BNA International

World Internet Law Report

International Information for International Businesses

Monthly news and analysis on Internet law and regulation from around the world

Volume 7, Number 1 January 2004

Articles

Case Reports

News

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

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: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £695; Eurozone €1150; U.S. and Canada U.S.$1150. 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.bnai.com*
ISSN 1468-4438

Welcome to the first issue of 2004 and to a new look *WILR*! To complement the changes we have made to our information service at *www.bnai.com*, we have taken the opportunity to update corresponding print formats and hope that you like the new design.

We are pleased to include a detailed article on mobile business in our E-Commerce section this month, provided by Esther Nunes and Camila Parise of Pinheiro Neto. The article focuses on the legal framework underpinning the telecommunications industry in Brazil and charts the development of mobile technologies. It also suggests that traditional discussions about the authenticity, security and privacy of electronic transactions, or the need for regulation might be losing ground to more relevant issues, focusing on Internet access infrastructure and the necessary telecommunications networks.

Other articles in this section include commentary on Standard Terms for E-Commerce in Germany and Electronic Invoicing and Filing, in both Central Europe and the Philippines.

Cases this month include a report by Wouter Pors of Bird & Bird on the recent Dutch Supreme Court ruling in the *Buma/Stemra v. KaZaA* case and Paul Barton, a partner in the Technology Law Group of London firm Field Fisher Waterhouse, analyses the significance of the DocMorris case to online pharmacists and to the concept of the free movement of goods within the European Union. The IE Domain Registry, responsible for administering the country code for Ireland, has delivered its first decision under the new .ie Dspute Resolution Policy (reported by Kate Ellis of Eversheds) and Patrick Michielsen of Stibbe provides an update on the first CEPANI ruling on a geographical domain name, in this instance: *www.belgie.be*.

I look forward to receiving your comments and suggestions at nicholad@bna.com

Nichola J. Dawson

We wish to thank the following for their contribution to this issue:

Paul Barton, Field Fisher Waterhouse, London; *Dennis G. Dimagiba, Shennan A. Sy* and *Saben C. Loyola,* Quisumbing Torres Law Offices (an associate firm of Baker & McKenzie), Manila; *Tim Dixon,* Baker & McKenzie, Sydney; *Kate Ellis,* Eversheds, Manchester; *Axel Freiherr von dem Bussche,* Taylor Wessing, Düsseldorf; *Gabriela Kennedy* and *Joanne Harland,* Lovells, Hong Kong; *Zbynek Loebl,* Central European Advisory Group, *Dr. Tamás Gödölle,* Bogsch & Partners and *Tomáš Rybár,* Èechová Rakovský Law Firm; *Patrick Michielsen,* Stibbe, Brussels; *Clara Bordoy Mateo,* Abril Abogados, Madrid; *Glyn Morgan,* Taylor Wessing, London; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Esther Donio Bellegarde Nunes* and *Camila Martino Parise,* Pinheiro Neto, São Paulo; *Dr Cristos Velasco,* Postgraduate Unit of Instituto Tecnologico Autonomo de Mexico; *Wouter Pors,* Bird & Bird, The Hague; *Heather Rowe,* Lovells, London; *Dr Cento Veljanovski,* Case Associates, London.

Competition

Regulation v. Antitrust: Gaps in the New EC Regulatory Regime for the Communications Sector

By Dr Cento Veljanovski, Managing Partner of Case Associates (competition and regulatory economists). The author may be contacted at cento@casecon.com

The new EC regulatory framework for communications creates a complementary and convergent relationship between competition and regulatory laws. Its central reform is to base *ex ante* regulatory intervention on competition law principles. It is also based on the premise that *ex ante* regulatory law should complement competition law and be applied only where it is established that *ex post* competition law is insufficient. While these are the legal presumptions underpinning the EC Framework Directive,[1] the reality may be quite different since no criteria are given to identify when competition law can be regarded as insufficient. Indeed, there is an inherent difficulty in areas other than price controls, since the remedies and principles of intervention are almost identical. In this article, several gaps and unresolved issues concerning the relationship between competition law and the new regulatory regime are discussed.[2] Since the Framework Directive's focus is to ensure that access to broadband network infrastructure and services is not unreasonably denied to those seeking access, the concerns here will be of particular interest to the Internet sector.

Insufficiency of Competition Law

The new regulatory framework does not give guidance to the National Regulatory Authorities (NRAs) on how to decide when regulatory intervention should be preferred to competition law. This appears to be left for the NRA to resolve, in consultation with the National Competition Authority (NCA) in each Member State. This provision makes sense at one level because NRAs do not generally enforce competition law. Yet the EC Commission has left the matter up in the air. In the EC Recommendation[3] a number of markets susceptible to *ex ante* regulation are defined with the implication that these are also markets in which competition law is ineffective. Yet the selection of these markets has been based on transitional requirements so that those sectors regulated under the old ONP framework would also continue to be regulated under the new framework, and hence subject to superficial market analysis only. The role that competition law has or could play in dealing with competitive abuses is simply not discussed.

The case for *ex ante* regulation is apparently based on claims that competition law is costly, slow and ineffective in dealing with the type of market power abuses encountered in the communications sector. This is odd since the administration and enforcement of competition and regulatory laws are fairly similar within the European Union – both are enforced by specialised administrative agencies; have available the same legal remedies, and face similar budgetary constraints, payoffs and operate at similar speed (with the exception of mergers). This contrasts with the situation in other countries, such as the United States, where antitrust law is essentially a judicial approach in which it is arguable that court proceedings are lengthy, resource consuming, and often leads to poor outcomes when a trial takes place before a non-specialised judge and jury. In such jurisdictions it is arguable that greater reliance on regulatory intervention is cheaper, and would be more effective than antitrust. This is not the case within the European Union.

Differential Evidentiary Standards

In some quarters it is argued that the difficulty with using competition law is that the legal standard of proof is too high. Oftel, which almost uniquely among EC Member States enforces both U.K. regulatory and competition laws in the communications sector, has stated that it rarely uses its competition law powers to intervene because establishing a competition law case is too demanding. This suggests that major criteria for the imposition of *ex ante* regulation will be administrative ease rather than the rigorous identification of permanent market power problems.

The proposition that NRAs can intervene on the basis of less analysis and evidence of market power abuses than NCAs is a highly suspect justification for *ex ante* regulation. This is especially so given that *ex ante* regulation is designed to deal with manifest and permanent market power concerns. The recent annulments of the EC Commission merger decisions point to the tendency for regulators to develop a culture of evidentiary short cuts which undermine their effectiveness and legitimacy.[4] There is a need for checks and balances on the NRAs' exercise of discretion, and the Framework Directive recognises this by requiring that NRA decisions under the Framework Directive be subject to an appeal process. However, an appeal process is not an adequate substitute for proper evidentiary standards and reasoned decisions, nor does it justify a bifurcated approach in which different evidentiary standards may be used to apply the same legal principles. Indeed, it is arguable that the evidentiary standard should be at least equivalent too if not higher than that used in competition law because of the permanence of *ex ante* remedies.

In the absence of clarification of the evidentiary standard there is a danger that the new regulatory framework will be administered as a strict liability regime in which the identification of Significant Market Power (SMP), which is identical to dominance under EC competition law, lead to mandatory regulation of operators. This will especially be so because the focus of much regulatory intervention is exclusionary practices (foreclosure) rather than exploitative abuses (high prices). The difficulty in determining whether an alleged exclusionary practice is anti-competitive or simply aggressive but legitimate rivalry is not straightforward.

Private Enforcement

Another "gap" in the relationship between antitrust and regulatory law is the role of private enforcement. Under EC law, antitrust actions can be brought before national courts by the harmed party. The EC Commission's modernisation proposals, which

come into force in 2004, will make private antitrust enforcement even more prominent.

It is arguable that private enforcement will increase the effectiveness of antitrust intervention in the communications sector. Those harmed by an infringement have an incentive to enforce the law driven by the prospect of halting anticompetitive abuses and securing substantial compensatory damages. All things equal, this will increase the level of antitrust enforcement activity, and thereby diminish the need for *ex ante* regulation. On the other hand, a finding of SMP may strengthen private antitrust enforcement by easing the evidentiary burden if it is admitted as evidence of dominance. Allowing this would make *ex ante* regulation more potent, since it would lead to the prospect of civil damages in addition to the regulatory sanctions.

Yet one senses hostility among NRAs and NCAs to the prospect of private actions. These are seen as unnecessary and inefficient, and have the potential to make the public enforcement of both competition and regulatory law more difficult. Whatever the merits of this view, private enforcement has not been analysed in any detail, and it has not been taken into account in the discussion of remedies under the Framework Directive. Clearly, the nature of judicial proceedings differs among Member States, and will have an impact on the sufficiency of the private enforcement of competition law. There is a need, for example, to investigate the differences between adversarial and inquisitorial approaches, and those of specialised judicial competition tribunals.

Emerging Markets

Ex ante regulation should not be applied to new or emerging markets. The EC Framework Directive states, albeit in a Recital, that emerging markets provide a safe harbour because "First Mover Advantages", which would give the innovator a high 'market share' for the new product, should not lead to SMP designation. In emerging markets, market power is likely to be transient, and if not the NRA will have an opportunity to intervene at a later date. The *SMP Guidelines*[5] warn against premature regulatory intervention based on speculative analysis.

The more difficult area is where a new product is introduced by an operator who has SMP in the provision of infrastructure or network services. In such cases the Framework Directive both accepts that leveraging SMP on downstream markets may be an abuse, but for new products this danger should "normally" be left to the case-by-case determination of competition law.

This is an area where there is a real danger of the illegitimate expansion of *ex ante* regulation. It is clear that some NRAs regard the prospect of operators with SMP leveraging their upstream market power onto new products as a frequent and serious anticompetitive abuse. This view may lead some NRAs to fashion per se rules which give downstream rivals and entrants access to the wholesale inputs to replicate the SMP operators' new products. That is, a mandatory access regime for any new products. This danger has already been realised in Oftel's *Access Guidelines*.[6]

The extension of ex ante regulation to emerging markets in this way is illegitimate for two reasons. First, it reverses the legal presumption at the heart of the Framework Directive - that regulatory law complements competition law – to one where competition law is seen as a stop gap to be progressively replaced by ex ante regulatory intervention. Secondly, it overturns the more measured approach adopted by a number of NRAs where the case for access has been granted only if there is a substantial likelihood of significant incremental consumer benefits, and/or it will not deter investment and innovation. This cost benefit approach is not only more economically rational but required under the Framework Directive.

Remedies

The final area where there are some real concerns is the determination of appropriate *ex ante* obligations. When an operator, or operators, has been found to have SMP, NRAs are required to impose "appropriate" and "proportionate" obligations which deal with identified competition concerns. The Access Directive states that *ex ante* obligations "shall be objective, transparent, proportionate and non-discriminatory". NRAs must satisfy a number of requirements in the selection of appropriate remedies:

- they must be justified in terms of the objectives laid down in the Framework Directive;
- applied only in the absence of effective competition (the only exception being mandatory interconnection for all operators);
- when competition rules are ineffective;
- "…specific to the problem, proportionate and maintained only for as along as necessary"; and
- removed when a market is effectively competitive.

While these principles are consistent with good regulation, no practical guidance is given for the matching appropriate obligations to market power problems, nor in selecting between a regulatory or antitrust response.

In recognition of this "gap" the European Regulators' Group (ERG), which consists of representative of E.U. NRAs, has produced a joint consultation document with the EC Commission outlining the approach to remedies.[7] While the discussion seems exhaustive, it fails to address the issues discussed above, nor does it provide any clear guidelines to the NRAs.

Conclusion

The above discussion has highlighted a range of issues which urgently require further discussion and resolution. In summary these include:

- criteria for the choice between regulatory and competition law;
- specification of evidentiary standards which must be satisfied for imposing *ex ante* regulation;
- definition of and criteria for determining emerging markets, and the apparent "safe harbour" provision; and
- the role and impact of private antitrust enforcement.

1 This used to refer collectively to the new "package" of directives, the principle ones being Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, April 24, 2002 (Framework Directive); Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, March 7, 2002 (Access Directive); and Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, 24 April 2002 (Universal Service Directive).

2 For a more detailed assessment see the author's report for the European Telecommunications' Network Operators' Association (ETNO), "Remedies under the New E.U. Regulation of the Communications Sector", June 20, 2003, posted at *www.casecon.com/data/pdfs/ ETNOfinalreport.pdf*.

3 "Commission recommendation on relevant product and service markets within the communications sector susceptible to *ex ante* regulation in accordance with Directive 2002/21/EC of the European Parliament and the Council on the common regulatory framework for electronic communications networks and services", 2003/311/EC,

February 11, 2003 (Recommendation). See also, "Explanatory Memorandum on the Commission's recommendation on relevant product and service markets", May 8, 2003.

4 Case T-342/99 *Airtours v. Commission* (2002) ; Case T-310/01 *Schneider Electric v. Commission* (2002); Case T-5/02 *Tetra Laval BV v. Commission* (2002).

5 "Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services", 2002/C 165/03, August 11, 2002. (SMP Guidelines).

6 "Imposing access obligations under the new E.U. Directive – Guidelines", (September 13, 2002). See Case's comments on Oftel's Consultation Document: "Imposing Access Obligations on Innovative Communications Markets, Annex 1 to BT Submission" posted at *www.btplc.com/Corporateinformation/Regulatory/RegulatoryInformation/oftelConsultativeDocuments/Accessobligations/Appendix1.pdf*.

7 Consultation Document on a Draft joint ERG/EC approach on appropriate remedies in the new regulatory framework, 21/11/2003.

Consumer Protection

News

MEXICO

Increased Protection for E-Commerce Consumers

On November 6, 2003 the Mexican Senate approved a Project of Decree (available for download at *www.profeco.gob.mx/html/juridico/juridico.htm*), to reform, add and amend several provisions to the Federal Law of Consumer Protection (FLCP). The scope of the reform is very broad; however the articles that specifically deal with consumer protection in electronic commerce are:

- Article 16, which provide an obligation for retailers and companies that use consumer information for marketing and advertising purposes, to inform those consumers at no cost that their personal data has been retained. If such information exists, retailers and companies must make it available at the request of the consumer or his representative. Companies must also inform consumers if any of their personal data has been shared with third parties, as well as informing them as to the identity of such third parties and the recommendations carried out. This article also sets forth the terms and conditions that the retailer's reply should contain and the criteria to make the correction of consumer's information.
- Article 17, which sets out the type of information, such as name, address, telephone and e-mail address which suppliers should make available to consumers when contacting them. Article 17 also provides for the right of consumers to opt out of receiving direct marketing materials by fax, e-mail or any other medium when suppliers offer goods, products or services.
- Article 18, which allow the consumer protection agency (PROFECO) to maintain a public registry of consumers that have opted out of receiving information for marketing and advertising purposes. Under this article, consumers may solicit their subscription to the said registry in writing or by-e-mail. Article18BIS prohibits companies and suppliers from using consumer information other than for marketing and advertising purposes, as well as preventing them from sending promotional materials to consumers who have opted-out, or who are registered in the consumer registry of PROFECO. Section VII of Article 76BIS specifies that suppliers shall abstain from using sales or advertising strategies that do not provide the consumer with clear and sufficient information on the services offered. This applies particularly to marketing practices, which target vulnerable sectors of the population, such as children, the elderly or infirmed. Suppliers must also incorporate mechanisms that warn when the information is not suitable for such groups.
- Article 97 allows consumer to file complaints before PROFECO using electronic means and through PROFECO's website.

Articles 126, 127 and 128 increase the penalties for non-compliance from $480,000 to a maximum of $2,520.000 Mexican pesos.

The decree, approved by the Senate, is still pending for publication in the Official Journal (Diario Oficial). Once published, the decree will enter into force 90 days after its final publication, except for some articles that will require a longer period for implementation by PROFECO.

The reforms to the FLCP only strengthen the rights of consumers with regard to the publishing and marketing information they choose to receive from companies and retailers in the context of e-commerce transactions. The reforms fail however, to address other important concerns for cyber consumers. One of the challenges of PROFECO under the new legislation will be to stop fraudulent commercial practices, such as the emerging "illegal pyramid schemes" (whereby a company offers consumers the promise of economic benefits in exchange of a membership fee and to persuade other people to get involved in the business and the payment of other membership fees until the scheme collapses.

Typically, these businesses have no physical presence, and it is usually very hard to tack their online activity and enforce the law.

These types of "illegal pyramid businesses" are causing an irreparable economic loss to vulnerable individuals with access to debit and credit cards. Therefore, it is important that PROFECO along with the Mexican Cybercrime Unit (DC Mexico) and other consumer and enforcement agencies around the globe work closely on this issue, to stop these activities in Mexico and impose severe sanctions and fines on the companies and persons involved.

*By **Cristos Velasco**, Professor of Internet and e-commerce law at the Postgraduate Unit of Instituto Tecnologico Autonomo de Mexico (ITAM); e-mail: cristosuofa@yahoo.com.*

E-Commerce

Mobile Business: The Brazilian Legal Framework for the Mobile Future

By Esther Donio Bellegarde Nunes and Camila Martino Parise, Partner and Associate Lawyer, respectively, in the Telecommunications and Internet Group of Pinheiro Neto. The authors are based in the São Paulo office of the firm and may be contacted at: esthernunes@pinheironeto.com.br and camila@pinheironeto.com.br.

The recent breakthroughs in information technology and communications have dramatically changed the way people interact and do business, their perception of time and space, and the infrastructure capable of catering for the day-to-day needs of ordinary citizens. As geographical barriers were removed, new cultural, social and business behaviours that were hardly imaginable until recently have come into existence.

This technological revolution came into full bloom as Internet use spread worldwide, promoting the interchange of ideas and information, while gaining recognition as the right environment for trade relations. The growth of the Internet and its unprecedented market penetration have surely contributed to the upsurge of new techniques designed to make deals and transactions effective, followed by the development of capabilities and strategies for the supply of products and services through the Internet (e-commerce).

E-Commerce

In its infancy, e-commerce limited its use of the Internet to the promotion of products and services; the closing of deals occurred through traditional means (via issuance of purchase orders and vouchers). Slowly but surely, however, other e-commerce initiatives gained momentum, such as virtual stores (accepting trades through the Internet), e-auctions and online banking transactions, all of which promoted the Internet as a tool for doing business.

E-commerce uses complex technologies to guarantee the authentication and security of transactions, but it was the celerity and straightforwardness of online transactions that turned the Internet into a success story for communications and business.

By July 2003, e-commerce sales in Brazil had exceeded R$ 98 million.[1] Brazil currently ranks ninth in the number of hosts[2] worldwide, ahead of countries like Spain, Russia and Mexico.[3] In South America, Brazil ranks first.[4] In addition, more than 450,000 domains have already been registered in Brazil, most of them being the so-called "com.br", which are generally intended for use in business transactions.[5]

Recent years have witnessed extensive discussions over the validity of e-business transactions; the need to pass specific rules and regulations for this new business mode; and the e-commerce perspectives in light of the "dot-com" fiasco.

Although some concepts germane to e-commerce (such as electronic signature, digital certification, spamming and cookies) are already part of everyday life, the speed at which applications appear and evolve in the cyberworld has placed a new reality ahead of us. This will perhaps return to the fore certain long-running debates about the role of the Internet and its use as an effective means for communication and business, as in m-commerce.

M-Commerce

"M-commerce" stands for the offer of products and services through the Internet, supported by mobile telecom services. It is generally viewed as a specie of the e-commerce gender, as both activities are based on data transmission and reception techniques as well as on the offer of products and services through the Internet.

The major distinctive feature between e-commerce and m-commerce lies in the telecommunication vehicle supporting the Internet access, as well as in the infrastructure for navigation by users. While e-commerce relies on fixed telecom services and PCs, m-commerce uses mobile equipment for access through mobile services.

As the concepts of e-commerce and m-commerce are quite similar, legal discussions involving m-commerce issues are unlikely to bring major innovations when compared to e-commerce. In general terms, such discussions will gravitate around the nature of electronic transactions as a whole, without special emphasis on the means adopted for their occurrence (fixed telephony, mobile telephony, cable, fax, *etc*.)

However, some of the issues relating to e-commerce may call for in-depth discussions and review because of some elements intrinsic to m-commerce, such as the mobility of infrastructure used for m-commerce transactions, as well as the technical features of handsets available for mobile access to the Internet, not to mention a number of other eminently technical issues.

So far, m-commerce has not prompted extensive discussion in Brazil, mostly because of the Brazilian regulatory framework for mobile services and the existing structure for Internet access, as will be explained below.

The Brazilian Regulatory Framework

Internet

Under Brazilian law, the term *Internet* is understood to mean the networks, transmission and switching means, routers, equipment and protocols necessary for communication between computers, as well as the software and data existing in such equipment.[6]

From a Brazilian legal perspective, the Internet *per se* does not qualify as a telecom service, since it entails no incoming or outgoing transmission of data or information of any kind through electromagnetic processes,[7] which is necessary to characterise a telecommunication service for whatever

purpose. As a result, the Internet is not subject to the rules and inspection authority of the Brazilian Telecommunications Agency (ANATEL). To achieve its major objective (*i.e.*, communication between computers), the Internet should be supported by a telecommunications service that will carry data and information from one point to another. This activity falls under the Value-Added Service concept set forth in the Law No. 9.476/97 (the "General Telecommunications Law LGT").[8]

Internet Connectivity Service

By the same token, Internet connectivity services are not comparable to telecommunications services under Brazilian law and, as such, the ANATEL rules do not apply in this case either. Besides, the legal definition of "Internet connectivity service" treats it as a value-added service by which users and providers may access the Internet. [9]

In this sense, an Internet Service Provider (ISP) should hire the transmission means (*i.e.*, telecommunications services) necessary to connect users to the World Wide Web and allow for the offer of products and services through the Internet.

This being so, the concepts of Internet or connectivity services are intertwined with telecommunications services. And, within the specific realm of m-commerce, mobile telecom services are brought into play, especially Mobile Cellular Services (Cellular Service)[10] and their successor, Personal Communications Services (PCS).[11]

Mobile Services in Brazil

From Public Monopoly to Market Competition

In Brazil, mobile telephony made its debut in the mid-1990s, in the so-called "A Band". At that time, Brazilian telecom services were provided under a veritable public monopoly, through incumbents within the Telebrás System[12] and mobile phone access was scarce (with c. 667 cell phones in operation).[13] Given the high activation costs and tariffs charged by the telcos, Cellular Service was for a privileged minority only.

The mobile telephony market in Brazil was opened up (as the first step forward in the ensuing development of mobile services) in the mid-1990s, when Constitutional Amendment 8/96 was enacted and Law 9295/96 was passed, allowing private concerns in the mobile telephony segment.

A number of rules and regulations were then issued for mobile cellular services, such as Ruling NGT 20/96, which laid down the standards and guidelines for competition among private companies and government-owned incumbents already operating mobile cellular phone services ("A Band"). On January 13, 1997, the Ministry of Communications published a bidding notice inviting private companies to offer mobile cellular services under the "B Band". According to the bidding notice, the winning bidder was ensured that, until December 31, 1999, the government would not allow the start-up of other new Cellular Service operations.

Several disputes delayed the bidding process, which extended the time frame for execution of the contracts.

At the end of the B-Band concession process, the Federal Government still controlled landline phone incumbents and A-Band mobile cellular phone companies. To complete the privatisation process, these federal incumbents were transferred to private control via privatisation of the Telebrás system.

The Benefits from Privatisation

After privatisation in mid-1998, competition developed in the mobile telephone industry. In 1999, Brazil had some 15 million mobile phone access, more than double the 1998 figures and nearly twenty times more than compared with 1994 figures,[14] with a better distribution of usage throughout the Brazilian social echelons. At the end of the first quarter of 2000, mobile phone access totalled approximately 18.5 million, and they nearly outnumber the total access of the Public Switched Telephone Services ("PST") installed today.

The determining factors for this rapid growth were the sharp reduction in service fees; the implementation of prepaid phone systems; and the improvement of technologies applied to these services.

In the short term, Brazil moved forward from the first generation of Cellular Service, based on analog technologies that offered only voice transmission capabilities (of a not always satisfactory quality) to a restricted number of cell phones served at each installed switch-station, to the second generation of technologies and, now, to an intermediate stage between the 2G and 3G mobile services. This latest stage has approximately 40.093 million cell phones in operation,[15] as opposed to the 39.1 million PST installed.[16]

2G Mobile Technology

The second generation of mobile telephone technology was marked by digitalisation of 1G analog networks. In Brazil, 2G materialised into the implementation and development of CDMA and TDMA technologies, which were compatible and offered automatic roaming capabilities, translating into a better quality of services and greater network capacity.

The transmission rate in 2G mobile services was increased to 14.4 Kbp/s. This rate served for the transmission of short messages and Internet access through mobile phones, but it was still inadequate for the advanced multimedia resources necessary for m-commerce applications.

In Brazil, 2G Internet access basically occurred through the Wireless Application Protocol (WAP), a set of communication protocols used for mobile Internet access. Despite the significant number of WAP users in Brazil, as well as the growth expected for this facility, the technology poses some inconveniences. WAP was the object of harsh criticism on the part of its users, irrespective of the service provider. Most complaints refer to the slowness, lack of content and security, and high tariffs involving such services.

Such factors frustrated user expectations about mobile access to the Internet, and were a substantial obstacle to m-commerce activities in Brazil.

However, as WAP is a technology (not a telecommunications service), and Internet services are treated as value-added services (not telecommunications services), ANATEL cannot issue any rules that are specific to their functionalities, nor can it establish quality standards in the way it does for telephone service providers.

2.5G Mobile Technology

Digital standards for 2.5G mobile services focused on frequency upgrades and new technologies, powering up data transmission capabilities and making narrow-band Internet access (and, by extension, electronic messaging) feasible. This

phase, known as 2.5G, precedes the much-coveted 3G mobile services currently being developed in Brazil.

Were it not for the incompatibilities between the 2.5G technological standards adopted in several countries (such as GSM, in Europe, and CDMA, in the United States), this mobile service generation could well be viewed as the cornerstone for development of m-commerce activities on a worldwide scale. After all, 2.5G technologies accept high wireless transmission rates, allowing greater interactivity between users and Internet mobile services, in addition to an extensive offer of products and services on the net.

But these technological incompatibilities create insurmountable barriers to trade relations characterised by the non-existence of frontiers and full user mobility. After all, a system running on CDMA technology cannot survive at a place served by the GSM system. This fact alone is enough to dampen the growth of m-commerce worldwide.

3G Mobile Technology: IMT–2000

These technological incompatibility setbacks were overcome by a system that is expected to serve as a unified standard for mobile services worldwide: IMT–2000.[17] This system seeks to harmonise, to the greatest extent possible, the myriad projects for 3G technologies the world over, thus avoiding new technical incompatibilities and fostering the development of m-commerce on a worldwide scale.

IMT–2000 was designed as a free system without spectrum or technological standard constraints. To that end, IMT–2000 sets out minimum requirements (such as minimum transmission rate or the availability of international roaming services), without actually imposing a technological standard on service operators.

In theory, the voice, data and image transmission rate under IMT–2000 may reach 2Mbp/s, and Internet connectivity may occur on a standing basis. International roaming will also make a difference in Internet access under this system. These two functionalities – international roaming and transmission at high speed – will bolster m-commerce as compared to traditional e-commerce activities.

3G technology has long been under scrutiny by developed countries in Europe and Asia. In Brazil, ANATEL set aside the following frequency bands for primary use by IMT–2000, without exclusivity rights:

- from 1,885 MHz to 1,895 MHz;
- from 1,920 MHz to 1,975 MHz; and
- from 2,110 MHz to 2.165 MHz.[18]

The conditions for use of said bands are yet to be governed by specific regulations, but ANATEL has not submitted this issue for public consultation to date.

When such frequency spectrum was set aside for the IMT–2000 technology, ANATEL expected to put it out for bidding auction in mid-2003. However, the failure of the PCS bidding process in Brazil and its negative repercussions, coupled with the lack of specific regulations for IMT–2000, delayed the launching of these services, with adverse effects on the inclusion of Brazil within the international m-commerce scene.

The Current Stage of Development

Currently, Brazil is lagging behind in implementation of IMT–2000. Brazilian operators are still implementing 2.5G PCS mobile services, as the sale of licences for these services took longer and was more troublesome than originally expected. This was mostly due to the frequency spectrum selected for these services (1.8Ghz), which called for the adoption of a new technological standard (GSM).

The introduction of PCS in the Brazilian market was intended to expand mobile services and offer new value-added services and functionalities, as well as to foster the transition to 3G technology.

Sale of PCS Licences

The first auction for sale of PCS licences covering the C, D and E Bands was scheduled for January 30, 2001. ANATEL viewed it as a landmark event in the telecommunications industry at that time.

Out of the nine PCS authorisations then offered, only those for the three D-Band regions were acquired: by Tele Norte Leste – TNL PCS S.A. (for Region I); by Blucel Group (Telecom Italia) for Region II; and by Starcel Group (Telecom Italia) for Region III. Also, one authorisation for Region I of E-Band was acquired by Unicel S.A. (Telecom Italia).

All subsequent attempts of ANATEL to sell C-Band authorisations for PCS services (totalling four auctions) were unsuccessful, due to the lack of interested parties, even after ANATEL changed the service rules. Faced with these successive failures, ANATEL decided to dilute the frequency bands allocated to C-Band for PCS services, and published a call for tender.[19] Under prevailing rules, every interested company could only acquire frequency bands up to 45 MHz; Cellular Service operators acquiring new C-Band frequency bands would have to migrate to PCS. But this call for tender was also useless, and there are currently no PCS operators at C-Band.

As for the E-Band frequencies set aside for PCS services, none of which was sold for lack of interested parties, ANATEL held one single bidding procedure on November 19, 2002 to sell these frequency bands and those returned by B-Band Cellular Service operators that had migrated to PCS. To that end, ANATEL also changed the original rules so as to split three into 10 regions. Only one of such regions received no bids.

Start-up of PCS Operations in Brazil

PCS operations in Brazil commenced in late 2001, when Telesp Celular (the then Cellular Service incumbent in the State of São Paulo) migrated to PCS. In addition to voice transmission, the company offered data transmission at a speed 10 times faster than that which was previously available.

The frustration of users over Internet mobile access under the erstwhile technology (WAP) has apparently been overcome by the introduction of PCS in Brazil, which adopted faster systems specifically designed to cater to user needs and to justify the substantial investments in this industry.

Current Developments

Despite the delay in launching these services, the mobile service penetration rate is extremely high in Brazil and, as mentioned above, there are currently 40.093 million cell phones in operation, up from 23.188 million in 2000, only 4.7 percent of which offered Internet mobile and multimedia capabilities.[20]

There are no estimates about the number of transactions carried out through PCS in Brazil, but the high mobile service penetration rate (coupled with the number of mobile sets offering mobile access to the Internet) are likely to bolster m-commerce in Brazil.

Technological Implications

Despite the regulatory implications described above, some aspects germane to m-commerce should be considered when promoting this activity, as will be addressed below.

Limited Text Generation and Storage Capacity

The mobiles currently available in the market have a restricted capacity to generate text messages (and most of these sets can store messages up to c. 100 characters). This may stand as an obstacle to the development of m-commerce, in that it limits the extensive disclosure and exchange of information.

Keyboard Size

The keyboard for mobiles currently available in the market is not text-friendly (the keyboard is small and crammed). This fact may discourage consumers to carry out online transactions via mobile.

Displays

Smaller displays make deals increasingly difficult, as products and services cannot be clearly displayed (leaving practically no room for supplier disclaimers as required by law). This might lead to uncertainties and discomfort on the part of users when buying products or services through mobiles.

Charges

Generally, mobile service operators charge for Internet access the same fees payable for local calls to other mobiles of the same incumbent (depending on the service plan). Calls are measured in minutes. However, the average time spent in Internet access calls is generally longer than voice calls. Unless operators create alternative charging plans for Internet access (offering different charges systems for data and voice transmission services), this capability will not be cost-effective for mobile users as opposed to Internet access through the PST network at a far lower rates.

Mobility

The mobility of cell phone users, including through distinct countries, may pose uncertainties for m-commerce, in view of the difficulty in identifying the place where deals were closed.

Prepaid Mobile Services

In Brazil, the introduction of prepaid mobile services came as a response from mobile telephone operators to an increasing default on phone bills that was affecting company profitability. Prepaid service fees are higher than those effective for ordinary (post-paid) mobile services, but no monthly service fee is charged. As a result, users may keep close track of expenses in the prepaid mode, making this service more attractive to the low-income sectors of the populace.

On the other hand, prepaid mobile services run counter to m-commerce development prospects, in that these services are primarily intended to meet basic user needs in terms of voice communication.

Currently, approximately 80 percent of mobile services activated in Brazil operate under the prepaid system.[21]

Legal Issues

As it happened with e-commerce through the PST network, some contend that specific rules should be passed to regulate m-commerce activities. In this sense, many of the legal initiatives underway at the Brazilian Congress to regulate e-commerce could well apply to m-commerce, such as Bill 4906/01 (sponsored by the Senate).[22]

Moreover, Provisional Measure 2200/01-2 – which instituted Brazilian Public Key Infrastructure (ICP-Brazil) to secure the authenticity, integrity and legal validity of documents in electronic form, support applications, and eligible applications using digital certificates, as well as to ensure the safety and security of electronic transactions – could well apply to m-commerce.

After all, at no point does Provisional Measure 2200/01-2 compare electronic documents or online transactions to those specifically carried out through the PST network. On the other hand, for all legal purposes and effects, "public or private documents" are defined as those electronically produced in accordance with such Provisional Measure. By extension, only the statements contained in electronic documents generated via ICP-Brazil are held to be true in relation to the respective signatories.

Despite the above, many of the provisions contained in the Brazilian body of laws (the Civil Code, Commercial Code, Consumer Protection Code and Copyright Law, among others) may likewise apply to m-commerce, as for e-commerce. The fact that legal transactions are being carried out electronically does not restrict or hinder enforcement of the legislation in effect.

Moreover, the technologies used to effect electronic transactions and ensure their validity and integrity should not be expressly regulated, as the rapid developments in this sector would soon render any such regulation obsolete.

Validity of Electronic Documents

The Brazilian laws are quite flexible regarding the means for contracting. According to article 104 of the Brazilian Civil Code, an act is valid whenever:

- the agent is capable of performing such act, according to the definition of capacity contained in the law;
- the object is legal, possible, choate or inchoate; and
- the formalities prescribed by law, if any, are observed.

In view of that, it is clear that electronic transactions are fully valid, unless any special formality is required for that specific act.[23]

In this sense, only transactions that are dependent on a special formality for performance of the respective act – for example, the purchase and sale of real properties, which is conditional on a public deed and respective filing with the Real Estate Registry Office – cannot be made by electronic means.

Offering and Advertising via the Internet

As a general rule, the offers made through the Internet (via fixed or mobile access) should comply with the Brazilian Civil Code (under its new version enacted by Law 10406/02) and,

whenever applicable, with the Consumer Protection Code (Law 8078/90).

Under the Brazilian Civil Code, a proposal is binding on its proponent.[24] The proposal may be carried out between *present* or *absent* parties, and will be binding:

- until the addressee expressly or implicitly rejects the proposal; or
- until one of the causes for suspension of this binding nature is evidenced, as set forth in article 428 of the Brazilian Civil Code.

The Civil Code considers present a person who contracts by telephone or similar communication means. The proposal in this case should be immediately accepted by its addressee, under the penalty of no longer being mandatory and binding on the proponent.[25]

The meaning of this expression "similar communication means" is not clear, particularly whether the Internet and e-mail fall under this concept.

The Consumer Protection Code sets out that:

> "all information or advertising sufficiently accurate, disclosed by any form or communication means, in connection with products and services offered or presented, is binding on the supplier that disclosed or used it, and is deemed an integral part of the contract to be entered into".

Furthermore, the offer and presentation of products or services must ensure correct, clear, accurate, visible and Portuguese-written information on their characteristics, quality, quantity, composition, price, warranty, "best before" period and origin, among other data, as well as on the risks to consumer health and safety. Additionally, suppliers must specify the term for compliance with their obligation.

Should the supplier fail to comply with the offer, presentation or advertising, the consumer may take judicial measures.

The Law furthermore prohibits all misleading and abusive advertising, including by omission of information.

Websites

In principle, an offer via a website may be accessed indiscriminately by any interested party at a specific electronic address. The relationship between the offering party and the user in this case would be in real time, like telephone communications.

The main difference between contracting by telephone and via websites lies in how the parties express their will in relation to the content of the proposal. When contracting by telephone, the parties' will is expressed by voice transmission, whereas in transactions via websites such will is expressed through data transmission.

Thus, in theory, despite the discussions on the matter, the proposals made via websites may characterise a relationship between present parties, similar to proposals by telephone. Such assumption, however, is only valid for contracts made via a website, and does not cover proposals sent by e-mail.

E-Mail

In contracts effected by e-mail, both the sending and the acceptance of a proposal occur in different and successive moments, which differs from telephone communication or access to websites. It is very similar to contracting by letter. The time lag between the offer and the answer of the contracting parties does not permit such relation to be considered as a contract entered into between present parties, as set out in the Brazilian Civil Code.[26] For this reason, contracting by e-mail would, in principle, characterise a relationship between absent parties.

Right of Change of Mind

Under the Consumer Protection Code, consumers have the right to change their mind whenever the purchase is made outside the commercial establishment. The code does not specifically address cases of purchases through the Internet, but it has been generally accepted that this cooling-off rule prevails whenever the consumer buys products by telephone, catalog, letters and the Internet.

The right of change of mind period for consumers is seven days as from (i) execution of the agreement, or (ii) receipt of the product. The stand taken by legal scholars is that, should the product be delivered subsequently to execution of the agreement, the cooling-off period should run from actual delivery, that is, from the consumer's first contact with the purchased goods. Consumers need not justify why they changed their mind.

Means of Evidence

Notwithstanding the provisions of Provisional Measure 2200-2/01, one of the major challenges and setbacks for the parties to an electronic transaction refers to the production of proper means of evidence. It is still unclear whether digital files are comparable to documents. The lack of clear-cut legal definitions about what a document is has stirred up discussions in this specific area.

The features necessary to classify an electronic file as a document are still a controversy among legal scholars. Some of them have cast doubts over the evidentiary value of e-commerce contracts, on the argument that:

- such contracts do not bear the handwritten signature of the parties;
- the identity of the contracting party is uncertain (leading to grounded fears that a party may purport to be another in these contracts); and
- the integrity of their content is not assured if the parties did not use a specific technology system for this purpose, such as cryptography (an electronic contract may conceivably be unduly changed without leaving any trace of whoever has made such amendments).

In light of such difficulties, these scholars contend that the existence and extent of an electronic contract must be proven in court through technical expert investigation, in addition to the provision of documents that might be attached to the action.

Applicable Law

As the deals carried out on the Internet often involve several foreign individuals and companies, it is important to check the laws governing the parties' obligations.

> Under article 9 of the Law of Introduction to the Brazilian Civil Code, "the law of the country in which an obligation has been created shall determine and govern such obligation", and "the obligation ensuing from the contract shall be

  WILR ISSN 1468-4438

deemed created in the place of residence of the party to said contract".

There is no consensus among legal writers as to whether the provisions of the Law of Introduction to the Brazilian Civil Code are mandatory or would only serve to bridge any gap that may arise should the parties fail to elect the applicable law. The stand usually taken in this regard is that, in principle, the parties are free to choose the laws that will govern the respective contract.

Privacy

The Federal Constitution warrants every citizen the right to privacy.[27] As a result, everyone has the right to avoid third-party intrusion into his private or family life or to deny access to information on his private affairs.[28]

The Federal Constitution also protects the secrecy of correspondence, telegraphic communications, data and telephone communications.[29] Secrecy of data communications is an innovation brought by the 1988 Constitution.

The Brazilian Civil Code supports the constitutional principle that,

> "the privacy of a person is inviolable, and the courts will take the steps necessary to prevent or curtail any act running contrary to this rule, upon request of any interested party".[30]

Most Brazilian legal scholars argue that the protection accorded to privacy under the Brazilian Constitution and prevailing laws should also extend to the Internet.

Marketing of Products

Despite the comments above on the Brazilian laws and regulations on Internet transactions, there are indeed some legal restrictions or requirements on the sale or even the mere import of certain products, such as foodstuffs, cosmetics, chemicals, animals, and others.

These restrictions or requirements are not specific to sales made through the Internet, but rather to the nature of the products to be marketed in Brazil. Consequently, the applicability of specific legal provisions should be considered on a case-by-case basis.

Conclusion

In recent years, the Internet has revolutionised the way people interact and do business, having evolved into a primary means of communication and dissemination of information, data and knowledge.

The discussions about the validity, authenticity, safety, security and privacy of electronic transactions, or the need to lay down specific regulations for Internet use and access, are losing ground to more relevant issues focusing on the Internet access infrastructure or the telecommunications network for such access (particularly, mobile services).

Mobile services have a high penetration rate in Brazil, but their current stage of technological development (2.5G), coupled with the high tariffs charged by mobile operators for Internet access through their network, may stand as an obstacle to dissemination of m-commerce in Brazil.

Brazilian society is slowly but surely discovering the possibilities of Internet mobile systems for business. And time (more than technological resources or regulatory issues) will be instrumental in building a success story for Internet mobile access and m-commerce in Brazil.

1 *www.folha.uol.com.br* (September 10, 2003).

2 According to Barron's Dictionary of Computer and Internet Terms, 7th ed., New York, Barron's Educational Series, 2000, p. 223, a "host" stands for "a computer that provides services to others that are linked to it by a network; [...] For example, when a user in Florida accesses a computer in New York, the New York computer is considered the host".

3 Brazilian Internet Management Committee.

4 Brazilian Internet Management Committee at *www.cg.org.br/indicadores/brasil-mundo.htm*.

5 *http://registro.fapesp.br/estatísticas.html*.

6 Article 3(a) of Rule 4/95, approved by Ministry of Communications Ordinance 148/95.

7 Article 60. - Telecommunication services are the set of activities that allow for the offer of telecommunication. Paragraph 1 – Telecommunication stands for the incoming or outgoing transmission, by wire, radio electricity, optical media or any other electromagnetic process, of symbols, characters, signals, writings, images, sounds or information of any kind (...).

8 "Article 61. – Value-added service means the activity that adds, to a telecommunication service that supports it and with which it is not confused, new capabilities related to access, storage, presentation, movement or retrieval of information.

Paragraph 1. – A value-added service is not equated with a telecommunication service, and the provider thereof shall be labelled as a user of the telecommunication service supporting it, with all rights and duties inherent to such status.

Paragraph 2. – Interested parties shall be assured of the right to use the telecommunication service networks to provide value-added service. To ensure said right, ANATEL shall regulate the conditions and the relations between value-added service providers and the telecommunication incumbents."

9 Article 3(c) of Rule 4/95, approved by Ministry of Communications Ordinance 148/95.

10 "Mobile Cellular Service" is the land mobile telecommunications service open to public correspondence, using a radio communication system with cellular technology, interconnected to the public telecommunications network and accessed by terminals that are portable, transportable or carried by vehicles for individual use. (Ministry of Communications Ordinance No. 1533 of November 4, 1996, which approved Rule 20/96).

11 Article 4. – "Personal Communications Service" is the land mobile telecommunications service provided in the collective interest, which allows for communication between mobile stations and between mobile stations and others, with due regard for the provisions of this Regulation. Paragraph 1. – PCS enables communication between stations within one same PCS service area, or access to telecommunication networks in the collective interest. (...) (ANATEL Resolution No. 316 of September 27, 2002).

12 A holding company established by the Federal Government in 1972 (i) to control the telecommunication utility companies in Brazil, and (ii) to implement the federal government policy for modernisation and expansion of the Brazilian telecommunications system.

13 Análise Setorial, Telefonia Móvel, vol. 1, Coleção Panorama Setorial, Gazeta Mercantil, p. 53.

14 See footnote 13.

15 www.anatel.gov.br/tools/frame.asp?link=/bibilioteca/releases/2002/release_12_09_2003.pdf.

16 See footnote 15.

17 International Mobile Telecommunications for the Year 2000; Generation 3 Wireless Concept.

18 ANATEL Resolution 312/02.

19 Public Call for Tender under ANATEL Act No. 25260 of May 2, 2002.

20 *www.anatel.org.br. Tools/frame.asp?link=/biblioteca/releases/2003/release_12_09_2003.pdf*.

21 Source: ANATEL.

22 In general terms, it acknowledges the legal effects, validity or effectiveness of information in the form of an electronic message, and establishes the rules and directives for the storage and maintenance of such electronic messages. This bill was widely discussed by civil society and entities of the sector. It was viewed as the best legislative initiative on e-commerce.
23 Article 107 of Law 10406/02.
24 Article 427 of the Brazilian Civil Code.
25 Article 428, I of Law 10406/02.
26 According to the concept of article 428, I of Law 10406/02.
27 Article 5, X of the Federal Constitution.
28 C. R. Bastos, I. G. S. Martins, Comentários à Constituição do Brasil, II, 2nd edition, São Paulo, Saraiva, 2001, p. 71.
29 Article 5, XII of the Federal Constitution.
30 Article 21 of Law 10406/02.

Esther Donio Bellegarde Nunes is Chair of the Advisory Board of the Brazilian Informatics and Telecommunications Law Association and Vice-President of the Executive Committee of the Computer Law Association.

Germany: Standard Business Terms for E-Commerce

By Axel Freiherr von dem Bussche, a Partner and member of the Commercial Law and Information Technology Practice Groups at the Düsseldorf office of Taylor Wessing. The author may be contacted at a.bussche@taylorwessing.com

It is common practice for companies operating on a global level to implement their standard agreements wherever they do business. This is particularly important in the borderless world of E-commerce. However, applying foreign standard agreements under German jurisdiction is often difficult given the constraints of the German Standard Business Terms (SBT) law.

The following article will provide an overview of SBT, focusing specifically on SBT in the electronic business environment and the relevance for both B2C and B2B agreements. The most important preconditions and legal consequences of the German law on SBT are discussed here.

German SBT Law

SBT are used in order to facilitate the conclusion of agreements that are entered into on a regular basis with several clients. In the event that a businessperson is located in a foreign country, it is questionable whether the regime of German law applies to the respective SBT. According to article 29 of the Introductory Act to the German Civil Code (*Einführungsgesetz zum Bürgerlichen Gesetzbuch*, "EGBGB") German law on SBT prevails under two prerequisites:

- the contract is entered into by a consumer residing in Germany; and
- the standard of protection of the foreign law is less advantageous for the consumer.

The latter will most often be the case, since the German law is rather strict and favours consumers. In order to be on the safe side, it would, thus, be useful to warrant that the SBT meet with the requirements set out in section 305 ff. of the German Civil Code.

Even if the clients are not consumers, because all parties of the respective agreement are traders (B2B), the respective SBT have to comply with German law, albeit the limitations are less strict.

The main focus of this article will be on B2C agreements. However, a brief overview regarding specific conditions for B2B context is also given.

General Requirements for Application of SBT

Irrespective of the utilisation of standard business terms in regular written agreements or contracts in electronic form, personal as well as objective conditions have to be fulfilled to comply with the provisions laid down in section 305 ff. of the German Civil Code.

Application of SBT for B2C and B2B Agreements

Pursuant to section 305 ff. of the German Civil Code, the rules on SBT are directly applicable in case of business to consumer (B2C) agreements. A consumer is a person who enters into a contract for merely private purposes, which are under no circumstances related to the person's commercial or self-dependant activities. However, an employed person may be seen as a consumer in case he concludes an agreement for purposes related to his employment. B2B, on the other hand, is assumed in case the contracting party intends to enhance his commercial or self-dependant activities.

SBT or Individual Clause?

Additionally, two objective criteria have to be met for the contract clause to be governed by section 305 ff. of the German Civil Code. The German law on SBT applies, if:

- the contract clauses are used several times (at least three); and
- are used for agreements with different clients.

However, in case an individual agreement has been concluded, section 305 ff. of the German Civil Code will not apply. Individual contracts premise that:

- each clause has been (mutually) discussed; and
- that it was seriously at the party's disposal.

German law places considerable demands with respect to individual contracts. Therefore, in most of the cases where companies had implemented contract clauses more than once, German law was held applicable, even if some terms had been negotiated.

Due to the specific methods of e-commerce, especially in day-to-day business, it is normally the case that contractual conditions are not negotiated individually but set out by the company. Clients of e-commerce businesses as a general rule, do not have the possibility to influence those terms and conditions guiding the agreement. The aforesaid must therefore

  WILR ISSN 1468-4438

be given serious consideration. A standard contractual term provided on a company's homepage and/or e-commerce platform has to be regarded as SBT, since the clause will generally, be intended to apply to various different e-commerce orders. There are only very few exceptions in which a contract concluded via the Internet will be the result of considerable negotiation.

Effective Inclusion

In order to become applicable at all, SBT have to be incorporated effectively. In case SBT do not comply with these conditions, the respective clauses are void and will be replaced by the ordinary rules of the German Civil Code. The prerequisites to be fulfilled are:

- an explicit notice in proper form pointing out that respective SBT shall apply (section 305, para 2, no 1 of the German Civil Code);
- the contractual partner must have the reasonable possibility to perceive the content of the SBT (section 305, para 2, no 2 of the German Civil Code); and
- the contractual partner must consent to the validity of the SBT (section 305 para. 2 German Civil Code).

These general conditions also apply to general SBT placed on the Internet. But the use of SBT on electronic business platforms demands special requirements concerning the presentation of the relevant information.

Special Requirements for the Use of SBT in E-Commerce

SBT have to be presented in a way that the average person cannot ignore the information, even if reading the terms in the most cursory fashion. The notice has to be seen at a glance.

Thus, the process of purchasing goods and services via e-commerce shall be configured in a way that the order shall only be placed after the user:

- has accepted the SBT expressly by clicking a box online which refers to the SBT, *e.g.*, by a link (though it is not necessary to prove that the user has actually read the SBT); and
- was given the possibility to both download and print a copy of the SBT.

The requirement of an explicit notice is only fulfilled in case the connection between the electronic order and integrated SBT is evident and unquestionable for an average person. A possible wording of an effective notice may be:

> "I hereby order, in reference to the general standard business terms of the company, the following goods…".

The indication at the company's main homepage referring to SBT will not be sufficient, because this does not ensure a connection between the electronic order form and the relevant SBT. However, an additional link on the homepage to support the SBT notice on the e-commerce platform is helpful, because a user might like to know the relevant SBT before placing an order online.

Reasonable Possibility to Perceive SBT Content

In order for the client to become aware of the SBT, the indication or notice must be displayed in a prominent position on the company's website where it is clearly visible. The wording of the SBT itself does not have to be included on the electronic order form or respective website in full. However, a link must be provided to the page where the SBT are displayed in full and can be easily downloaded free of charge.

An average person must be able to comprehend the wording of the SBT without difficulty. Therefore, SBT have to be concise, as well as clearly structured.

The recommended or ideal extent of SBT is disputed. As a general rule, the length of the SBT should be appropriate to the nature of the respective e-business. In case of day-to-day businesses, SBT have to be rather short and readable in the minimum time. In case of a more complex business transaction, the SBT would be increasingly detailed. The more complex the SBT, the more important it is to make a free download of the SBT available to the client.

The Internet is multi-lingual; the client generally, is not. Nonetheless, a business person may assume that the client is capable of the language in which the e-commerce platform is verbalised. If the client is able to place an order in a different idiom, he is presumed to be able to comprehend the SBT in that tongue. Nonetheless, SBT should, as a general rule, be:

- written in a popular and established language;
- furthermore, according to the so-called Regulation of Information Duties (*Verordnung über Informationspflichten nach bürgerlichen Recht*), the company has to inform the client about the languages provided for the conclusion of the contract.

Consent of the User

For the SBT to become part of the agreement, the user's direct consent must be obtained. In case the company has provided for the above mentioned preconditions, the user agrees to the SBT when sending the electronic order form to the respective company. Thus, it is advisable to provide a separate button at the e-commerce order platform, which must be clicked by the user before submitting the respective order. The button should inform the client that he gives his consent to the SBT by clicking a box online (*e.g.*, the user ticks a box in a pop-up window with a link to the downloadable and printable SBT).

Legal Consequences

The SBT, by compliance with the three aforementioned requirements, become part of the agreement between the parties. This is the first step. The subsequent step, once the SBT are part of the agreement, is to examine whether or not the content of the respective contractual clauses comply with the strict regime of German law on SBT. This is usually the most frustrating part for foreign companies doing business in Germany, whether this is e-commerce or other types of business.

Validity of the SBT Content

Contracting parties are, as a general rule, free to negotiate contractual obligations. SBT, however, are neither discussed nor negotiated. Hence, a high standard of consumer protection is implemented by section 307 ff. of the German Civil Code. The presentation of SBT in either traditional written form or in the context of e-commerce is not relevant for the legitimacy as regards the textual substance.

Prohibitions concerning the content of SBT are partly outlined by statutory law and partly established by case law. The content of SBT is assumed admissible, in case the SBT withhold the provisions laid down in sections 307, 308 and 309 of the German Civil Code. The latter outlines specific prohibited clauses such as:

- terms that award unreasonable respites concerning the accomplishment of the user's duties;
- clauses that confer the possibility of recession from the contract without objectively justifiable reason to the user of SBT;
- terms rewarding unreasonably high compensation for the user of SBT in case of recession of the client;
- the exclusion or limitation of liability in case of personal and bodily harm; and
- the exclusion or limitation of liability in case of intent or gross negligence.

Section 307 of the German Civil Code sets out general prohibitions that implicate the invalidity of SBT in case of breach. Instances in which standard business terms are inadmissible due to section 307 are:

- They are surprising or ambiguous and do not comply with the principle of transparency. Clauses in contracts which in the circumstances are so unusual that the client of the businessperson could not be expected to have reckoned with them, do not form part of the agreement. The client may have the confidence in standard business terms to only include provisions usually provided for in contracts of the specific kind.
- Stipulations in SBT are invalid, if they place the client of the businessperson at an unreasonable disadvantage. An unreasonable disadvantage is assumed, if a condition cannot be reconciled with crucial basic principles of the statutory rule from which it derivates. A clause is inadmissible, in case essential rights or duties resulting from the nature of the contract are restricted in such a way that the purpose of the contract is in the risk of not being achievable. The unreasonable disadvantage for the client may also result from the fact that the condition is not clear and comprehensible.

In case of doubt, standard business terms are interpreted against the user. The point of view of an average third person is relevant, not the opinion of the contracting parties. Hence, the wording is important.

Recommendations for Use

If all or some standard business terms have not become part of the contract, or are invalid for breach of legal provisions, the remainder of the agreement prevails. Additionally, the contract is determined by statutory rules where the void clauses no longer guide the rights and duties of the parties.

Initially, contractual clauses have to be examined with respect to individuality and negotiation or standard utilisation. Secondly, in case of SBT, there are three options:

- Review of every clause and sentence of the SBT pursuant to the applicable German law. This would be time consuming and requires a translation into German.
- Redrafting the SBT at the outset, pursuant to section 305 ff. of the German Civil Code.

Companies using SBT may also take the risk that clauses may be void and will be replaced in case of legal disputes by German statutes, as well as case law. This option is particularly dangerous if the contracting partner is aware of the circumstances outlined above. The other party might be aware that a contract clause is void due to breach of German SBT law and consequently, such party might appear to accept a particular clause, but is aware that in case of a conflict the void clause will be replaced by less strict German Civil law.

SBT and B2B

German law on SBT may also apply in a B2B context, pursuant to section 310 para. 1 of the German Civil Code. The application of the rules concerning SBT is, as yet, limited:

- SBT that apply for B2B do not have to comply with the requirements of section 305 para. 2 of the German Civil Code. An explicit notice, the reasonable possibility of comprehension as well as the expressed consent of the business client is not required. Any implied approval of the business client is sufficient for an effective incorporation of the SBT. A businessperson is presumed less in need of protection than a consumer due to his experience in the economic environment. A contracting businessperson must reckon the utilisation of SBT and perceive the content of the relevant SBT, even if the user of SBT has not explicitly brought this to the client's attention as it is required – and outlined above – for B2C relations.
- Generally, the specific prohibitions of standard clauses due to section 308 and 309 of the German Civil Code do not apply in the B2B context. The content of SBT in B2B cases has only to hold out against the provisions of section 307 of the German Civil Code. Hence, a standard contractual term is presumed invalid, if the contracting business partner suffers "unreasonable disadvantages" from the application of the SBT in question.

Jurisdiction will take into account the commercial custom and the habit of the specific business when deciding whether a disputed SBT is to be held permissible or not.

Electronic Invoicing in Central Europe

By Zbynìk Loebl, Head of the E-Economy Practice Group, Central European Advisory Group (www.ceag.biz), in co-operation with Dr. Tamás Gödölle, Attorney at Law at Bogsch & Partners Law Firm (www.bogsch-partners.hu) and Tomáš Rybár, an associate with the Èechová Rakovský Law Firm, Slovak Republic.

Electronic invoicing establishes a basis for innovative business models in B2B e-commerce services. In this brief commentary, we will outline the legal environment for electronic invoicing in the Czech Republic, Hungary and Slovakia.

On the eve of accession to the European Union, these countries have incorporated into their national legislation, E.U. Directives dealing with electronic invoicing as it relates to electronic signatures (Directive No.1999/93/EC), data protection (Directive No. 2002/58/EC), and regulations on VAT (Directive No. 2001/115). The recent E.U. Invoicing and VAT Directive must be implemented within the national laws for each E.U. Member State by January 1, 2004. From this date, invoices sent by electronic means would be valid documents in all EU Member States. Accession States, having generally implemented the rules established by the Directive, have proven their readiness to keep pace with the developments in e-commerce in Europe.

All of the Accession States mentioned above allow accounting and tax documents (including invoices) to be generated, maintained, and archived in electronic form, provided that the requisite technical and security measures are guaranteed, ensuring the authenticity of the document and its origin, as well as protecting the integrity of the data it contains. With electronic tax documents, the burden of proof regarding their authenticity and integrity must be borne by the tax payer who issued the tax document in electronic form.

These requisite security measures bridge electronic invoicing with the more general issue of electronic signatures as a means of electronic identification. This connection is seen in the direct or indirect references made to "advanced electronic signatures" and related measures as defined by the EC Electronic Signatures Directive within the national electronic signature laws of Central European countries. For example, Hungarian accounting legislation specifically allows tax documents in electronic form if these documents can be regarded as "certified electronic documents" as defined by Hungarian law on electronic signatures (i.e., advance electronic signatures, time stamping, *etc*.). When regulating electronic tax documents, Czech VAT legislation specifically cites the Czech law on electronic signatures; however, it does not contain an explicit requirement to use advanced electronic signatures. Nevertheless, parties wishing to exchange electronic invoices in the Czech Republic will probably use advanced electronic signatures verified by qualified certificates and created by a secure-signature-creation device, so that they can rely on statutory assumptions contained in the Czech law on electronic signatures relating to the authenticity and originality of the document.

Official accounting and tax documents may also be stored by electronic means, provided that the method ensures that all the data of the original document can be reproduced without delay, it can be read at any time, and that there is no possibility of its subsequent modification. In addition, national laws of the Czech Republic, Hungary and Slovakia enable the conversion of written tax documents into electronic ones, provided that the above-mentioned requirements are fulfilled.

Nonetheless, in the Czech Republic Hungary and Slovakia, there is no regulation expressly targeting electronic invoices using the EDI standard. This means that EDI has a somewhat "discriminated" status. As a result, the Czech Republic is currently amending its laws on electronic signatures to provide for "qualified server certificates," something similar to qualified certificates but in the context of server-to-server communications. In addition, laws on VAT are being changed to support the use of tax documents in a secure EDI format.

Filing one's taxes by electronic means is interconnected with the issue of electronic invoicing. Although current legislation in all of the above-mentioned Accession States enables taxes to be filed electronically, the actual application of legal provisions has only just begun, and in practice, it is not commonplace. Nevertheless, national administrations tend to see electronic tax filing as one of the important aspects of the "information society", and therefore, visible progress has been made in its implementation in each of the Accession States.

In Hungary the recently adopted new act on tax proceedings prescribe to certain corporate taxpayers that they must file their tax returns and data using electronic means. As of January 1, 2005, any taxpayer may submit his/her/its tax return electronically, provided that certain procedures and methods are observed.

In Slovakia, the actual application has been delayed by a complex overhaul of the taxation system with effect from January 1, due to the introduction of a flat income tax rate and amendments of most of the tax laws, however it is expected to accelerate throughout 2004. The tax authorities are being technically equipped to facilitate the application of new legislation.

While EDI continues to grow, economic forecasts state that in the near future it will be eclipsed by the Internet in the B2B setting. Rapid technological developments urge national governments, as well as international and regional organisations, to spur the development of the legal infrastructure allowing innovative practical approaches to e-commerce, its reliability and predictability. These developments are being actively pursued by the Accession States.

The Electronic Filing and Payment System in The Philippines: A Paperless Experience

By Dennis G. Dimagiba, Shennan A. Sy and Saben C. Loyola of Quisumbing Torres Law Offices (an associate firm of Baker & McKenzie), Manila, Philippines.
The authors may be contacted as follows: dennis.dimagiba@bakernet.com, tel. (632) 819 4912; shennan.sy@bakernet.com, tel. (632) 819 4954; and saben.loyola@bakernet.com, tel. (632) 819 4938.

The Bureau of Internal Revenue ("BIR") has introduced a modern system of filing tax returns and paying taxes through the Electronic Filing and Payment System ("EFPS"). Thus, the age of hassle-free payment of taxes has begun. The EFPS "refers to the system developed and maintained by the BIR for electronically filing tax returns, including attachments, if any, and electronically paying taxes through the Internet".[1] Accordingly, taxpayers need not physically go to the BIR or to Authorised Agent Banks to file returns or pay their taxes. All that is needed by the taxpayer is to have a computer, an e-mail account, and Internet access.

Initially, 1,369 Large Taxpayers and 226 Volunteer Non-Large Taxpayers and BIR National Office Employees were using the EFPS. On December 2003, the EFPS was also made available to the top 1,000 taxpayers in the 40 computerised Revenue District Offices throughout the Philippines. As of late, the number of qualified taxpayers who avail of the EFPS is growing. Thus, the BIR has reason to be optimistic that ten percent of the total tax paying population will make use of the EFPS by the end of 2004.

Availability of the EFPS to Specific Taxpayers

The EFPS is presently available only to the following taxpayers:

- Large Taxpayers;
- Non-Large Taxpayers as identified by the BIR; and,
- BIR National Office Employees.

A Large Taxpayer is defined as one who has been classified as such and duly notified by the Commissioner of Internal Revenue (CIR) as having satisfied any or a combination of set criteria for classification as a large taxpayer. Large Taxpayers have been required to use the EFPS as of August 1, 2002. Thus, in the case of Large Taxpayers, only tax returns that are not covered by the EFPS can be filed manually.

For Non-Large Taxpayers and BIR National Office Employees, the use of the EFPS is on a purely voluntary basis. To encourage the use of EFPS, the BIR has extended the due dates for filing tax returns via EFPS to generally five days later than the deadlines for filing tax returns under the manual system. This incentive, however, does not apply where the deadline for filing the return is fixed by law. In which case the deadlines as fixed by law must be complied with at all times.

To avail of the benefits of the EFPS, a person must first register with the BIR Integrated Tax System. Then the taxpayer should enroll with the EFPS through the BIR website (*www.BIR.gov.ph.*). After going through the required procedure online, the taxpayer will receive an e-mail advising on the status of his application for enrolment in the EFPS. Once the taxpayer's application is approved and his account is activated, he is ready to use the EFPS. If the taxpayer intends to pay his taxes via EFPS, he must first enroll with an Authorised Agent Bank (AAB). It is only with the intervention of an AAB that a taxpayer can pay his taxes via EFPS.

24-Hour "Round the Clock" EFPS Services

Qualified taxpayers can take advantage of the 24-hour network services of the EFPS. The time for filing of returns is no longer limited by the BIR's office hours. Even beyond the normal office hours, a taxpayer may file his return through EFPS. However, the payment of taxes through EFPS is subject to the internal rules of AABs. Each bank has its own cut-off time. By agreement with the BIR, this cut-of time is generally fixed later than the usual banking hours. Some banks have a cut-off time of 8:00 p.m. while others have set theirs as late as 11:00 p.m. With these breakthroughs, taxpayers are encouraged to pay the proper taxes through the EFPS because of the convenience that goes with it.

Among the services provided by the EFPS on a 24-hour basis is the Help Desk for Taxpayers. Through the Help Desk, the BIR may attend to taxpayer's queries/issues regarding the EFPS. Taxpayers are also advised of the system's unavailability through the Help Desk.

Electronic Filing ("E-Filing")

The filing of returns through the EFPS is available 24 hours a day for seven days a week. But to ensure that returns are filed on the due date as set by law, returns are required to be filed before 10:00 p.m. of the due date. The return is deemed filed on the date appearing in, and after a Filing Reference Number is generated and issued to the taxpayer via the EFPS.

With the initial implementation of the EFPS, 13 tax forms can be filed through the BIR website. The BIR is now enhancing the EFPS by increasing the number of tax forms that may be filed electronically from 13 to 27 tax forms. At present, the following tax return forms can be filed through the EFPS:

- Monthly Remittance Return of Income Taxes Withheld on Compensation.
- Monthly Remittance Return of Creditable Income Taxes Withheld (Expanded).
- Remittance Return of Final Income Taxes Withheld.
- Quarterly Remittance Return of Final Income Taxes Withheld on Fringe.
- Benefits Paid to Employees other than Rank and File.
- Annual Income Tax Return for Individuals Earning Purely Compensation Income.
- Annual Income Tax Return for Corporations and Partnerships.
- Quarterly Income Tax Return for Corporations and Partnerships.
- Excise Tax Return for Alcohol Products.
- Excise Tax Return for Petroleum Products.
- Excise Tax Return for Tobacco Products.
- Monthly Value Added Tax Declaration.
- Quarterly Value Added Tax Return.

- Percentage Tax Return (Quarterly).

Electronic Payment ("E-Payment")

E-Payment can be availed of only through the intervention of EFPS Authorised Agent Banks (AABs). Before a bank may be authorised to receive payments through the EFPS it must pass the BIR accreditation criteria. The chief consideration being that the AAB must be an Internet-ready bank. Then the AAB must be indorsed by the Bureau of Treasury for EFPS accreditation and certified by the Information Systems group of the BIR that the applicant bank's system is acceptable and compatible with the EFPS of the BIR.

The tax due is deemed paid after a Confirmation Number is issued to the taxpayer and to the BIR by the AAB. An Acknowledgment Number shall be issued by the AAB to the BIR to confirm that the tax payment has been credited to the account of the government or recognized as revenue by the Bureau of Treasury. Pursuant to the "pay- as-you-file" principle adhered to by the BIR, taxes are to be paid the moment the tax return is filed. Nevertheless, even if the tax return was filed ahead of the payment of the tax due, the "pay-as-you- file" principle is deemed not violated as long as the payment of the tax is made on or before the due date of the applicable tax.

Security of EFPS Transactions and Availability of Returns

Taxpayers who avail of EFPS need not worry about the security of their electronic transactions since security features are embedded in the EFPS. The transmission of data on every transaction is encrypted and secured by the state-of-the-art technology provided by SSL (Secure Sockets Layer), which is the industry-standard protocol for secure web-based communications, and VERISIGN. Likewise, user validation or authentication is handled by the system's enrolment and log on facility, which has two levels of security – user name/password and challenge question.

In addition, the taxpayer can have access to the tax return electronically filed by him via the EFPS for a period of two months from the filing thereof. After this period, a taxpayer may secure a certification from the BIR containing the information supplied by him in the return, which he filed via EFPS.

EFPS Provides Boost to Government Tax Collection

The EFPS will inevitably boost government tax collection. The convenience and availability of the EFPS will provide taxpayers less reason to be delinquent in paying taxes. The EFPS serves as an open invitation to taxpayers to settle their tax liabilities promptly. The BIR hopes that taxpayers will soon find this invitation hard to turn down. However, this may depend largely on the investments of the BIR on systems technology that makes the EFPS user-friendly, convenient and secure. The efforts of the BIR in increasing the availability of the EFPS give taxpayers a sign of things to come. The EFPS serves as an indication that the BIR is keen on enhancing tax collection through modern means.

On the government's part, the adoption of the EFPS is a cost-effective means of tax administration since the processing costs for returns and payments will inevitably be reduced. AABs will also benefit from the EFPS as volume of business transactions with banks for e-payment of taxes will definitely rise. This may explain the growing list of AABs accredited by the BIR.

The EFPS, without doubt, paints a bright future for tax administration in the Philippines. In the words of the Commissioner of Internal Revenue, Guillermo Parayno, Jr., "The EFPS is a win-win situation not only for the BIR, but for taxpayers and banks".[2]

1 Section 2.1 Revenue Regulations No. 9-01 dated August 3, 2001.

2 BIR Monitor Volume 5 No. 11, page 1.

News

MEXICO

Introduction of E-Signatures and Digital Tax Invoices for Tax Purposes

Steps to introduce electronic tax invoices (known as "Comprobantes Fiscales Digitales") began in Mexico over three years ago. During the LVIII legislative session, the Mexican Federal Tax Authority (Servicio de Administracion Tributaria, "SAT") proposed a set of rules in 2000 to amend the Fiscal Code of the Federation (Codigo Fiscal de la Federacion) and allow for the use of electronic tax invoices. These amendments were passed by the Senate on December 17, 2003 through a "Dictamen" recommending amendments to various provisions to the Fiscal Code of the Federation.

Finally, on January 5, 2004, *"SAT"* published a Decree in the *Diario Oficial* that amends the Fiscal Code of the Federation. The Decree incorporates a new section, entitled "On Electronic Means" and incorporates new articles 17-D, 17-E, 17-F, 17-G, 17-H, 17I, and 17J to the Fiscal Code of the Federation.

The said proposal seeks to regulate the use of advanced digital signatures and certificates by using the PKI of Mexico's Central Banking Authority. The amendments:

- establish the functional equivalence of digital signatures in relation to written signatures contained in digital certificates;
- provide electronic signatures with functional equivalence, legal evidence and authentication levels in relation to written signatures contained in printed documents;
- provide the term of digital certificates and rules for its revocation and cancellation;
- set out the rights and obligations of the signatories;
- provide for acknowledgement of receipt of digital documents and the corresponding legal presumption;
- guarantee the authenticity of digital seals issued by SAT;
- provide the registry of identity elements with electronic identification mediums used by the signatories and the information to authenticate advanced electronic signatures and certificates;
- list the criteria and rules for Certification Service Providers authorised by Banco de Mexico; and
- provide the exclusion to use advanced electronic signatures for tax payers involved in agricultural, cattle and fishing activities.

Some of the advantages that the utilisation of *Comprobantes Fiscales Digitales* would bring are:

- they could facilitate the payment of federal taxes and improve the relation between the authority with the private sector and natural persons; and
- they would diminish the use of paper and improve the tax federal administrative system, which continues to have tremendous technical flaws.

One of the challenges of SAT under this reform is to make its technical infrastructure compatible not only with internationally accepted standards but also with the private sector's infrastructure. The latter will shortly be rendering certification services for electronic commercial transactions.

By Cristos Velasco, Professor of Internet and e-commerce law at the Postgraduate Unit of Instituto Tecnologico Autonomo de Mexico (ITAM); e-mail: cristosuofa@yahoo.com.

Intellectual Property

Spain: Copyright Implications of the Amended Criminal Code

By Clara Bordoy Mateo, a lawyer in the copyright department of Abril Abogados, Madrid.

Organic Act 15/2003, of November 25, amending Criminal Code Organic Act 10/1995 of November 23, was published in the Spanish Official State Gazette on November 26, 2003.

Along with substantial changes to the General Part of the Act (which affects the penalties system and its application) changes have been made in the Special Part of the Act to introduce new types of criminal offences which update copyright protection law to make it more suitable for application in dealing with present-day crime (for example, cybercrime).

The details of the amendment will be discussed later in this article though by and large, penalties are augmented for copyright offences, the wording of which in the legislation has been amended to better apply to social and crime-fighting needs.

Accordingly, the affected party need no longer first make a complaint in order for action to be taken in such offences, which shall henceforth be actionable *ex officio*, and the Spanish police will therefore be able to take action against the illegal trading of goods which infringe copyright.

The common interest in fighting piracy and online crime resulted in the Criminal Procedure Act being amended before the Criminal Code. A new fast trials procedure was set up under article 282, providing for entry of a judgment into law within 72 hours in the case of a misdemeanour, or within 15 days in the case of an offence, in connection with certain criminal acts, *inter alia* that of violating intellectual property rights.

A measure which will clearly boost the fight against piracy is the amendment of article 127 of the Criminal Code, providing for the seizure of assets not subject to litigation equivalent in value to the value of assets that are subject to litigation. Provision is also made for the possibility of the Judge ordering the seizure of assets even where there is no criminal liability or such has lapsed when there is definite proof as to the unlawful ownership of assets.

Chapter XI, "Intellectual property, market and consumer related offences", and specifically section one, "Copyright related offences" and section four "Common provisions of the preceding Sections" have been amended as follows:

- The basic offence of article 270 of the Criminal Code still refers to engaging in acts of reproduction, plagiarism, distribution, *etc*., for a profit and to the detriment of another, albeit with an improved technical-legal wording, but the penalty has been increased. Offences will now be punishable with imprisonment of six months to two years and a fine of 12 to 24 months in lieu of six to 24 months.
- An amendment to article 271 of the Criminal Code which deals with aggravated offence means that the following are now considered:
  - the use of minors (under-18s) for committing these offences; and
  - membership of a criminal organisation, however brief.
- The penalty consisting of a fine, provided for in this same article, is also augmented, and now consists of imprisonment of one to four years, a fine of 12 to 24 months in lieu of eight to 24 months and a special disqualification for practising the profession related to the offence committed.
- As mentioned above, the requirement for the aggrieved party to first make a complaint in order for an intellectual property offence to be actionable, is no longer a stipulation. Such requirement will only remain under article 287 for section 3 offences, namely "Market and consumer related offences".

This amendment by an Organic Act has also affected provisions of the Criminal Procedure Act, and intellectual property offences perpetrated by three or more individuals shall henceforth be considered organised crime for the relevant purposes.

All changes resulting from the amendment discussed herein however, will not enter into force until October 1, 2004. The exception to this is amended paragraph 4 of article 282bis of the Criminal Procedure Act, which has been in force since November 27, 2003.

In spite of the delayed application of the changes for which provision is made in this Amendment, the effectiveness those changes seek to achieve will put an end, *inter alia*, to piracy and the mafia hiding behind it.

Patents and the Internet

By Glyn Morgan, a Partner in the information technology and electronic communications group of Taylor Wessing, London. The author may be contacted at g.morgan@taylorwessing.com

Increasing numbers of patents are being obtained, particularly in the United States, that cover the way in which the Internet is used to transmit video and audio files. This article considers (from the perspective of English law) the extent to which patents such as these may threaten to have an adverse effect on Internet use.

For example, in the U.S., there is a specific patent which covers the selling of digital copies of video or music files and the resulting transfer of the files from one computer to another. In addition to this example, there are an increasing number of patents that have been granted which appear to cover (at least to an extent) general methods of doing business over the Internet and that are used by the majority of Internet users. Some of these patents, at least, may not appear to the lay person to contain any great technical advance or insight, but seem to cover very general methods of using the Internet that have been in use by many for some time.

Common Concerns Surrounding Internet Patents

Some of the concerns that have been raised about the type of patent referred to above are as follows:

- Patents like these may have the potential to affect a material proportion of the people using the Internet. For example, businesses that use the Internet to sell and supply products and services to their customers may find that, in order to carry on doing so, they have to pay a royalty to one or more patent owners. They may even be prevented from continuing to trade online.
- There is the possibility that large numbers of businesses that use the Internet may find themselves subject to court actions for patent infringement. These are likely to cost a lot to defend, even if the defence is ultimately successful.
- Businesses that supply the infrastructure (for example, client-server systems) to enable other businesses to supply their customers over the Internet may find that patent owners target them *and* their customers with claims of patent infringement. This may result in their customers asking for an indemnity against the costs and liability involved in the patent infringement claims. This, in turn, will increase the risk of supplying this type of infrastructure which may increase its cost and may remove it from the market altogether.
- If too many people try to profit by staking out patent rights over commonly used processes employed when using the Internet, it may result in the use and growth of the Internet being significantly curtailed.

Obtaining Patents

In order for it to be possible to protect an invention with a patent:

- The invention must be new. This means that the same (or a substantially similar) invention must not have been available to the public anywhere in the world before the patent for the invention is applied for.
- The invention must not be obvious. This means that, taking account of what was available to the public before the patent was applied for, the invention covered by the patent would not have been obvious to someone who was reasonably skilled and knowledgeable in the field to which the patent relates.
- The invention must be capable of being applied industrially, *i.e.*, it is possible to use the invention to produce or supply something.
- There are some things that by law, a patent cannot be obtained for. In Europe for example, it is not possible to obtain a patent for a method of doing business.

Once a patent has been granted, if it can be shown that the invention covered by the patent did not fulfil the above criteria, the patent will be invalid and will be revoked (and will be treated as if it had never existed). As a result, if a patent owner sues for infringement, the person being sued will usually try and win the case by proving that the patent is invalid.

Patents are national rights. That is, a patent is granted to cover a given country, like the United States or the United Kingdom (although it will shortly be possible to get a patent that covers the entire European Union). In order to infringe a patent, it is necessary to do something covered by the patent in the country to which the patent relates. For example, it is not usually possible to infringe a U.S. patent by doing something in the United Kingdom (although the use of the Internet complicates this somewhat and makes application of this rule more difficult).

A patent has to describe the invention it covers. This description is set out in a series of claims. Parties risk infringing the patent by doing anything which falls within the description of any of the claims in a patent, unless they have permission of the patent owner to do so.

A patent effectively lasts for up to 20 years from the date it was applied for (some patents for drugs can last longer). The owner must remember to renew the patent at regular intervals during that time (for which a fee is payable).

You do not have to know about the existence of a patent, or what it covers, in order for you to infringe it.

It usually takes from 18 months to a few years for a patent to be granted, from the time of application to the patent being granted. For at least the first 18 months of that time, the patent application is not published and is not available. Accordingly, pending applications will not show up in a search of granted patents.

U.S. Patent 5,191,573

An example of a patent that might apply to many Internet users is given by U.S. Patent 5,191,573. This patent was applied for in September 1990 and was granted in March 1993. Quoting the patent, its main claim covers the following:

"A method for transmitting a desired digital audio signal stored on a first memory of a first party to a second memory of a second party comprising the steps of:

- transferring money electronically via a telecommunication line to the first party at a location remote from the second memory and controlling use of the first memory from the second party financially distinct from the first party, said second party controlling use and in possession of the second memory;

- connecting electronically via a telecommunications line the first memory with the second memory such that the desired digital audio signal can pass there between;

- transmitting the desired digital audio signal from the first memory with a transmitter in control and possession of the first party to a receiver having the second memory at a location determined by the second party, said receiver in possession and control of the second party; and

- storing the digital signal in the second memory."

So, in essence, the primary claim of the patent involves:

- one computer with digital audio stored on it connected to another, remote, computer (for example, via the Internet);
- a transfer of money for the sale of digital audio files carried out electronically (for example, via the Internet); and
- the subsequent electronic transfer of the relevant files from the first computer to the second.

This is a fairly broad description might fit a lot of people doing business over the Internet today, given that audio file transfer is relatively widespread. To make matters more complicated, there is a later, related patent that covers the transfer of both audio and video files.

Status of Patent 5,191,573 and Future Implications

The company that owns this patent has received permission from a U.S. District Court to proceed with a patent infringement action in the United States against two companies. If that action were to be successful, then this would potentially require the defendant companies to pay damages to the claimant for past infringement of the patent, and to pay royalties for future use. Anyone else held to be infringing the patent would be in the same position.

It is too early to say whether this particular patent will be successfully enforced and will survive any challenge to its validity. Obviously, the patent owner believes that the patent is valid and is being infringed. If, however, the patent is held to be invalid, then that would mean that no-one would be in danger of infringing it. Conversely, if the court action succeeds then it is likely that the owner of the patent will be looking for royalties from others.

Overall, this seems to be one part of a wider trend for patent owners to try and assert patents that cover fairly general aspects of doing business online. Similar attempts to assert patents have been, or are being made, in relation to practices such as linking and framing, compression of visual images and encryption.

Patent Systems Outside the United States

Broadly speaking, the patent systems in the United States and Europe have many similarities. However, they also have a few differences and as a general principle historically, it has been easier for a patent of the type described above to be obtained in the United States, as opposed (for example) to the United Kingdom or other countries in Europe.

However, even if a business is not based in the United States (and its server is not sited there), if the company is doing business with customers in the United States via the Internet, there may still be a possibility of it being affected by U.S. patents of this nature (although any infringement action would have to be brought in the United States). Also, of course, much of the world's Internet-based business is located in, is connected with, or transits through the United States.

Consequences of Net Patents

It is difficult to say at this stage how serious the consequences would be of this type of patent becoming more widespread and being successfully asserted so as to obtain royalties or damages.

The Internet community has attacked many patents of this type that the patent owners have tried to assert as covering old technology or not being relevant to the Internet. One example was a U.S. patent that communications service provider, British Telecom tried to enforce. BT alleged that the patent concerned covered linking on the Web (the patent related to technology originally developed for the Prestel service in the 1980s). A court case brought in New York by BT to try and enforce the patent foundered amidst suggestions that it did not in fact cover linking on the Web.

Other patents (for example, one that has been alleged to cover the use of JPEG compression technology) have inspired communities on the Internet to band together to try to show that the technology covered by the patent was known before the patent was applied for (which, if correct, would make the patent invalid).

Some companies faced with an allegation of patent infringement have simply paid up in order to buy off the patent owner with a licence fee. It is this possibility that may be encouraging the use of this type of patent to try and obtain revenue from other peoples' business transactions on the Internet.

Action: Protection for Business

Businesses will need to take different types of action to resolve patent issues depending on how they are affected.

Companies are quite likely to be at somewhat greater risk of being affected by this type of patent if they do business in the United States (which includes doing business with customers in the United States, even if the company is not based there itself). This may be because companies do business via the Internet or some other form of electronic communication or because they supply the equipment to allow others to do so. Having said that, the United States is not the only place where this type of patent can be obtained and there are an increasing number of patents covering aspects of processes used over the Internet that are being granted (for example) in Europe.

The increasingly high profile of this kind of patent may have a number of effects:

- Companies may receive demands from patent owners for royalties or damages. The best course of action open to the company will depend on a variety of factors including: the scope of the patent; the extent to which it is open to challenge; whether the patent has been successfully enforced in any court cases; whether other people are paying royalties; the potential costs of fighting the claim; and the potential effect on customers.
- Customers may be concerned about the possibility of a claim against them. As a result, a company may be asked to give customers an indemnity against anything it supplies to them, which may infringe any third party intellectual property rights (including patents). Companies may risk losing customers if they fail to meet any such demand on the customer's behalf. Depending on a company's particular circumstances, it may (or may not) place the company in a worse position to indemnify its customers against claims than if the claims are made directly against the company by the patent owner. However, if a company regularly gives indemnities of this type, it might consider (for example), trying to reduce the risk by (for example) saying that the indemnity does not apply to infringement claims based on U.S. patents.
- For customers, it has become increasingly important to make sure that an appropriate indemnity is in place in contracts with suppliers, so as to ensure that suppliers are responsible for meeting the costs of any intellectual property rights infringement claims.

Depending on the nature of a business and its particular circumstances, it is sometimes possible to insure against the risk of patent (or other intellectual property rights) claims being made.

Companies should consider whether a patent of a similar nature to the one described would be likely to cover something they do, or are involved in. The scope for patent infringement is wide and it is useful to remember that this extends to matters such as contracts with customers and suppliers.

Case Reports

BELGIUM

State Wins "www.belgie.be" Domain Name Dispute

Belgische Staat v. Domain Services Rotterdam BV [CEPINA case n° 44040]

Centre for Arbitration and Mediation, December 11, 2003

On December 11, 2003 a third party decider appointed by the Belgian Centre for Arbitration and Mediation (CEPANI) had to decide on the rightfulness of a licensee's claim on the domain name "www.belgie.be" (referring to the denomination of Belgium in Dutch). This domain name had previously been registered by the Dutch company "Domain Services Rotterdam B.V." (a provider of various commercial websites) following the liberalisation of the domain name registration procedure which took effect from December 12, 2000. Prior amicable negotiations with the Belgian State about a possible sale of the domain name had taken more than two and half years, but these remained unfruitful. In light thereof, the Belgian State filed a complaint with CEPANI on October 9, 2003 whereby a third party decider was appointed to resolve the domain name conflict.

In its decision, the third party decider found that there did not exist any natural link between the Dutch company and the domain name, since this company was not involved in any activity linked to Belgium as a geographical or political entity and since the underlying website did not offer any information or warning relating to Belgium. It was found that such use of the domain name is confusing and contrary to the legitimate expectations of the general public. Thereby the legitimate interests and rights of the Belgian State as the natural and logical rightholder prevail over the "first come, first serve" registration principle. According to the third party decider, this reasoning even applies when at the actual time of registration those interests and rights were not yet explicitly protected in any domain name registration rules or in any statutory provision.

Moreover, the third party decider found that the domain name registration and its subsequent use clearly took place in bad faith since it was obvious that:

- the Dutch company knew or reasonably had to know that the domain name constituted an "essential facility" between the political-geographical institutions and the Belgian citizens, especially in the framework of the further development of e-government;
- visitors to the underlying website were captured and referred via hyperlinks to other commercial websites without being offered any information on the Belgian State;
- the main purpose of the Dutch company was to sell the domain name in consideration for a transfer.

Subsequently, the third party decider ordered the immediate transfer of the abusively registered domain name to the Belgian State.

This decision is the first CEPANI ruling on a geographical domain name and it is in line with the principles as set forth in the Belgian Act of June 26, 2003 against abusive registration of domain names, which entered into force in September 2003.

This Act protects amongst others: brand names; geographical indications; commercial denominations; geographical entities; and denominations of associations or patronymics from abusive domain name registration.

Complementary to the CEPANI third party domain name resolution procedure laid down in the existing general terms and conditions of the Belgian domain name registration authority DNS, this Act also grants a specific jurisdiction to the Presidents of the ordinary courts to hear such cases, according to the rules of summary proceedings, provided the domain name in question is a ".be" domain name or has been registered by a person established in Belgium. This Act can thus also apply to any physical or legal person domiciled or having its company seat in Belgium, who abusively registers a domain name under any generic (.com; .biz; *etc.*) or any foreign country specific Top Level Domain.

The text decision is available (in Dutch only) at *www.cepina.be/domainnames_internet.html*.

By Patrick Michielsen, Stibbe, Brussels office; e-mail: patrick.michielsen@stibbe.com

IRELAND

First Decision under the .ie Dispute Resolution Policy

Electricity Supply Board of Dublin v. Lislyn Retail Limited

On December 19, 2003 the first decision under the new .ie Dispute Resolution Policy ("the Policy") was delivered. The IE Domain Registry, which administers .ie (the country code for Ireland), launched its own dispute resolution procedure in July 2003. The Policy, which is administered by the World Intellectual Property Organisation (WIPO), was introduced to facilitate the resolution of .ie domain name disputes. The Policy is similar to the widely used Uniform Dispute Resolution Procedure (UDRP) which has been adopted in relation to disputes concerning generic Top Level Domains (gTLDs), such as .com and .org.

The first dispute under the Policy related to the registration of the domain name, shopelectric.ie. The complaint had been filed by the Electricity Supply Board of Dublin, the largest electrical retailer in the Republic of Ireland, which provides services under the name SHOP ELECTRIC. The Complainant sought to rely on its use of the name since 1968 and its Republic of Ireland trademark. The respondents to the complaint were Lislyn Retail Limited (formerly Northern Ireland Electricity Retail Limited) and Northern Retail Limited which formed part of the Shop Electric Group of companies, based in the United Kingdom. Lislyn had provided electrical retail services under the name SHOP ELECTRIC in Northern Ireland for about 30 years. The Respondents had a number of U.K. trademarks (which cover Northern Ireland) for the name SHOP ELECTRIC.

Under the Policy, the Complainant has to successfully overcome three hurdles. First, it has to establish that the disputed domain name is identical or misleadingly similar to a protected name in which the Complainant has rights. In the shopelectric.ie dispute, the Panellist found that shopelectric.ie was identical to the Complainant's trademark, notwithstanding that the complainant had a stylised word mark.

Secondly, the Complainant has to establish that the registrant of the name has no rights or legitimate interest in the name. In the shopelectric.ie decision, the Panellist noted that, whilst there are similarities between the Policy and the UDRP, the non-exhaustive factors which are provided in the Policy differ substantially from the UDRP to determine whether the registrant has a legitimate interest in the name. In particular, unlike the UDRP, in the Policy there is no mention as to whether the registrant is making a "legitimate non-commercial or fair use" of the name or is "commonly known by the name". In the Policy, factors which may be taken into account in relation to whether the registrant has a legitimate interest in the name include "where the domain name corresponds to the personal name or pseudonym of the registrant" and "where the name is identical or misleadingly similar to a geographical indication has been used, in good faith, by the registrant before such geographical indication was protected in the island of Ireland".

Finally, the Complainant has to show that the domain name was registered or is being used in bad faith which is similar to the UDRP.

In the shopelectric.ie dispute, the Respondent successful proved that it had a legitimate interest in the domain name due to its long use of the name in Northern Ireland and its U.K. trademarks.

By Kate Ellis, an Associate in the Manchester office of Eversheds. The author may be contacted at: KateEllis@eversheds.com

THE NETHERLANDS

File Swapping Software Does Not Violate Dutch Copyright Law

Buma/Stremra v. KaZaA

Supreme Court of the Netherlands, December 19, 2003, C02 186/HR

On December 19, 2003 the Dutch Supreme Court ruled on the recent KaZaA case.[1] The Court made its decision however, without ever actually deciding any copyright issues itself. The Supreme Court dismissed Buma/Stemra's appeal on procedural grounds related to the wording of the claims as brought by Buma/Stemra. At the same time this means that the Amsterdam Appellate Court's judgment, that KaZaA is not committing copyright infringement, still stands.

The Amsterdam Court of Appeal relied heavily on an expert witness, Professor Huizer, who made the following observations:

- KaZaA is the producer of so-called peer-to-peer software that enables users to exchange data files with other users without the use of a central server or database.
- Any user can act as a possible source for downloading files through the Internet.
- Some users will act as Supernodes, which means they act as a meeting place for other users, and as a search engine to locate desired files. Once the file is found, it will be downloaded directly from the source location without passing the Supernode. A list of current Supernodes is made available when the KaZaA software is first installed. Once a desired file is located by a user, that file can be downloaded directly from the PC of another user who is in possession of the requested file and is willing to make it available to other users. No involvement on the part of KaZaA is needed for this to happen.

In addition, Professor Huizer advised that the use of KaZaA software was by no means limited to music files. In his view, KaZaA software was very useful as a communications tool to autonomous communities that do not want to use a central database, such as freelance photographers, real estate agents and individuals who want to publish content independently.

Furthermore, Professor Huizer said that KaZaA software could only be adapted to recognise copyright protected files if there was an unambiguous way to do this, which however is not the case. Even if a worldwide standard for file recognition was available, this could easily be circumvented. The use of KaZaA's software is not dependant on the involvement of KaZaA. Introducing a mechanism to block the exchange of copyright protected files is not technically feasible at present. Finally, Professor Huizer also noted that the closing down of KaZaA's website had had almost no effect on the number of KaZaA users.

  WILR ISSN 1468-4438

The Court of Appeal, relying on Professor Huizer's expert opinion, concluded that KaZaA could not prevent the use of its software to copy files that are copyright protected, such as MP3 files. The Court also took into account that the only option KaZaA had to comply with the injunction imposed by the District Court, was to completely shut down its website. The Court of Appeal ruled that KaZaA itself did not commit any copyright infringement. In as far as committing any acts which were relevant under copyright law, this was done by KaZaA users and not by KaZaA itself. Providing the means to publish or multiply works that are copyright protected is not itself an act of publication or multiplication. It is not true either that the KaZaA software is exclusively used for illegally downloading copyright protected works. Therefore, supplying KaZaA software is not unlawful, according to the Court of Appeal.

In this part of its ruling, the Court of Appeal clearly decided that KaZaA was not committing any copyright infringements and was not acting unlawfully in any other way. However, strictly speaking, there was no need for the Court of Appeal to decide this, since there was a different reason entirely why Buma/Stemra's claim could not have been awarded. The Court of Appeal also rejected Buma/Stemra's claim as it believed KaZaA could never fulfil the obligation as claimed by Buma/Stremra.

Buma/Stremra claimed that KaZaA should be ordered to take every precaution necessary to prevent copyright infringements by its users. Professor Huizer advised that this was not technically feasible. Remarkably, Buma/Stremra had not amended its claim after the organisation received a copy of Professor Huizer's report. At that stage, the collective society could still have included a secondary claim, for instance for an injunction on future distribution of the software. Buma/Stemra however chose not to do so and so their claim was rejected.

At that stage, the most sensible option for Buma/Stremra would have been to bring a new action with better claims, but instead they chose to appeal to the Supreme Court. This was not a wise decision, since the Supreme Court merely judges whether the Court of Appeal has applied the law correctly and whether it has substantiated its rulings sufficiently. One cannot present new facts or bring new claims in the Supreme Court.

Theoretically, the Supreme Court could have referred to the Court of Appeal's ruling on the copyright issue. However, it was not required to do this and chose not to so so.

Buma/Stremra argued in the Supreme Court that the Court of Appeal should have construed its claim in such a way that it would have included other, in Buma/Stremra's view, less far reaching claims.

More specifically, the claim should have been understood to include a claim for an injunction on future distribution of software that could be used to copy rights protected works. The Supreme Court ruled that this would amount to a total injunction on distribution of the software, which could not be regarded as a less far reaching claim and therefore, could not have been regarded as included in the claim as filed.

Buma/Stremra also argued that its claim should have been construed to include a claim for an order to re-design the software in such a way that it could no longer be used to copy rights protected works. The Supreme Court ruled that the Court of Appeal's assumption, that the re-design necessary to achieve this, was not possible.

Thus, the Court of Appeal had made no errors in its claim construction and had therefore correctly rejected the claim on the grounds that KaZaA could never fulfil such an obligation. Thus the Supreme Court focused on whether the lower court's decision correctly applied Dutch law and therefore, did not have to debate the copyright issues.

As previously stated, the Court of Appeal's ruling on the copyright issues still stand. Buma/Stremra could of course bring a new action with better worded claims. However, the District Court and the Court of Appeal would simply reject any such claim on the basis of the Court of Appeal's ruling on the copyright issues. This means that Buma/Stremra would have to go back to the Supreme Court to try to get the new Court of Appeal judgment overturned and have the case referred to another Court of Appeal. Only at this stage (the fourth instance in the new proceedings) would Buma/Stremra then have any chance of obtaining an injunction against KaZaA.

Buma/Stremra's lawyer is reported to have said that his client is considering other methods to prevent copyright infringements. In a statement, Supreme Court lawyer Cohen Jehoram, described the ruling as a missed opportunity whereby the Court could have given some guidance on the legal issues surrounding peer-to-peer software and how it can contribute to copyright infringement.

Even a new Supreme Court hearing will not be the end of the matter. Since the Supreme Court does not grant injunctions, but only affirms or overturns Court of Appeal judgments, an injunction could only be obtained after referral to another Court of Appeal.

Effectively this means that the Amsterdam Court of Appeal judgment of March 28, 2002 is going to be the standing case law in the Netherlands for many years to come. The Court of Appeal judgment may also be used as a precedent in other jurisdictions, since copyright law has been partly harmonised almost worldwide through the Berne Convention. Of course, the Berne Convention, last updated in 1971, contains no provisions related to file swapping software, but Courts throughout the world have also given proper consideration to precedents from other countries when ruling on the equally new phenomenon of Internet provider liability. The Supreme Court judgment itself will not serve as a precedent, since it does not deal with any copyright issues, as has been explained here.

The ruling does not of course mean that individuals who use KaZaA software to upload copyright protected works without permission from the right owners do so without any risk. By doing so, they continue to infringe rights protected works and actions may be brought against them successfully. This is the correct procedure; attacking new technology in order to stop infringers is not.

Wouter Pors and Camilo Schutte, both of Bird & Bird, were the Supreme Court litigators for KaZaA.

1 In 2001, Buma/Stemra, a Dutch collecting society representing music writers and publishers began legal proceedings against KaZaA B.V., developers of the KaZaA software which is used by music fans to swap files via a peer-to-peer network. Burma/Stemra alleged that KaZaA's software infringed music copyright.

The Amsterdam District Court ruled in favour of Burma/Stemra on November 29, 2001, though this ruling was overturned by a Court of Appeals judgment (March 28, 2002).

By Wouter Pors, Bird & Bird, The Hague.

News

HONG KONG

Launch of Second Level .hk Domain Names

The Hong Kong Domain Name Registry ("HKDNR") has announced that it will be launching second level domain names under the top-level country-code domain .hk in early 2004. Second level domain names will be generally available to the public after a Soft Launch Period, during which priority for second level .hk domain names will be given to applicants that satisfy certain requirements (see below).

There are no registration requirements for second level .hk domain names unlike for third level .hk domain names (which can only be obtained by entities with a local presence in Hong Kong). Second level .hk domain names will be available to any entity (including individuals aged 18 years or older) irrespective of their location. No supporting documents will be required when applying for a second level .hk domain name save where the domain includes words such as "bank" or "insurance".

There is no restriction on the location of name servers and there is no limit to the number of domain names that can be registered by any one individual or entity. The minimum registration period is one year and the maximum is five years.

Soft Launch Period for Second Level Domain Names

Prior to the launch of second level .hk domain names to the general public, priority will be given to:

- owners of Hong Kong trademarks or service marks (Priority Registration Period);
- current holders of third level of .hk domain names (Pre-Registration Period);
- individuals or entities that seek to register a second level .hk domain name before the general launch (Sunrise Period).

Priority Registration Period

The Priority Registration Period runs from 12 noon on January 26, 2004 until 12 noon on March 19, 2004. Only owners of registered Hong Kong trademarks or service marks qualify for the Priority Registration.

The following documents/information must be provided with the application during the Priority Registration Period:

- a copy of the trademark or service mark certificate from the Hong Kong Trademarks Registry;
- a letter of declaration from the applicant that it is the owner of the trademark or service mark.

If two or more entities apply for the same second level .hk domain name during the Priority Registration Period, priority will be given to the applicant who also has an equivalent third level domain name. If more than one applicant has an equivalent third level domain name, the applicant with the longest standing equivalent third level domain name will have priority. If none of the applicants has an equivalent third level domain name, or if the equivalent third level domain names are equally long standing, priority will be decided by random draw.

The Pre-Registration Period

The Pre-Registration Period runs from 12 noon on April 6, 2004 until 5:30pm on May 7, 2004.

Current holders of .hk third level domain names can seek to obtain the corresponding second level .hk domain name during the Pre-Registration Period. No supporting documents are required for applications during the Pre-Registration Period.

If two or more entities apply for the same second level .hk domain name during the Pre-Registration Period, HKDNR will give priority for allocation in the following order:

a. government organisations (namely, organisations that hold the equivalent .gov.hk third level domain name);

b. statutory organisations under Hong Kong law. If there are two or more applicants that are Hong Kong statutory organisations, the applicant with the longest standing equivalent third level domain name will have priority;

c. all other applicants except for the applicant with the equivalent .idv.hk domain name. If there are two or more applicants the applicant with the longest standing equivalent third level domain name will have priority.

d. the applicant with the equivalent .idv.hk domain name.

If in relation to (b) or (c) there are two or more applicants with an equivalent third level domain name that is equally long standing, allocation will be by random draw.

The Sunrise Period

The Sunrise Period commences at 12 noon on May 17, 2004 and ends at 5:30pm on May 28, 2004.

There are no qualification requirements for the sunrise period. Once the sunrise period closes, if two or more entities have applied for the same second level .hk domain name, HKDNR will allocate the second level .hk domain name by random draw.

Objections

HKDNR has put in place a procedure for the public to object to the allocation of a second level domain name during the Soft Launch Period. The person objecting to an allocation must provide evidence that the allocation was not made in accordance with the Soft Launch Period Rules. Objections for any other reason will not be entertained. An objection must be made within 14 days of the date on which HKDNR announces the registration results for the respective tier of the Soft Launch Period, using the objection form available on HKDNR's website.

An Objections Committee, consisting of board members of the Hong Kong Internet Registration Corporation Limited and/or external parties as required, will render a decision in relation to any objections within 30 calendar days. Decisions of the Objections Committee will be final. If the Objections Committee determines an objection is justified, the Objections Committee may require HKDNR to cancel a second level domain name registration obtained during the Soft Launch Period.

General Launch of Second Level Domain Names

Second level domain names will be generally available to the public after the Soft Launch Period, that is from 12 noon on May 31, 2004. There will be no registration requirements and allocation will be on a first come first served basis.

By Gabriela Kennedy, Partner, and Joanne Harland, Registered Foreign Lawyer with Lovells TMT Group, Hong Kong. For further information about issues raised in this article please contact either gabriela.kennedy@lovells.com or joanne.harland@lovells.com.

Jurisdiction

Case Report

EUROPEAN UNION

E-Pharmacies and the Free Movement of Drugs

Deutscher Apothekerverband eV v. 0800 Docmorris NV & Jacques Waterval (2003), ECJ Case C-322/01

European Court of Justice, December 11, 2003

(Preliminary ruling by the Landesgericht Frankfurt am Main, August 10, 2001)

From featuring in 2003's top ten spam culprits to being implicated in several unfortunate deaths, the effects of online pharmacies are widespread. Their regulation is an important issue which has inspired varying responses from different countries.

Characteristically, the United States has taken a hard-line in its regulatory measures and has issued orders to various online pharmacies. In contrast, the European Commission (EC) has validated the selling of medicines online in the spirit of the free movement of goods, as the case of *Deutscher Apothekerverband eV v. DocMorris NV and Jacques Waterval* demonstrates.

Background

The proceedings were brought by Deutscher Apothekerverband eV, a German organisation which advances the economic and social interests of German pharmacists, much like the Association of the British Pharmaceutical Industry and the Royal Pharmaceutical Society in the United Kingdom.

DocMorris is a Dutch limited company. It sells prescription and non-prescription drugs via a traditional chemist's shop and an Internet site. DocMorris is fully licensed and also controlled by the authorities in the Netherlands. Mr Waterwal is a Dutch pharmacist, who was a director of DocMorris and was, and still is (at the time of writing), one of its legal representatives.

The website *www.0800DocMorris.com* has Dutch, German and English language options with the intention that both German and Dutch customers will use the service to order medicines which have been authorised in either Germany or Holland. Significantly, this site reveals a genuine, well-run and legitimate business. For example, prescription drugs can only be ordered by sending DocMorris the original copy of the prescription and advice can be requested from qualified pharmacists by e-mail or telephone. In short, it offers: a discreet, anonymous service for those who may be embarrassed to pick up an order for Viagra; home delivery for those who may be too infirm or too busy to shop; and a value-for-money service, unlike other, more unscrupulous, Internet pharmacies.

Notwithstanding the above, Deutscher Apothekerverband eV sued DocMorris and Mr Waterval asserting that pursuant to both Arzneimittelgesetz (AMG) and Heilmittelwerbegesetz (HMG), German laws on the sale of medicinal products and the advertisement of medicines state respectively, that by selling both prescription and non-prescription medicines via the Internet, DocMorris was in contravention of German law.

The claimant suggested that the AMG ban on the mail order selling of medicinal products, which was limited to pharmacies, extended to the sale of these products on the Internet. Other stipulations include the necessity for a pharmacist to advise and consult the customer before purchase.

The HMG prohibits any advertisement selling medicinal products which may only be supplied by pharmacies, and advertising which sells medicinal products by teleshopping. It also restricts the advertisement of prescription-only medicines to doctors, dentists, vets, pharmacists; and states that psychotropic drugs may only be advertised in professional circles. A further piece of legislation regulated the price to be paid by the end consumer of medicines, which the website would have significantly undercut.

The Issues

The Landgericht Frankfurt am Main, the court of the First Instance, made an Article 234 reference to the European Court of Justice to determine the questions of EC law which this case posed. Firstly, was the AMG infringing Article 28 *et seq*. – free movement of goods in that the national prohibition might be construed as being a measure equivalent to a quantitative restriction and, if so, whether or not it falls within one of the justifications provided for by Article 30? Secondly, were the measures relating to the prohibition on advertising compatible with Articles 28-30; and the way in which Articles 28-30 interact with Directives specifically relating to the sale and advertising of medicinal products? Finally, if some aspects of an e-pharmacy of a Member State infringe provisions concerning the advertising of medicines, should it be inferred from Articles 28-30 that cross-border trade which takes place because of this very advertising should be regarded as lawful in order to realise the principle espoused by the concept of the free movement of goods?

The issues were decided by separating the categories of medicine into prescription and non-prescription drugs.

Responses

The ECJ had to examine whether the concept of the free movement of goods was being infringed. German law restricted the importation, via mail order, of medicines. Medicines which, in Germany, could only be sold in pharmacies but, in the Netherlands, were available on the Internet.

The ECJ took the view that where medicinal products had not been authorised for sale in Germany, then

notwithstanding that those medicines have been authorised for sale in the Netherlands, they cannot be sold to and purchased by German consumers. It was found that national legislation implementing this, such as in the AMG, would not be considered equivalent to a quantitative restriction.

Conversely, restricting the sale, by mail order, of products which have been authorised for sale in Germany by the German authorities was considered to be equivalent to a quantitative restriction. The justification given was that even if the law applied equally to both German pharmacies and pharmacies situated in other Member States, non-German pharmacies would be affected disproportionately – it would be difficult for them to gain access to the German market without the medium of the Internet and so free trade would be hampered.

Of course, certain measures that are quantitative restrictions can be justified pursuant to the Article 30 derogation. In this case the German government was arguing that it was warranted in restricting the sale of medicines via mail order because it was protecting the health and life of its citizens. The various Member States outlined their views and concerns. For example, the Greek government agreed with the Germans and Austrians declaring that it felt that restricted medicines should only be sold in pharmacies because, for example, of the importance of the public gaining the advice of a qualified pharmacist before purchase to ensure that the medicinal product would be completely suitable. The Irish Government preferred a complete ban on the sale of medicinal products over the Internet citing the potential for both mistaken use of drugs and actual drug abuse.

All these views were considered by the ECJ. However, it concluded that if the health and life of humans could be protected in a way which was less restrictive than a measure equivalent to a quantitative restriction then that should be the case. It considered the fact that the Dutch government controlled the DocMorris e-pharmacy as strictly as it regulated its physical pharmacy and that DocMorris itself had imposed its own security measures. It would not dispense prescription drugs without being sent a valid prescription and the decision of whether a certain drug needs to be prescribed with a doctor's prescription has been harmonised within the European Union. This was not held to be a valid reason for restricting the sale to German consumers.

Consequently, because of the fact that the sale of prescription drugs has been harmonised, whereas the sale of non-prescription drugs remains less well-controlled at a European level, the ECJ felt it prudent to make the distinction between prescription and non-prescription medicines when making its Article 234 response.

Non-Prescription Medicines

It was held that none of the reasons given by Apothekerverband could justify an absolute prohibition on the sale by mail of non-prescription medicines, as: the DocMorris website was staffed by qualified pharmacists who could give advice and assistance; if a consumer were going to abuse a non-prescription medicine he would do so whether he had purchased the product by mail order or in a conventional shop; the pharmacy was subject to Dutch obligations; and price controls to which German prescription drugs were subject did not apply to German non-prescription medicines so this could not be used as a justification either.

Prescription Medicines

Given that certain medicines are available by prescription only (due to their potency), it was acknowledged that these types of medicine needed to be more strictly controlled. It was also recognised that the object for controlling the price of these medicines was in order to provide a revenue stream for the German healthcare system.

As a result it was determined that Article 30 could be used as a justification for prohibiting the sale of prescription drugs via mail order. It emphasised that, although in general terms a purely economic aim could not be used to justify a prohibition, it would be contrary to the Member State's interest if its healthcare system were allowed to become destabilised. More importantly, it was accepted that allowing prescription medicines to be supplied on receipt of a prescription could lead to abuse or inappropriate use, particularly if the medicine were labelled in a language which the end consumer could not understand.

Advertising

Since it was held that the prohibition on the selling of medicines which had to be authorised in Germany was compatible with EC Law, it followed that the prohibition on the advertising of authorised medicines on the Internet was also compatible.

Again, since it was held that a prohibition on the selling of prescription medicines via mail order was justified pursuant to Article 30, a prohibition on the advertising of such medicines on the web was also justifiable.

But it was found that there could be no justification for the prohibition in relation to the advertising of the non-prescription medicines.

Effect of the ECJ Ruling on U.K. Law

In the United Kingdom there is nothing inherently unlawful about selling or advertising drugs on the Internet. Instead, the general rules in force concerning the selling and advertising of drugs apply. The consumer can use the services of several reputable and scrupulous companies such as Allcures.com and Healthexpress.co.uk. But there are still many online pharmacies which are driven by commercial considerations with little, if any, regard for the health and safety of its customers. Compliance in this area lies with the Medicines Healthcare Products Regulatory Agency. Historically, the Agency has been unwilling to use its powers against online pharmacies which have defied the law. It is clear from this case that the U.K. Government could be much tougher in its legislation using the Article 30 justification of the protection of human health and life to justify any prohibition.

By Paul Barton, a Partner in the Technology Law Group at London law firm, Field Fisher Waterhouse.

Legislation & Guidance

News

UNITED KINGDOM

Oftel Releases 2003 Annual Report

Oftel, the U.K. regulator for the telecommunications industry, has recently published its 2003 Annual Report, submitted to the Secretary of State for Trade & Industry in mid-December 2003. It is the final report of David Edmonds as Director General of Telecommunications. Oftel has now been incorporated into the new Office of Communications (an overarching telecoms, broadcasting and media regulator).

The Report is available from Oftel's website at *www.oftel.gov.uk* or from The Stationery Office, with reference HC 54, priced £22.

The Report reviews Oftel's work in 2003 and, in particular, gives reviews of the fixed telecoms market, the mobile market, the narrowband Internet market, the broadband market, broadcasting, international activities and Oftel's legislative framework.

In addition to the body of the document analysing the work carried out in 2003, Annex 1 lists Oftel's impressive publications during that year on a whole range of topics.

As always, the document is extremely thorough and gives a very comprehensive view of the work that has been carried out by Oftel during 2003.

In his covering letter to the Secretary of State for Trade & Industry, submitting the Annual Report, the Director General said,

> "2003 was… a significant milestone throughout Europe with the implementation of the new regulatory framework. Oftel was ahead of all other European regulators in its work to implement the new Directives".

By Heather Rowe, a Partner with Lovells, London

Security & Surveillance

The E.U. Safer Internet Action Plan

By Avv. Alessandro del Ninno, a Partner in the Information & Communication Technology Department of Studio Legale Tonucci, Rome. The author may be contacted at: adelninno@tonucci.it

The Internet offers positive benefits particularly in education, by empowering consumers, aiding the creation and distribution of content and offering wide access to ever richer sources of digital information. However, the amount of harmful and illegal content carried over the Internet, while limited, could adversely affect the establishment of a favourable environment in which initiatives and undertakings can flourish. In order to ensure that consumers make full use of the Internet, it is essential that a safer environment for Internet use is created. Use of the net for illegal purposes, such as offences against children and for the dissemination of racist and xenophobic ideas must be curtailed.

In this regard, E.U. institutions have adopted specific measures aimed at giving increased protection to minors, for example:

- on April 24, 1996 the Council requested that the Commission produce a summary of problems posed by the rapid development of the Internet and to assess, in particular, the desirability of Community or international regulation;
- on October 23, 1996 the Commission transmitted a communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the Internet and published a Green Paper on the protection of minors and human dignity in audiovisual and information services;
- the Council and the Representatives of Governments of the Member States, in a Resolution of February 17, 1997 welcomed the report of the Commission working party on illegal and harmful content on the Internet and requested Member States and the Commission undertake a number of actions;
- in its Resolution of April 24, 1997 on the Commission communication on illegal and harmful content on the Internet, the European Parliament called on the Member States to strengthen administrative co-operation on the basis of joint guidelines and on the Commission to propose, after consulting the European Parliament, a common framework for self-regulation at European Union level;
- in the Ministerial declaration adopted at the initiative of the German Government during a International Ministerial Conference ("Global Information Networks: Realising the Potential", held in Bonn during July 1997), Ministers stressed the role which the private sector could play in protecting the interests of consumers and in promoting ethical standards online.
- It was suggested that this could best be achieved through self-regulation, in compliance with and supported by the legal system. Industry however, was encouraged to implement open, platform-independent content rating systems, and to propose rating services which meet the cultural and linguistic needs of different users. Ministers further recognised that it is crucial to build trust and confidence in Global Information Networks by ensuring that basic human rights are respected.

- on September 24, 1998 the Council adopted a Recommendation on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and protecting human dignity.

Combating Illegal and Harmful Content on Global Networks

Considering that the promotion of industry self-regulation and content-monitoring schemes will play a crucial role in consolidating a safer Internet environment, in 1999, the E.U. Commission launched the so called "Safer Internet Action Plan" ("the Action Plan") which promotes safer use of the Internet for children by combating illegal and harmful content on global networks and by encouraging, at European level, an environment favourable to the development of the Internet industry. The Action Plan initially covered the period 1999–2002, but it has recently been extended to December 31, 2004.

The main points of the Action Plan are set out below:

Encouraging Self-Regulation and Codes of Conduct

An effective way to restrict circulation of illegal material is to set up a European network of centres (known as hotlines) which allow users to report offensive or controversial content which they come across in the course of their Internet use and which they consider to be illegal. Responsibility for prosecuting and punishing those responsible for illegal content remains with the national law-enforcement authorities, while the hotline aims at revealing the existence of illegal material with a view to restricting its circulation. Differences in national legal systems and cultures must also be respected.

So far, hotlines exist only in a limited number of Member States. Their creation needs to be encouraged so that there are hotlines in operation which cover the Union both geographically and linguistically. Mechanisms for exchange of information between the national hotlines, and between the European network and hotlines in third countries need to be put in place.

In order for this network to develop to its full potential, co-operation between industry and law-enforcement authorities is essential to ensure Europe-wide coverage and co-operation, and increase effectiveness through the exchange of information and experiences.

This action will take the form of a call for proposals for participating organisations (20-25) to establish a European network of hotlines, and links between this network and hotlines in third countries, develop common approaches and stimulate transfer of know-how and best practice.

The participating organisations will be supported by a cross-section of industry players (access and service providers, telecoms operators, national hotline operators) and users. They will have to demonstrate a forward-looking and innovative approach, in particular in their relationship with national law-enforcement authorities.

For the industry to contribute effectively to restricting the flow of illegal and harmful content, it is also important to encourage enterprises to develop a self-regulatory framework through co-operation between themselves and the other parties concerned. The self-regulatory mechanism should provide a high level of protection and address questions of traceability.

In view of the transnational nature of communications networks, the effectiveness of self-regulation measures will be strengthened, at E.U. level, by the co-ordination of national initiatives between the bodies responsible for their implementation.

Developing Filtering and Rating Systems

To promote safer use of the Internet, it is important to make content easier to identify. This can be done through a rating system which describes the content in accordance with a generally recognised scheme (for instance, where items such as sex or violence are rated on a scale) and by filtering systems which empower the user to select the content he/she wishes to receive. Ratings may be attached by the content provider or provided by a third-party rating service. There are a number of possible filtering and rating systems. However, their level of sophistication is still low and none has yet reached the "critical mass" where users can be sure that content in which they are interested and content which they wish to avoid will be rated appropriately, and that perfectly innocuous content will not be blocked. Uptake of rating systems by European content providers and users remains low.

Current filtering and rating systems are limited in their scope. The objective of this point in the Action Plan is to encourage the establishment of European systems and familiarise users with their use. Filtering and rating systems must be internationally compatible and interoperable and developed with full co-operation of representatives of industry, consumers and users.

Promoting Public Awareness

Internet use amongst the general public is increasing and people are reaping the benefits of the new services. At the same time, there is a degree of uncertainty as how to deal with every aspect of network communication; parents, teachers and children need to be made aware of the potential of the Internet and its drawbacks and do not always have sufficient knowledge about the means to protect children from undesirable content.

Fostering greater public awareness is necessary to underpin the other action points in the Plan, since the efforts of industry to implement self-regulation and filtering and rating will only succeed if users are aware of them.

Other Points for Consideration

The Internet operates on a global basis. The law operates on a territorial basis – nationally or, in the case of Community law, covering the European Union. The Action Plan can be also be supported by considering other legal questions which are not dealt with by E.U. initiatives. Points for consideration here might include the issues of applicable law and procedure.

Co-ordination with similar international initiatives and the sharing of experience and best practice between operators and other parties in both the European Union and worldwide is necessary to ensure coherence between European action and similar initiatives in other parts of the world. Regular consultation meetings will help to achieve this.

Achievements and Further Steps

On November 3, 2003 the E.U. Commission adopted a communication (COM 2003 653, hereinafter "Communication") on the evaluation of the Safer Internet Action Plan Programme 1999–2002 (hereinafter "the Programme"). The evaluation was carried out by a team of external consultants, who recognised the positive impact of the current programme (particularly in fostering networking and providing a wealth of information about the problems of safer use of the Internet and their solutions) and

who recommended the continuation of the Community efforts in this area via means of a follow-up programme.

The Communication concerns the evaluation of the Programme. The objective of the Programme, as specified in the European Parliament and Council Decision adopting a Multiannual Community Action Plan to promote safer use of the Internet by combating illegal and harmful content on global networks, promoted safer use of the Internet and encouraged, at European level, an environment favourable to the development of the Internet industry.

The Programme covered the four-year period from January 1999 to December 2002 with a reference budget of EUR25 million. The programme was implemented through three main channels:

- creating a safer environment (creating a European network of hotlines and encouraging self-regulation and codes of conduct);
- developing filtering and rating systems;
- encouraging awareness actions.

During the years 1999–2002, 37 projects were co-financed, involving over 130 different organisations.

Two service contracts were concluded for advice to self-regulatory bodies and for exchange of information about best practices. Decision 199/276/EC (amended by Decision No. 1151/2003/EC) extended the duration of the programme until December 31, 2004, increasing the indicative budget by EUR13.3 million and making a number of changes (*i.e.*, including the new 10 E.U. Member States from May 1, 2004) to the title and scope of the programme and its implementation.

Finally, the European Union's particular interest in promoting a "safer Internet" by combating illegal or harmful content is illustrated by some of the recent measures adopted by the Commission and the Council. Amongst these is the recent enaction of the Council's Framework Decision of December 22, 2003 n. 2004/68/GAI (OJ L 13, 20.01.04) aimed at combating the sexual exploitation of minors. This Decision binds the E.U. Member States to adopt by January 2006, specific legislative measures aimed at criminally sanctioning individuals and legal entities who use electronic means to produce, distribute or transmit such content.

Another interesting and recent E.U. measure is the E.U. Parliament and Council's Decision N. 2256/2003 (OJ L 336/1, 23.12.03) adopting a multi-annual Plan for monitoring the eEurope Action Plan 2005. This Decision requires amongst other things, the development and strengthening of the Information Society's network security.

All the above mentioned acts must also be evaluated in light of the commercial impact of the new rules, aimed at developing network security. The main players in the related markets will be required to develop innovative products and services to achieve the legislative targets which have been set.

News

HONG KONG

Fraudulent Copycat Websites

The Securities and Futures Commission of Hong Kong (SFC) has issued guidance for businesses, warning against fraudulent websites and how to identify the copycat sites.

Fraudulent copycat websites are a type of Internet fraud where the fraudsters imitate the websites of reputable or well-known financial institutions when in fact the websites are not authorised by or related to the relevant financial institutions in any way. The operators of the copycat websites may claim to be providing investment or banking services. Investors who are taken in will be tempted to part with their money and/or disclose personal information such as Personal Identification Numbers (PINs) which the fraudsters may use to swindle investors.

Common Features of Fraudulent Copycat Websites

- A fraudulent copycat website usually adopts a website name or address which is very similar to or contains part of the name of a legitimate financial institution, its subsidiaries or associates.
- Fraudsters may copy legitimate websites and build their own with similar URL's to disseminate false information, or to induce unwary investors to transfer funds into their bank accounts or submit personal information.
- Sometimes, fraudsters may also transliterate the name of a legitimate website into a language used by the investors, such as Chinese, as its domain name. Investors may then be led to the fraudulent website when they type in the transliterated name using Internet search engines.
- The fraudulent websites may contain links to the websites of other reputable financial institutions which are not authorised and where there are no affiliations between the fraudsters and the legitimate financial institutions.
- The websites may contain contact details for the public to verify the authenticity of the organisations which are however answered by the fraudsters themselves.
- In general, operators of fraudulent copycat websites will try to create a false impression that their websites represent those of legitimate financial institutions or that they are somehow related or affiliated to the financial institutions so as to swindle investors.

How to Identify Copycat Sites

- Verify the website address and the legitimacy of a website directly with the financial institution concerned.
- Avoid using the contact details provided on the website. Find out the contact details from an independent source as scam operators may publish telephone numbers or e-mail contacts on the website which are answered by the fraudsters themselves.
- Check with the relevant regulators whether the financial institution is properly accredited. The licence status of brokerages may be checked from the Public Register of Licensed Persons and Registered Institutions on the SFC's website (*www.hksfc.org.hk/eng/licensing/html/persons/lpfl.htm*). The Public Register contains the names and addresses of all SFC's licensed brokerages and, where available, their website addresses. The brokerage or the SFC may be contacted for additional verification.
- Do not submit any personal information or send money to anyone before verifying the legitimacy of the recipient.
- Report any suspicious websites to the relevant regulators and the Police.

Further information is available from the Hong Kong Monetary Authority and the SFC at www.info.gov.hk/hkma and www.hksfc.org.hk, respectively.

General

ICANN: A Review

By Kate Ellis, an Associate in the Manchester office of Eversheds. The author may be contacted at: KateEllis@eversheds.com

In February 2002, the Internet Corporation for Assigned Names and Numbers – ICANN – embarked on an ambitious reform process which was designed to improve its effectiveness and overcome widespread criticism of its role and performance. But have these reforms adequately addressed the key challenges faced by ICANN and the Internet community?

ICANN's Background and Role

ICANN is the organisation responsible for the technical co-ordination of the Internet and the Domain Name System (DNS). Whilst ICANN itself may be unknown to all but a relatively small number of Internet users, its activities impact directly on the stability and security of the Internet for all users. As approximately 750 million users access the Internet each day, the successful operation of the Internet is critical and underpinning its success is a complex technical system which, in order to function, requires sophisticated technical standards to be developed and maintained.

ICANN was formed in 1998 as a not-for-profit organisation, incorporated in California, which was intended to help implement the U.S. government's intention to transfer its role in the operation of the Internet into the private sector. The U.S. Department of Commerce (DoC) entered into a Memorandum of Understanding (MOU) with ICANN which effectively gave ICANN temporary authority for the technical and management responsibilities of the Internet. The four principles behind the U.S. government's privatisation 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. It was initially envisaged that the process of transferring responsibility for the Internet to ICANN would be completed by September 2000. However, the MOU has been amended and extended six times and the MOU is now due to expire on September 30, 2006.

ICANN, as a private sector entity capable of overseeing the management of the DNS and of developing consensus-based policies applicable to the worldwide Internet, is a uniquely difficult undertaking. At the time of ICANN's incorporation (and indeed today), no comparable undertaking existed which could be used as a model and as the diversity of economic, geographic, social and cultural interests of Internet users needs to be accommodated, it is a particularly difficult undertaking.

By 2002 ICANN's deficiencies had become apparent and its performance and role was the subject of intense scrutiny in several circles: the Internet community at large, the U.S. Senate and within ICANN itself. Problems were identified which limited the future potential of ICANN. Amongst these were included the inadequate participation of key stakeholders and ineffective procedures which were compounded by a lack of funding.

The Reform of ICANN

Following debate, ICANN was obliged to undertake significant reforms in a number of key areas and the scope of its operations was more sharply defined. On September 19, 2002, the DoC and ICANN entered into Amendment 5 to the MOU. The amended MOU reflected the continuing goal of the DoC to "privatise the technical management of the DNS in a manner that promotes stability and security, competition, co-ordination, and representation". It also identified the scope of ICANN's activities as: making the management of the root server system more robust and secure, encouraging the creation of stable agreements between ICANN and Regional Internet Registries (RIRs), and advancing ICANN's efforts to achieve stable agreements with the organisations which operated the country code top level domains (ccTLDs). The MOU also anticipated the continued improvement of ICANN's consensus policy development process.

On December 15, 2002, ICANN's Board of Directors adopted a series of bylaws which it anticipated would enable ICANN to improve its performance and which recognised the importance of a robust public/private partnership. The bylaws focussed ICANN's mission to the co-ordination of the allocation of the Internet's systems of unique identifiers, in particular to ensure the stable and secure operation of the Internet's naming and addressing systems and to co-ordinate policy development relating to these technical functions. It was also intended that the bylaws would establish a structured policy development process for issues relating to naming policies on the DNS which would be more inclusive of the Internet communities' views and how advice from governments, via ICANN's Governmental Advisory Committee, would be considered in relation to public policy issues.

Enhancing the Participation of Key Stakeholders

A major criticism of ICANN was that it had failed to engage its primary stakeholders. It was recognised that ICANN needed the participation of the main communities which are collectively responsible for the infrastructure of the DNS; namely, the bodies responsible for the underlying Internet protocols – the RIRs, the operators of the ccTLDs and the operators of the root name servers.

RIRs

There are currently four RIRs: APNIC (Asia/Pacific region), ARIN (North America, Africa south of the equator and parts of the Caribbean), LACNIC (Latin America and parts of the Caribbean) and RIPE NCC (Europe, parts of Asia, Africa north of the equator and the Middle East). Each RIR is a non-profit making organisation which is responsible for distributing and managing Internet protocol (IP) addresses on a regional level to Internet Service Providers and local registries. New RIRs may be established in the future. Currently, AfriNIC (which would be responsible for Africa's IP addresses) has "observer" status.

  WILR ISSN 1468-4438

Representatives from each RIR are appointed to the Address Supporting Organisation (ASO), the ICANN body which is responsible for policy development relating to address allocation which, in turn, reports to ICANN's Board.

Throughout 2003, representatives from ICANN and the RIRs met regularly to discuss the most appropriate form of involvement of the RIRs in ICANN's new structure. Discussions primarily focused on the revision of the ASO's policy development process to make better use of the RIRs' existing processes as a means of achieving supported global address policies. ICANN and the RIRs also looked at ways in which the methods of allocating numbering resources among the various regions to manage the numbering resources could be achieved in a way that reflects the interests of the RIRs' members and Internet users.

From these discussions, whilst the trust between the parties (which was at a low in 2002) appears to have grown, there are still a number of important issues which need to be resolved. Agreement has been reached in respect of a statement of procedures to be followed in the allocation of numbering resources to the RIRs. However, there is still no agreement in relation to a number of key issues, including the structure and operation of the address policy development process and the nature of the contractual relationships between ICANN and the RIRs.

ccTLD Operators

There are currently approximately 250 ccTLD operators. Since 2002, ICANN has made efforts to reach agreements with ccTLD operators to achieve, amongst other matters, the stable and secure operation of the DNS, including the delegation and redelegation of the ccTLDs, the allocation of global and local policy formulation responsibility and the clarification of the relationship between a ccTLD operator and its relevant government.

In June 2003, the Country-Code Names Supporting Organisation (ccNSO) was established. This was an important step for ICANN in securing the participation of a key stakeholder. ccNSO's aim is to provide targeted, influential participation by ccTLD operators. A ccNSO Assistance Group was also appointed which consists of ccTLD administrators and other interested persons. Since its appointment, the Assistance Group has considered the specific issues which arise in relation to the interaction between, on the one hand, ICANN which is designed to consider the global technical requirements of the Internet and, on the other, the ccTLDs which are focussed on national interests.

Whilst progress has been made in a number of areas including the establishment of frameworks for accountability of ccTLD operators, ICANN itself accepts that the pace of progress in relation to the framework agreements with the ccTLD operators has been slow which is, in part, due to the need to reach agreements that involve the ccTLD itself, the relevant national government and the local Internet community. To date, ICANN has completed agreements with 13 ccTLD operators, the most notable of which are Australia and Japan. However, with over 250 ccTLDs operators, ICANN still has a long way to go in engaging the ccTLD operators and, thereby improving the stability of the Internet.

Root Nameserver Operators

Another key objective was to improve the stability and security of the Internet. With an increasing focus on global terrorism, the vulnerability of the Internet to disruption has been a longstanding concern. The root servers are at the heart of the Internet. However, in 2002 the relationship between ICANN and the operators of the root servers was poor and there were no arrangements in place between the parties to ensure the stable and secure operation of the Internet.

Today, whilst agreements between ICANN and the root servers operators have still not yet been reached, during 2003 there was increased co-operation between the parties. However, with internationalised domain names becoming a reality and the introduction of IPv6, the stability of the Internet is now under greater pressure than ever.

Technical Management of the DNS

ICANN has continued to undertake its operational activities for the management of the Internet throughout its reforming process and, in this regard, ICANN has achieved a number of successes. It has continued to carry out the responsibilities of IANA (the Internet Assigned Numbers Authority) which is responsible for, amongst other matters, the co-ordination of the assignment of technical protocol parameters, administrative functions which are connected with root management and the allocation of IP address blocks.

ICANN has also been involved in a number of consumer driven initiatives. For example, in early 2003, the Dot Org registry was reassigned from Verisign, the organisation which administers generic Top Level Domains (gTLDs), to the Public Interest Registry (PIR). During the reassignment process, eleven bids to operate the Dot Org Registry were submitted to ICANN and the bids were considered by three independent teams. The bidding process generated a degree of criticism from the wider Internet community. However, since its appointment, PIR has successfully implemented its plan for the transition of the Dot Org Registry from Verisign and a reasonable proportion of the 111 operational .org registrars have now gone through the transition process.

During 2003, ICANN sought to improve protection for gTLD domain name registrants. However, its proposals in this area have created a substantial amount of debate and criticism from within the Internet community. In particular, the adoption by ICANN of Verisign's Waiting List Service (WLS) attracted opposition. The WLS was designed to allow individuals or companies to purchase "options" on existing domain names and, in the event that a domain name was not renewed, the domain name would be acquired by the individual or company which had acquired the option on the domain name. It was proposed that Verisign would administer the system and it would receive $24 for each subscription. ICANN voted in favour of adopting Verisign's WLS proposal, notwithstanding public opposition. In particular, the Names Council which adopted a report by the DNSO Transfers Task Force recommended that the service should not be introduced. Among the wider Internet community, objections to the monopoly Verisign would have over the service were expressed. Despite the strong objections, ICANN supported the adoption of the service and in July 2003 the WLS was introduced. Following its introduction, legal proceedings were brought by 3 registrars against ICANN. The basis of the claim was that ICANN, in adopting Verisign's WLS, had breached its Registrar Accreditation Agreements pursuant to which ICANN is obliged to refrain from unreasonably restricting competition. The Registrars argued that the WLS would effectively allow Verisign to become the sole provider of services to potential registrants

seeking to register expiring domain names. This episode illustrates that, whilst ICANN may have improved the ability of the wider Internet community to offer input into policy decisions, ICANN does not necessarily take into account the views of the Internet community in its actual decision making process.

Improved Transparency and Accountability Mechanisms

In 2002, ICANN faced extensive criticism about its perceived lack of accountability and governance. In its "Blueprint for Reform" which was published in June 2002, ICANN proposed that it would appoint an Office of Ombudsman together with a "Manager of Public Participation" to improve accountability. In the bylaws which were adopted in December 2002, a provision was included to establish an Office of Ombudsman which would be responsible for the overseeing of complaints about unfair or inappropriate actions by ICANN's Board or staff. However, the progress in establishing an Office of Ombudsman has been relatively slow. Whilst ICANN has taken steps to appoint an individual who will provide assistance to it in developing ICANN's Ombudsman programme, policies and operating practices the Office has not, as yet, been established and a person has not been appointed to lead the Office.

Improved Mechanisms for Informed Participation in ICANN

The bylaws also identified that a core value for ICANN was to facilitate "broad, informed participation reflecting the functional, geographic and cultural diversity of the Internet at all levels of policy development and decision-making". As part of this mission, ICANN has, over the past year, taken steps to achieve this goal. In particular, ICANN has focused on the creation of an At-Large Advisory Committee (ALAC).

The bylaws created an ALAC which included regional representatives from around the world to provide informed input on ICANN's policy decisions. Through an appointed representative from each region, the regional views are to be fed through to ICANN's Board. ICANN expected that the ALAC would provide an important channel through which Internet users from throughout the world would be able to contribute to ICANN's decision making process. Whilst the framework which outlines the criteria, guidelines and processes that are needed to begin to organise the global network of ALAC representatives was approved by ICANN's Board in June 2003, the full participation of the wider, world-wide Internet community is a substantial undertaking which will take goodwill, time and resources to be successful.

Whilst ICANN has made some steps forward in engaging its key stakeholders and the wider Internet community, on a broader level, ICANN is still accused by some users that its structure is too complex which impedes its ability to achieve its objectives, such as engaging the key stakeholders and the wider Internet community. Its acronym-ridden hierarchy of committees, Assistant Groups and Supporting Organisations which are operated by an uneasy coalition of private sector interest groups, under the umbrella of the DoC with the increasing involvement of the wider Internet community has led to criticism that its structure is unduly complex and that it should be tailored to a more narrow role of the technical management of the Internet.

Notwithstanding its attempts to engage full participation in its activities, ICANN is also still hampered in its efforts to reform due to the long-standing arguments which are raised by some members of the Internet community that ICANN does not have a legitimate basis from which to be responsible for the operation of the Internet. In some circles, it is perceived that ICANN derives its authority from the U.S. government through the MOU which, it is argued, is not a legitimate basis from which to be responsible for the management of the Internet. It is difficult for ICANN to overcome these assertions and its success in persuading the wider Internet community that it is the right organisation to be responsible for the technical management of the Internet will, to a large degree, depend on its ability to successfully ensure that it has appropriate mechanisms in place for the Internet community to actively participate in its policy making decisions.

The Wider Picture

Whilst ICANN has, over the past 18 months, set itself on a reforming path and has, with varying degrees of success, continued to successfully develop the technical management and co-ordination of the Internet, engaged with its key stakeholders and increased the level of global representation it now faces increasing challenges to its position as the leading Internet governance organisation which may, to an extent, be out of ICANN's control.

The Internet, as the global means of communication and information technologies, is developing at an exponential speed. The convergence between telecommunications, broadcasting multimedia and information and communication technologies is driving the pace of the development of new products and services. Increasingly, governments, businesses and civil organisations from around the world are recognising the importance of the Internet and they all want to ensure that they have a say in its management. However, over the past few years, a digital divide has opened up between the rich countries, which have access to the Internet and the poor countries, whose access to the Internet is much more limited. Developing countries are now pushing for a greater role in managing and developing policies for the Internet. Over the past few years, as the Internet has emerged as a dominant force, the resentment of many members of the international community in relation to the way the Internet is run, under heavy U.S. influence which supports a private sector led Internet, has increased.

In December 2003, the issue of who should have responsibility for the operation of the Internet came to a head at a conference which was held by the World Summit on the Information Society (WSIS). The conference, which was attended by about 60 heads of state and governments and about 12,000 delegates, was aimed at advancing the management and world-wide use of the Internet. However, the key debate at the conference was the governance of the Internet. Many participating countries at the conference supported the creation of a new, more international management of ICANN. The US, backed by the European Union, Japan and Canada rejected a bid by developing nations to place the Internet under the control of the U.N. or its member governments.

Whilst discussion about the role of ICANN and the governance of the Internet threatened to derail the conference, following discussions, negotiators side-stepped their differences by agreeing to set up a U.N. group which would study possible new ways of running the Internet which would report back in 2005 at the next WSIS conference which is due to be held in Tunisia. 2004 is, therefore, plainly going to be a critical year for ICANN.

