge of them, it oversees the registrars who sell domain names and it has adopted a dispute resolution policy for resolving certain types of domain name disputes, the Uniform Dispute Resolution Policy, or "UDRP".

The four principles behind the U.S. government's privatisation effort for the technical management of the Internet were: to ensure stability on the Internet, increase competition, secure representation from the wider Internet community and "bottom up" co-ordination rather than government control. Originally, the U.S. government envisaged that the process of transferring responsibility for the Internet to ICANN would be completed by September 30, 2000. However, the MOU has been extended twice and was due to expire on September 30, 2002.

In June 2002, the U.S. Senate Sub-committee on Science, Technology and Space conducted a hearing into the governance of the Internet. Some of the evidence presented to the Sub-committee was critical of ICANN. Some U.S. senators expressed concerns about ICANN and recommended that responsibility for the Internet should be brought back within the ambit of the U.S. government.

In August 2002, ICANN submitted a Fourth Status Report to the U.S. Department of Commerce, which provided an update in relation to its progress towards the objectives contained in the original MOU, namely it had:

- partially achieved its task of providing expertise related to the technical management of the DNS;
- partially completed its objective of securing a stable relationship with the Regional Internet Registries ("RIRs");
- not completed its development of an Independent Review process;
- partially completed the improvement of root server security;
- made only limited progress to improve relationships with the registries which operate the country name Top Level Domains; and
- made good progress with the introduction of new TLDs.

In the Report, ICANN stated that "successful completion of [the] reform process is ... critical to the successful completion" of the transfer of responsibility for the Internet to it.

Whilst it has been uncertain as to whether the U.S. government would agree to extend the MOU, on

September 20, it was announced that the MOU would be extended until 30 September 2003. However, in its statement regarding the extension, the U.S. Department of Commerce stated that it has "frankly been disappointed that ICANN's progress on the MOU tasks has moved so slowly". It was recognised that

> "ICANN has been troubled by internal and external difficulties that have slowed its completion of the transition tasks and hampered its ability to garner the full support and confidence of the global Internet community".

A further reason cited by the U.S. government for the extension of the MOU was the lack of an alternative structure for the long-term management of the DNS.

Following the criticism about ICANN, the MOU has been revised. It is more restrictive and obliges ICANN to undertake significant reforms in a number of key areas. ICANN's efforts are now to be focussed on:

- addressing the scope of its mission;
- improving the transparency and accountability of its decision-making;
- its responsiveness to Internet stakeholders;
- defining an effective advisory role for governments; and
- the security of the Internet.

In its statement, the U.S. government provided a clear message to ICANN that the next year is "critical" and that it will be "closely monitoring ICANN's efforts" through a quarterly reporting mechanism. Accordingly, whilst ICANN has survived, the U.S. government has sent a clear signal to ICANN that unless it acts quickly and decisively to achieve its goals under the MOU, its existence in the longer term will be in jeopardy.

The Reform of ICANN

On June 28, 2002, ICANN adopted a paper, prepared by ICANN's Committee for Evolution and Reform – "A Blueprint for Reform" – which set out proposals for reform in response to the concerns which had been expressed about it. ICANN also directed the Committee for Evolution and Reform (or, the "ERC") to oversee the implementation and transition work based on the Blueprint.

To assist it with the reform, the ERC appointed four "Assistance Groups" to address specific issues, namely:

- global names policy development;
- accountability;
- the formation of an "At Large Advisory Committee"; and
- the implementation of a Country Names Supporting Organisation.

It was envisaged that the Assistance Groups would not be a substitute for input from the wider Internet community – which ICANN has been heavily criticised for excluding – but they would rely on qualified personnel to address the specific issues within a short time frame, independently of the ERC. The interim reports produced by these Groups have been made available to the public for comment. The ERC has also produced Interim Implementation Reports on August 1, and September 2, 2002.

The process of consultation is expected to be concluded prior to ICANN's meeting in Shanghai in October during which the ERC will put forward its recommendations, having reviewed the Assistance Groups' proposals, to ICANN's Board for consideration.

Global Names Policy Development

The ERC appointed a 'Names Policy Development Process Assistance Group' to consider the Blueprint's proposals for domain name policy development. On August 21, the Group posted its recommendations, which included the implementation of a designated time frame (95 days) for the evaluation and resolution of any policy development process.

The ERC's Second Interim Implementation Report, stated that the ERC was "inclined to recommend the acceptance" of the Group's proposals with only a few slight modifications to ICANN's Board. It is likely that the introduction of a timetable and process for the consideration of names development policies will be welcomed by the broader Internet community.

Accountability

ICANN has faced extensive criticism about its perceived lack of accountability and governance. In the Blueprint, it was suggested that, to improve accountability, an Office of Ombudsman should be created together with a 'Manager of Public Participation' ("MPP") and that ICANN's independent review policies should be reconsidered.

In its First Implementation Report, the ERC stated that

> "a principle focus for the ICANN reform process is the structuring of workable and appropriate mechanisms to permit adequate public input into the ICANN process, while ensuring that those mechanisms are consistent with an effective and workable ICANN".

It was recognised that there were two conflicting issues that had to be considered. First, the right of the wider Internet community to have the opportunity to participate in ICANN and secondly, the need to ensure that the processes and procedures are workable.

On August 23, the Group tasked with reviewing ICANN's accountability recommendations (that the selected Ombudsman be "an advocate of fairness" who would be responsible for assessing complaints about ICANN) endorsed the suggestion of an appointment of a MPP, who would be responsible for developing mechanisms to encourage public participation in ICANN.

The Group also made a number of additional observations that had not been included in the Blueprint. First, it recommended that ICANN's bylaws should be amended to provide flexible protection against "mission

creep" – stepping outside its ambit of responsibility – for which ICANN has been criticised. It went on to suggest that "ICANN lacks an accountability mechanism to check misuse of authority to determine whether or not a particular action would constitute or require the development of policy" and that such a system should be established.

In its Second Interim Report, the ERC indicated its general agreement with the Group's recommendations, particularly in relation to the proposals for an Ombudsman and MPP. However, whilst the ERC said that it welcomes comments about the introduction of mechanisms to protect against mission creep and abuse of certain processes, it thinks that "these issues are likely [to be] beyond the scope of the current reform process". It is probable that such a comment will incite criticism from those parties advocating a root and branch overhaul of ICANN.

At Large Advisory Committee

A further criticism of ICANN has been a perceived lack of representation within ICANN. In this regard, the Blueprint advocated the creation of an "At Large Advisory Committee" (or, "ALAC") as a "vehicle for informed participation in ICANN by the broader user community".

On August 19, the ALAC Assistance Group, filed a Report which set out its proposals for the establishment of an ALAC. It was recognised that the creation of an ALAC was "a critical first step towards structured involvement of the individual user community in ICANN" and that

> "without a structured entity such as an ALAC capable of presenting user perspectives, a critical group of stakeholders would be excluded from the reformed-ICANN".

To ensure user participation in ICANN it was recommended that procedures should be put in place for the dissemination of information from ICANN to the wider community. The developing world was also identified as being a key target for increased involvement and outreach programmes were recognised as being useful tools to fulfil the ALAC's objectives.

In its Second Interim Report, the ERC agreed that establishment of an ALAC was a critical step towards involvement of the Internet community in ICANN and it indicated that it will probably recommend the Group's proposal to ICANN's Board following the conclusion of the consultation process.

Country name registries

The lack of agreements between ICANN and the country code domain name operators has been identified as a key challenge for ICANN. The funding of ICANN is a critical issue. ICANN derives most of its funding through fees paid to it by the registries responsible for the top level domains (such as .com, .net) and country name registries. However, only four country name registries have put themselves under a contractual obligation to fund ICANN. Reaching agreements with these registries is a priority for ICANN. The Blueprint suggested that a Supporting Organisation should be established for the registries which operate the country name TLDs to promote greater liaison and consensus between ICANN and the registries.

However, the Blueprint's proposals did not meet up to the country name registries' demands and the registries posted a critical response to the Blueprint. In particular, they did not agree that ICANN should be able to impose policy decisions on them without their consensus support (that is, a two thirds vote of the code name registries voting in each region). They also suggested that the country name registries must be part of the decision processes that determine which issues are "global" and within ICANN's jurisdiction. The registries also sought sole responsibility for appointing members to the Supporting Organisation.

The ERC only appointed an Assistance Group to review the implementation of a country names Supporting Organisation on September 13, 2002 and, at the time of writing, the Group has not submitted its report. However, ICANN's ambition to enter into formal agreements with the country name registries is undoubtedly going to be difficult to achieve, particularly as there is little incentive for the registries to enter into such agreements.

Observations on the Reforming Process

It is accepted – even within ICANN itself – that reform is required. From its Implementation Reports, it appears that the ERC is listening to the comments it is receiving from the Internet community – or, at least the powerful players. For example, following the country name registries lodging their criticisms of the Blueprint, the ERC – belatedly – appointed an Assistance Group to consider the position of country name registries. Also, on September 13, the three Regional Internet Registries (the regional bodies which allocate IP numbers) publicly declared that they were unable to support the ERC's proposed reforms as they felt that ICANN had ignored their proposals for reform. Almost immediately, ICANN issued a statement in an attempt to placate the RIRs notwithstanding that the ERC had, from the outset, stated that it would not respond to comments from the wider Internet community.

The consultation process is now drawing to a close and it should be completed prior to its meeting in Shanghai in October when the ERC will put forward its recommendations for reform to ICANN's Board. It will then become clear whether ICANN has listened not only to the criticisms of the 'powerful' sectors within the Internet community, but also the individual users of the Internet.

It is not yet certain whether the reforms will be sufficient for the U.S. government to ultimately transfer its obligations for the technical management of the Internet to ICANN. However, it is certain that ICANN will always have its critics.

■ DOMAIN NAME DISPUTES

Special Relationship Extends to Domain Names

In the first example of the United Kingdom and United States co-operating to deal with domain name issues, the Office of Fair Trading (OFT) has recently intervened to stop two London-based companies offering .brit, .usa, .scot and .sex domain names under the promise that "the latest domain name has arrived".

All of these domains do not register on usual browsers or through usual search engines. They can only be accessed via a modified browser. The OFT took the view that "the adverts gave the impression that the domain names on offer operated as top-level names such as .com and that was misleading".

Although the OFT has powers to obtain a court injunction, it has settled for written assurances from the individuals involved that they will not publish these or similar adverts for the registration of domain names.

John Vickers, Director General of Fair Trading, commented:

"It is important that consumers and businesses seeking domain names know exactly what they are buying and how accessible the domain names will be. This case illustrates that consumers can be protected wherever traders are based. The OFT will co-operate with international enforcement partners to achieve this".

This action by the OFT is encouraging for both consumers and businesses and should sound a warning to many other businesses offering similar services. Equally, those who have inadvertently registered such unofficial domain names should act now to register an official domain accessible by all Internet users.

Vanessa Barnett, Berwin Leighton Paisner; e-mail: vanessa.barnett@blplaw.com

FORTHCOMING EVENTS

■ INFORMATION TECHNOLOGY

IST 2002 – Europe's Main IT and Communications Research Event to be held in Copenhagen

A conference for research and development in Information Society Technologies (IST) will be held in Copenhagen in November 2002. The two-day event, which will run from November 4 to November 6 inclusive, has been organised by the European Commission, in partnership with the Danish Ministry of Science, Technology and Innovation.

The Commission has highlighted the conference as a "networking" opportunity and an ideal place for researchers to meet and be met by other researchers wanting to form consortia for research projects in the IST field.

The main purpose of the event is to assist European researchers and industrialists in building and strengthening their networks for research and technological collaboration, at a time when the IST priority within the E.U.'s sixth Framework Programme for Research and Technological Development is getting underway.

For the first time, this annual event will be open to all European research in the IT and communications sector; whether this be funded at European, national, or regional level or even entirely by industry. A series of "Calls for Ideas" for conference sessions and exhibits, launched in March 2002, have generated a high level of interest and response from organisations across Europe.

> "This is an event designed to capture the ideas and imagination of Europe's Information Society community, and to strengthen the European Research Area in the field of information and communications technologies", explained Erkki Liikanen, European Commissioner for Enterprise and the Information Society.

Further information and online registration facilities are available at: *http://2002.istevent.cec.eu.int/*