WORLD INTERNET LAW REPORT

Volume 4, Issue 8 August 2003

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

BNA International Inc., London

INTERNATIONAL INFORMATION FOR INTERNATIONAL BUSINESS

WORLD INTERNET LAW REPORT

Publishing Director: **Deborah Hicks**
Editorial Director: **Joel Kolko**

Editor: **Nichola Dawson**

Production Manager: **Nitesh Vaghadia**

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 £595; Eurozone €975; U.S. and Canada U.S.$995. Web version (standard licence): £695/€1125/$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. Reproduction of this publication by any means, including facsimile transmission, without the express permission of The Bureau of National Affairs, Inc. is prohibited except as follows:

1) Subscribers may reproduce, for local internal distribution only, the highlights, topical summary and table of contents pages unless those pages are sold separately;

2) Subscribers who have registered with the Copyright Clearance Center and who pay the $1.00 per page per copy fee may reproduce portions of this publication, but not entire issues. The Copyright Clearance Center is located at 222 Rosewood Drive, Danvers, Massachusetts (USA) 01923; tel. (508) 750-8400. Permission to reproduce BNA material otherwise may be obtained by calling (202) 452-4471; fax (202) 452-4084.

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

We are pleased to open this August issue of *World Internet Law Report* with a new Review section, in which we intend to feature occasional reviews of relevant publications we hope will be of interest to readers. This month, we include a review of the *PLC E-Commerce Practice Manual*, written by international law firm, Baker & McKenzie.

Our thanks go to Prof. Chris Reed (head of the Centre for Commercial Law Studies at Queen Mary University of London and Counsel to Tite & Lewis) for his work in reviewing this extensive and detailed title.

Our commentaries and case reports this month cover a wide variety of topics. Carl Rohsler of Norton Rose opens the E-Commerce section of the journal with an article on the themes and dissonances involved in gambling on the Internet. The article offers a view of the legal issues involved and the implications for international trade and the international e-gambling industry.

An important new standard exempting operators and users of computer networks from liability, has been set by the recent U.S. Court of Appeals decision in *Batzel v. Cremers*. Coverage of the case and further comment is provided by D. James Nahikian of the Avendia Law Group in Chicgao.

Our article from Alan Steele-Nicholson, a Partner and Head of the TMT Department of Simmons & Simmons Trenité, takes a look at how law firms are using websites and the required codes of conduct for lawyers in several European jurisdictions.

Please contact me with your comments and feedback at nicholad@bna.com, or on tel. (+44) (0)20 7559 4807.

Nichola J. Dawson

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

Axel Freiherr von dem Bussche, Taylor Wessing, Düsseldorf; *Nicola Finegold*, Lovells, London; *Elizabeth Levinson* and *Natalie Ceola*, Freehills, Melbourne; *D. James Nahikian,* Avendia Law Group, Ltd., Chicago; *Alan Steele-Nicholson, Jaap Bremer* and *Marta Borrat i Frigola*, Simmons & Simmons Trenité, Rotterdam; *Mouammar Oozeer*, Office of the Mauritian Attorney General; *Riccardo Roversi,* Studio Legale Abbatescianni, Milan & Rome; *Prof. Chris Reed,* Centre for Commercial Law Studies, Queen Mary University of London; *Sandeep Parekh,* P.H. Parekh & Co, New Delhi; *Carl Rohsler,* Norton Rose, London; *Richard Venerus*, Allstream; Subramaniam Vutha, Subramaniam Vutha & Associates, Mumbai; *Katie Withers,* Eversheds, Manchester.

REVIEW

Books

PLC E-Commerce Practice Manual

By Baker & McKenzie

Published by the Practical Law Company, London, December 2002. Edited by Roger Wesson.

ISBN 1 899461 18 3. Price: £475.

Reviewed by Chris Reed, Professor of Electronic Commerce Law, Centre for Commercial Law Studies, Queen Mary University of London. Of Counsel to Tite & Lewis.

This is a substantial work, both in size and content. It is what its title conveys; a two-volume, A4 looseleaf manual covering the main aspects of the law relating to e-commerce. Volume 1 comprises seven sections: How the Internet works; Access to the Internet; Domain names; Setting up and operating a website – Contractual issues; Liability for website content; and Data protection and privacy. Volume 2 consists of the following eight sections: Making contracts online; Electronic data interchange; Security and digital signatures; Payment on the Internet; Enforcement of rights; Telecommunications; and E-mail and Internet use at work. All of these contain useful information for the e-commerce lawyer, with the possible exception of the Telecommunications section. This has specialist appeal, concentrating as it does on telecommunications licensing. It is unlikely therefore, to be used by the typical e-commerce lawyer advising a client undertaking activities in the general sphere.

The final two sections contain a number of precedents with commentary and checklists for selected activities.

Although the *E-Commerce Practice Manual* does not include a foreword or introduction outlining its aims and target audience, the latter is reasonably obvious from its contents. The audience appears to be those advising on the law relating to e-commerce, whether in-house or as external legal advisers. Both would find it useful. This review perhaps can be most helpful by describing the work's approach and suggesting how that audience might use it.

In the reviewer's opinion there are three ways in which a work on e-commerce law could be written:

- A conceptual analysis of the legal issues involved, drawing examples from as wide a range of sources as possible and attempting to produce a synthesis which, while not completely accurate for any particular jurisdiction, aims to provide the reader with a deep understanding and conceptual framework into which national law details can be fitted. This type of work is traditionally undertaken by academics and alone is insufficient when advising a client on a specific problem.
- A detailed description of all the laws relevant to e-commerce, in all the countries where an online business might conduct its activities.
- A blend of the first and second approaches, offering some conceptual analysis with details of selected topics in selected jurisdictions. This is how Baker & McKenzie have produced the *E-Commerce Practice Manual*.

Five of the sections: How the Internet Works, Access to the Internet, Setting up and operating a website – Contractual issues, Electronic data interchange and E-mail and Internet use at work, are practice-related essays. The remaining sections adopt a different format. Each begins with Practice notes, a conceptual analysis of the issues involved, which occupies 20-30 percent of the section. The remainder of the section consists of 14 country questionnaires, in each case for Australia, Belgium, Brazil, Canada, France, Germany, Italy, Japan, the Netherlands, Singapore, Spain, Sweden, the United Kingdom and the United States. The reader is thus able to see how a particular issue is treated in each of these countries.

The reasons for choosing these 14 countries are not given, and perhaps Brazil is not necessarily representative of Latin America, nor Singapore of the Southeast Asia "tiger" economies. However, each is a substantial world trading country in its region. The biggest country omissions are Russia and China, both of which are dealt with extensively on the Baker & McKenzie website and could presumably have been included (see *www.bmck.com/ecommerce/intlegis-t.htm* which covers 51 countries, treating U.S. state and federal as one, plus sections on the European Union, OECD and UNCITRAL). It may have been helpful for the manual to include a separate, detailed section on E.U. e-commerce legislation rather than making reference to it in the introductory parts of each country section, where some repetition is inevitable.

The authors and editor of the *E-Commerce Practice Manual* most likely did not intend readers to work through both volumes systematically. Instead, faced with an issue on which advice is required, the user will turn to the relevant section, digest the introduction, and then read the country replies to the questions which have a bearing on that issue. The remainder of this review adopts the same approach, looking in more detail at two sections of the *Manual*. It concludes with an assessment of the extent to which the assumed target audience will

find the *Manual* helpful in giving that advice, and some more general comments on the rest of the book.

The first section examined is "Domain names". My hypothetical client had just acquired a new brand via an acquisition, and wished to register domain names in all 14 countries. In some of these countries, identical or similar domain names were already registered. The question was, how much assistance did the *Manual* give me in framing my advice?

The Practice notes, which form the first part of this section, are extremely good. The author takes us through the development of the domain name system to the present rules governing its operation. This is an approach which some practitioners might feel forces them to read irrelevant information, but in fact one obtains a deeper understanding of the current rules (and thus gives better advice) by discovering what has been rejected or superseded. From the Practice notes, it would be easy to prepare an advice note to the client explaining the overall constraints in registering names and opposing existing registrations, and advise on names registered in the gTLDs such as .com. The country questionnaires gave very detailed answers, and the questions covered all the issues that arose in respect of my client. From this information, it is possible to explain how to register and with whom, and whether there were any practicable routes to attempt to overturn existing registrations. It was also clear where it would be necessary to take more detailed local advice and what questions would need to be put to the local lawyer.

The second section to be examined was Payment on the Internet. For the purpose of evaluating this section, a second client was invented whose online activities included an online payment service. The client wished to know whether the service could be offered in the 14 countries and if so how it would be regulated. The Practice notes here were less helpful. The explanation of the E-Money Directive was not detailed enough to enable me to decide whether it applied to my client's problem. The country questionnaires were very short and gave brief and general answers, which took me no further, though the U.K. section was more detailed. The Belgian questionnaire stated surprisingly that there were no real e-money technologies in use there, but made no mention of the Proton system which was certainly operational in 2001 and is currently one of the largest e-money schemes in Europe. I would have difficulty advising my client based on the content of this section.

The most successful Practice notes elements of the *Manual* were those which attempted to analyse the information in the country questionnaires and put it in the wider context. This is important when one is attempting to give a preliminary view on some aspect of a foreign country's law, prior to seeking more detail from local lawyers. Because every lawyer's training in his or her home country colours the view of foreign legal provisions, it is most helpful to be given an indication of how those laws fit into the more general legal regime in that jurisdiction. The "Domain names" section does this particularly well, and would be a good model for updates and revisions to the other sections.

How useful then, is the hybrid approach of the *E-Commerce Practice Manual*? The answer is that it succeeds for the majority of sections. Using these, an in-house lawyer or external adviser could produce a preliminary report which gave a reasonable overview of the legal effects of an online business's global activities (with a major caveat for Russia and China, each of which is likely to treat some issues in quite a different way from any of the 14 countries for which detailed information is given). In most cases, the salient issues in the 14 countries could be identified and a brief prepared for local advice.

Keeping such a work up-to-date will be a challenging task. Updates are apparently available via *www.practicallaw.com* but as the reviewer had no access to these, no comment is possible.

Overall, the positive aspects of this book substantially outweigh the negatives. If the updating issue is addressed adequately via the website, the *Manual* is certainly worth buying for anyone practising in this field. The process of assembling a work of this size and scope must have been immense, and the editors are to be congratulated.

Editor's Note: The entire E-Commerce Manual is also available online through the Practical Law Company (www.practicallaw.com) as part of the PLC Global Counsel Web service, or the PLC Law Department service. From October 2003, the Manual will also be available as part of a new PLC IP & IT service. The Manual will be updated annually, with the first update scheduled for March 2004.

08/03 Copyright © 2003 The Bureau of National Affairs, Inc. WILR ISSN 1468-4438

COMPETITION

Case Report

EUROPEAN UNION

LEADING ISP FINED FOR ABUSE OF DOMINANT POSITION

On July 16, 2003 the European Commission adopted a decision against Wanadoo Interactive, a subsidiary of France Telecom, for violating E.U. competition rules. Wanadoo Interactive was found to have abused a dominant position in the form of predatory pricing in ASDL- based Internet access services, which provide high-speed Internet access using a telephone line. A fine of EUR10,35 million has been imposed, which reflects the gravity of the abuse and the length of time over which it was committed.

Background

This decision is the culmination of a Commission investigation started in September 2001, from which it emerged that the prices charged by Wanadoo's prices were well below variable costs until August 2001. After that period they were approximately equal to variable costs, but significantly below total costs. The Commission considers that the abuse began in March 2001, when the mass marketing of Wanadoo's ADSL services began. It was clear that Wanadoo's policy was deliberate, as it was designed to take the main share of a booming market despite the level of losses that Wanadoo incurred in the early stages of the policy.

As a result, Wanadoo's market penetration increased significantly. Meanwhile, the level of losses required in order to compete with Wanadoo had a dissuasive effect on competitors. Consequently, market entry was restricted and, at the end of the period where the abuse was committed, no competitor held more than 10 percent of the market.

The abuse ended when France Telecom began to charge wholesale prices in October 2002. Since then high-speed Internet access in France has been growing more rapidly and in a more balanced manner.

Legal Issues

The principal legal issue was to determine whether Wanadoo's actions constituted an abuse in the form of predatory pricing, according to Community case law established in *Akzo v. Commission* [1991] (Case C-62/86 ECR-I-3359). It was held that Wanadoo's actions satisfied the necessary tests that where variable costs are not covered, an abuse is automatically presumed, and where variable costs are covered, and total costs are not, the pricing constitutes an abuse if it forms part of a plan to eliminate competitors.

Comment

This decision builds upon the decision of May 21, 2003 where the Commission fined Deutsche Telekom for the process it charged for access to the local loop.

These two decisions demonstrate the hard line taken by the Commission against practices designed to capture strategic markets. It is interesting to note that, although the abuse was no longer continuing, nonetheless the Commission felt that it was important to adopt a decision against Wanadoo. This was justified by the risk of the abuse being repeated, which reflects the Commission's role in preventing, as well as in certain circumstances sanctioning, abuses of dominant positions.

By Nicola Finegold, Lovells, London.

E-COMMERCE

Internet Gambling – Worldwide Themes and Dissonances

By Carl Rohsler, a lawyer specialising in Internet gambling at International law firm Norton Rose. Mr Rohsler may be contacted at: carl.rohsler@nortonrose.com; or on tel: (+44) (0) 7793 917 621

The purpose of this article is to give Internet lawyers an introduction to the legal issues which lay behind Internet gambling in its many forms, to chart in broad terms how the industry has developed and to set out the most important factors likely to influence its development in the medium term. In taking on such wide terms of reference, it has been necessary to simplify and generalise – but it is hoped that this paper will provide a useful first point of reference for those wanting to know more about this highly regulated and very fast changing area of e-commerce.

Some Definitions

Human imagination has devised a huge number of permutations of forms of gambling entertainment over the years, but they can broadly be categorised as follows:

Gambling: a generic term for betting gaming, lotteries or other entertainments where one wins a valuable prize as a result of an outcome based somewhat on chance.

Betting: a bet occurs where two or more individuals stake a valuable consideration on a future uncertain event. There are many forms of betting, the two most common being fixed odds (where one may win a multiple of the stake and have the stake returned) "pool", or "pari mutuel" bets, where the amount to be won is not fixed but based upon the total amount staked by all players.

Gaming: is the playing of a game of chance for winnings in money or money's worth. Games which are based both on chance and skill will still fall within the definition, but athletic sports games or contests of pure skill are usually excluded. The dividing line between betting and gaming is a blurred one. However, betting which takes place in the context of or incidental to a game, normally falls within the definition of gaming.

Lotteries: These are entertainments involving the division of prizes between players who have paid for the chance to win the prize.

Broad Legal Concepts

Gambling is restricted and regulated in almost all jurisdictions. In some, it is banned altogether on religious or moral grounds. Where legal, regulation is normally most relaxed for free prize draws (*i.e.*, lotteries, but where the players do not pay to enter). Betting tends to come next, with gaming and lotteries the most restricted forms of gambling. This is partly because of the perceived social harm which can result from addiction (gaming is normally considered more likely to result in addiction or severe losses than betting) and also because lotteries are the most prone to state ownership, and therefore generating revenue which governments are keen to monopolise.

One of the few common features of gambling laws worldwide is that, in almost every jurisdiction (except, for example, Nevada and Monaco), gambling debts and credit tendered for the purposes of gambling are legally unenforceable contracts. The industry operates therefore, on the basis of trust and reputation.

From the philosophical point of view, the United States shares something in common with the European Union. In the United States, the federal government devolves the regulation of gambling down to the level of the state – allowing prevailing religious and moral attitudes within individual states to determine the extent of regulation. In the European Union, gambling is one of those matters which has been subject to the concept of "subsidiarity" – dealing with matters at a level of government which is appropriate to them. In the case of gambling, this means regulation under national laws rather than by European Directives or Regulations. The result is that on both continents, there is a complex mosaic of laws covering the subject. The way in which these philosophical positions impact upon Internet gambling is discussed more fully later.

So far as the rest of the world is concerned, Asian governments generally tend heavily to restrict the channels through which their citizens can gamble (notwithstanding that gambling is perhaps more widespread and more intense in Asia than on any other continent). State control in China is, as would be expected, heavy, and both the Malaysian and Taiwanese authorities are stepping up measures to restrict gambling channels. In Hong Kong and Macau, there are virtual state monopolies. Australia and New Zealand, once tipped as the parodyme of the liberal regulation model, have been forced to rethink their models which in some case caused state to compete with each other to hand out licences and which, on the basis of some studies, appears to have led to a growth in problem gambling. This in turn led the government to create a 12-month moratorium on Internet gambling between 2000 and 2001. Since July 2001, the Interactive Gambling Act has been in place, banning the provision of gaming services to Australian citizens, but still allowing the provision and advertising of betting on sporting events.

So where is regulated Internet gambling flourishing? The answer is that it is still alive and well in the Tropical islands was where it was borne. Antigua, Curacao and

the Dominican Republic have all been favoured destinations, offering operators low tax, and a generally lower level of regulation than first world jurisdictions. They are still favoured by a number of casinos and bookmakers, but other jurisdictions have quickly sprung up to compete in terms of regulatory framework, fiscal policy, accessibility and technological infrastructure. There are currently over 50 jurisdictions offering some form of Internet gambling licence and, of these, some (such as Gibraltar and the Isle of Man) are generally considered well regulated, offering a limited number of licences to those who can demonstrate sufficient liquidity and financial probity.

How Internet Gaming Operates

In order to understand where the difficulties in gambling regulation arise, it is necessary to recap on the way in which such transactions operate. Assume, therefore, that a player (sitting at home, say in London) links to a website run by a company whose place of business and servers are located in Antigua and where it is properly licensed by the government there. The player has established an account with the casino, and has either wired or used a credit or debit card to send cleared funds to his account. The establishment of the account usually requires verification of the identity of the gambler including location, status and age). The gambler is able to interact with the gambling server either to place bets or to game with an electronic random number generator. Winnings and losses are credited or debited to the account, and funds can be wired back to the player's bank account. One final issue remains, however, how does the player come to know of the location of the casino in the first place? The answer may be that he used a search engine, or clicked on a banner ad – but it also may be that the casino has advertised its existence in the media within the jurisdiction where the player is located.

The Key Question of Jurisdiction

It always eventually, comes down to the issue of jurisdiction. No matter what the precise terms of national statutes, the primary question in assessing risk is whether they should apply at all. In the model discussed above, some of the activities take place in London, and some in Antigua. The question, then, is has a sufficient part of the overall activity taken place in the United Kingdom such as to allow the English authorities to regulate the gaming?

So far as the English Courts are concerned, the general consensus is that the location of any offence relating to gaming is to be judged on the basis of the so-called "last act" test. This provides that unless the last act constituting the *actus reus* of the offence takes place within the jurisdiction, the offence will not be justifiable by the U.K. courts. In the above example, the view taken is that the receipt of the player's instruction, or the operation of the random number generator in determining the result, is the point at which the last act in "playing the game" takes place. For betting, the receipt and acceptance of the bet is considered to be the last act. Consequently, neither the casino nor the player are committing a criminal offence within England. The conduct, of course, is legal in Antigua, where it is licensed by the government.

Issues often arise, however, in relation to the advertising of gambling. Many legislatures (including the United Kingdom) control the ability for gambling operations to advertise. In this case, the *actus reus* of the offence may be completed simply by placing the advertisement where it will be viewed by the relevant public – in the case of a newspaper advertisement, the last act will have been completed in the United Kingdom. There is still, of course, the issue of effectively summonsing a foreign company to appear before the English courts. However, that is a matter of practicality rather than principle – and it usually possible to find someone within the jurisdiction (in this case the newspaper) who can effectively be made responsible for the offence.

Not all countries operate the same tests of jurisdiction. In the famous case of *People v. World Interactive Gaming Corporation*,[1] the New York Judge held that

> "The act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within the New York state".

That is to say, it was the location of the *gambler* and not of the gambling operation which was key to establishing jurisdiction.

In Germany, a slightly more moderate point of view has been adopted, but the effect is much the same. The Court of Appeal of Hamburg[2] considered that the operation of the casino *www.goldenjackpot.com* amounted to a criminal offence of illegal gambling simply because a player could select a German language version of the website in question. The judge held:

> "The fact that the game was not operated on German soil or exclusively for German users but on the basis of an English homepage over the Internet does not change the situation. All games of chance carried out in Germany require permission from the German authorities. In this context, we do not need to decide whether any Internet casino which is accessible over the world wide web is carried out in Germany. This is due to the fact that the Internet casino in issue has directly targeted the German market by means of the German version which could be chosen on their homepage."

The French Courts, too, take a wide approach to jurisdictional issues on the Internet as evidenced by the famous "Yahoo" case.[3] In that litigation the French Court found that it had jurisdiction against Yahoo on the basis that one of its auction sites offered Nazi memorabilia for sale (contrary to French law), notwithstanding that the site in question operated from the United States (where such behaviour was not a criminal offence).

From this brief survey of jurisdiction, it becomes immediately apparent that jurisdiction becomes the central question in the assessment of the legality (and commercial risk) of gaming services. Such cases demonstrate also the stark choices which gambling operators currently face, and the fact that they may unwittingly fall within a jurisdiction, even if they take some steps to exclude players from certain countries.

Back to Philosophies – Gambling as International Trade

As mentioned above, both the European Union and the United States have a "constitutional" obligation to ensure that each state or Member State is able effectively to legislate for gambling within its state as it sees fit. But such principles also have to fit with issues of freedom to trade. In the United States, the foundation of the framework as far as gambling is concerned was created under the terms of the Wire Act 1961, which was intended to prohibit gambling across interstate lines. Decisions in the Louisiana Federal Court appear to have restricted the applicability of the Wire Act to betting rather than gaming, but it still forms the basis of a number of prosecutions. In the European Union, free movement of goods and services between Member States is of course, governed by the Treaty of Rome. However Member States have a significant ability to derogate from this principle and impede the free provision of services, provided that the restrictive measurements are:

- not-discriminatory;
- justified by reasons general interest and;
- proportional and necessary to achieve the objectives pursued.

Both systems have recently been placed in the spotlight as a result of cases brought by Internet gamblers.

For example, the Antigua and Barbudan government have recently applied to the Dispute Settlement Body of the World Trade Organisation to establish a panel to examine its dispute with the U.S. Government over the provision of cross-border gambling services. The Antiguan authorities contend that certain aspects of the policy of central and local government in the United States are

> "inconsistent with the United States' commitments and obligations under the General Agreement on Trade in Services (GATS) with respect to the cross-border supply of gambling and betting services".

In particular, Antigua points to the disparity between the total prohibition on the provision of gambling services offered from outside, when seen in the context of legislation allowing gambling which has been passed at both the U.S. Federal level and state level. The Antiguan government also cites the restriction of international transfers and payments relating to gambling and betting services offered from outside the United States as a further cause for action.

In the European Union, the recent opinion of Advocate General Alber in the case of *Criminal proceedings against Piergiorgio Gambelli and Others*,[4] has thrown into doubt whether governments can prevent the existence of cross-border betting. In this case, the Italian authorities prosecuted Gambelli (and a number of other individuals and companies) for running data transfer operations between Italian citizens and a British bookmaker. The Advocate General held that Italian laws prohibiting a bookmaker from operating in the jurisdiction were framed in an openly discriminatory manner and were more than was necessary for the protection of consumers and social order, particularly given that the laws of the state of origin of the bookmaker already provided a sufficient guarantee of integrity. Of course, it is possible that the Advocate General's opinion will be overturned by the European Court of Justice when they make their final determination – but it provides a useful indication of how the freedom of trade argument can work against national regulation in a powerful way.

Divergent Pasts, Divergent Futures

Given what has already been said, it is hardly surprising that different countries have remarkably divergent views on the future of Internet gambling. In the United Kingdom, online betting is already commonplace, and a Royal Commission Report on Internet Gambling has proposed that e-casinos be licensed and regulated.[5] Those proposals are currently the subject of a White Paper and Government Draft Bill[6] aimed at wholesale liberalisation of the gambling market. By contrast, in the United States, there are various legislative attempts to hamstring the international e-gambling industry by preventing the use of credit cards and other financial instruments to operate Internet gambling.[7] The anti-gambling lobby is not unopposed,[8] but has recently been enjoying a considerable boost as a result of fears that Internet casinos may be used to launder the proceeds of crime or fund international terrorism. The threat to ban the use of credit cards has, in fact, already partially been put into place as a result of government pressure on card issuers not to allow their cards to be used for gambling transactions. Credit card operators can generally tell when a card has been used for a gambling transactions as a result of transaction codings (so-called "7995") which arise when a card is used for depositing money with a gambling site. Since the United States still represents just over half of the world online gambling market, there is a significant incentive to create alternative (and perhaps more anonymous) mechanisms for depositing money. It is a moot point, therefore, whether such attempts to prohibit gambling transactions actually help or hinder the struggle against organised crime.

Regulatory changes continue to rock the industry, and it is too early to say whether the prohibition model or the regulatory one will win through. All that is clear is that the battles between the industry and regulators will continue and that the industry will continue to buck global economic trends, despite the best efforts of many governments to restrict its availability. It is

difficult to see how the continuing rise of a significant new industry, with new types of customers, new freedoms and new social problems can be held back in any meaningful way.

1 No. 404428/98 (Sup. Ct. N.Y. Cty., July 22, 1999).
2 Judgment of November 4, 1999.
3 TGI Paris, May 22, 2000.
4 European Court of Justice: Case C-243/01.
5 The Report of the Gambling Review Body, chaired by Sir Alan Budd.
6 White Paper: "A Safe Bet for Success" Draft Bill: "Modernising Britain's Gambling Laws". Cm5878
7 Unlawful Internet Gambling Funding Prohibition Act H.R.2143.RFS.
8 For example, see the bill introduced in March 2003 to the House of Representatives by Congressman Conyers (HR 1223).

Law Firms' Websites in Certain European Jurisdictions: Advertising Rules and the Unauthorised Practice of Law

By Alan Steele-Nicholson Partner and Head, TMT Department, Simmons & Simmons Trenité, Rotterdam, The Netherlands. These remarks are adapted from a speech prepared for the Computer Law Association congress, held in Washington, D.C. during May 2003. The author expresses his gratitude for the assistance of Mr. Jaap Bremer and Ms. Marta Borrat i Frigola, lawyers at Simmons & Simmons Trenité, Rotterdam, The Netherlands.

The author can be contacted by telephone on:+31 (0)10 404-2111, or by e-mail at: alan.steelenicholson@simmons-simmons.com.

Introduction

Nowadays, every self-respecting law firm has established a website. These websites can be used for many purposes. Some law firms, mostly small ones, only use them as a means to provide very basic information regarding the firm, such as address details and a brief description of the areas of law that are practiced. Larger law firms usually provide much more information through their website. Besides the most basic information, most of them provide a résumé and legal experience of individual lawyers, and, in the case of British and American law firms, this is usually accompanied by a list of the lawyer's major cases. Some firms even provide access to legal content by means of hyperlinks to other websites or databases.

The conclusions provided in the following article derive from a comparative study of the advocates/lawyers' rules of conduct of four European jurisdictions: the Netherlands, Germany, the United Kingdom and France.

A common denominator in all these jurisdictions is that the deontological codes for lawyers had to be accommodated to a new medium, the Internet, in which these professionals can also deploy their legal activities or advertise their services in addition to the traditional methods. It has been said that, "lawyers are using web pages to solicit class-action plaintiffs, participate in real-time chat forums, conduct computer-mediated dispute resolution, bid for legal engagements, and many other uses".[1]

To combat the impunity that the Internet provides to many of the activities that are conducted in this medium, a number of mechanisms are being put in place by states and associations (*i.e.*, European directives on telecommunications, e-commerce, privacy, codes of conduct of associations, *etc.*). Such activities have begun to receive the attention of Bar Associations of several countries with one purpose: the guarantees provided in the off-line world should also apply to the online sphere.

The following paragraphs will deal with the codes of conduct for lawyers in the jurisdictions mentioned above. The codes ensure that the legal profession also maintains good ethical standards on the Internet.

Unauthorised Practice of Law

One of the consequences of lawyers' making extensive use of the Internet is the fact that it enhances the possibilities for malpractice and the practice of law by intruders. The fact that websites are accessible from any given location may lead to confusion amongst users. For instance, legal aid websites in Spanish may refer to Chilean or Argentinean law and not to Spanish law. It is difficult for a user to know whether the relevant articles or legislation refer to what is being sought.

Addressing this problem, the 1998 version of the Code of Conduct for Lawyers in the European Union[2] (as well as various other codes for national Bars in Europe) stipulated in this regard that:

> "Advertising and personal publicity shall be regarded as taking place where it is permitted, if the lawyer concerned shows that it was placed for the purpose of reaching clients or potential clients located where such advertising or personal publicity is permitted and its communication elsewhere is incidental".

Law firms making use of a website should therefore, clearly indicate to which group of people the website is directed. This requires careful wording of the content of the site.

Most websites do not contain warnings on each web page that the content on that page is only intended for people within a certain jurisdiction, *e.g.*, the Netherlands. Arguably, a website should be assumed to comply with the above section of the European Code of Conduct if the website has been arranged in a clear and unambiguous way, if it contains links to country-specific web pages and if it contains a clear and easy-to-reach list of national contact persons. Meeting these requirements would seem to minimise the risk of creating the false impression that a certain lawyer is authorised to practice in a (foreign) jurisdiction.

Based upon the above, bar associations should introduce specific guidelines in their codes of conduct with regard to the use of websites by lawyers, *e.g.,* regarding the kinds of disclaimers or warnings that should be stated in each website to avoid confusion (for instance, that the information is only valid for those matters connected to the law of a given country, or that the information downloaded from a legal website cannot be relied upon unless previously discussed with a qualified lawyer).

Another problem is the relative ease of erecting a website and claiming to be able to provide (free) legal advice. Consumers should be warned about these kinds of activities and always consult a specialist before relying on the information of such websites. Unfortunately, the Internet is a medium whereby unscrupulous individuals may rather easily pretend to be qualified lawyers and so offer advice under false pretenses (presumably for a fee). It can also occur that an advocate or law firm may create the impression that it is willing and able to provide legal advice in a jurisdiction in which it is not licensed to practice. This raises the problems mentioned above of the unauthorised practice of law.

Generally speaking, lawyers in the European Union are permitted to establish themselves in a jurisdiction within the European Union in which they have not (yet) become admitted. This has resulted from European Directive 98/5 (which was implemented into the Dutch Code for the Practice of Law (the "*Advocatenwet*") in 2002). Such lawyers, however, can only practice law under their "home title". This means that a British solicitor is allowed to practice law in the Netherlands, as long as he clearly indicates that he is a solicitor and not a Dutch "attorney" ("*advocaat*").

Each country provides for its own criminal law mechanisms to combat the unauthorised practice of law. In the Netherlands, for instance, this is prohibited under section 436 of the Dutch Criminal Code.

This paper does not deal extensively with criminal law, nor will it discuss the remedies in civil law that one may employ in claiming damages from the conduct just described. The topic of this paper is purely "ethics on the Internet" and will focus exclusively on the ethical rules that a number of bar associations have incorporated in their deontological codes, with regard to the use of the Internet by the legal profession.

The Netherlands

Advertising

Law firms in the Netherlands regularly promote their services through websites.

The current version of the Code of Conduct for Lawyers in the European Union (of which the Dutch bar is a member) gives the general permission for a lawyer "to inform the public about his services provided that the information is accurate and not misleading, and respectful of the obligation of confidentiality and other core values of the profession" (Art. 2.6.1). Article 2.6.2. makes explicit that this rule applies, *inter alia*, to "electronic commercial communications or otherwise".[3]

The previous version of the European Code (1998) simply referred the lawyer back to the rules applicable in his or her national jurisdiction.[4]

There is also no express guidance regarding electronic promotional material in the rules of the Dutch National Bar Association (*Nederlandse Orde van Advocaten* or *NOvA*) (the "Dutch Bar"). The Dutch Bar has adopted a regulation that specifically applies to publicity.[5] This regulation stipulates that a Dutch lawyer, or "advocate" is in principle permitted to seek publicity, unless the regulations explicitly prohibits it. The Regulation, however, is silent regarding the types of media that the advocate may use for promotional purposes, and thus one assumes that he/she can do so by means of a website.

The general rule in the Netherlands is that an advocate must ensure that the publicity, whether created by him or herself or someone else, is in accordance with the care that may be expected from a member of the legal profession and that such publicity does not violate the relation of mutual understanding and trust among lawyers.[6]

The Regulations deal further with more specific aspects. An advocate is, for instance, not permitted to compare his/her services to those of other individual advocates.[7] In most cases, advertising by an advocate comparing services to those of specific colleagues will not be permitted considering the fact that the threshold for permissibility of comparative advertising is very high in the Netherlands. One might argue, therefore, that the inclusion of this rule in the above-mentioned Regulation is superfluous.

It is permitted, however, to compare one's services to those of other advocates in general, or other groups of advocates, as long as they are not mentioned by name.

In practice, law firms do not use their website to promote themselves at the cost of (specific) competitors. Therefore, this rule does not pose major concerns for current legal practice.

Furthermore, an advocate is not permitted directly and individually to approach possible clients, unless it is done in writing.[8] It seems clear enough, however, that the advertising done by law firms via their websites does not constitute an individual approaching potential clients. One might even argue (although less convincingly) that the use of a website does not constitute an approach in written form.

An advocate is only permitted to promote the fact that he/she has specialist expertise in certain areas (of the law) if this is apparent on the basis of his/her acquired experience and knowledge.[9] The burden of proof in this regard is on the advocate claiming to have specialist expertise in a certain area.

Law firms and individual advocates should therefore, be very aware that they do not exaggerate their specialist expertise. Stretching may result in a breach of the Regulation.

Advocates are not permitted publicly to mention the outcome of cases they have dealt with, nor are they permitted to publish success rates. Details of cases the advocate is currently handling, *inter alia* the identity of the

client and the nature of the case, may only be published with the client's prior consent.

The quality of the advocate's service is not measured by success rates. Publishing cases the advocate has won or the percentage of cases won may be misleading and is therefore prohibited.[10] However, it may be in the interest of the client if the advocate does publicly disclose details of a case being handled. The lawyer's decision should depend on the client's interest and the care that may be expected from a member of the profession.[11]

Publicity regarding an advocate's fee rates is only permitted if it is clear and unambiguous. This means that the publicity should clearly indicate to what services the rates apply and whether the rates include other costs. Any applicable Value Added Tax must be included in the published rates.

As mentioned, an advocate is not allowed to compare his services to those of a colleague. This also, in effect, bars comparing fee rates to those of specifically named colleagues.

Advertising by an advocate may not create the impression that someone other than the advocate is responsible for it.[12] This is meant to prevent the consumer/customer from being mislead. This does not mean, however, that the advocate's employer is not allowed to advertise the advocate's services.

Finally, the advocate is not permitted to publish the fact of a membership of a committee of the national or local bar association.[13] This rule is meant to prevent advocates from becoming members of said committees for the wrong (marketing) reasons.

Nor is the advocate permitted to advertise holding the position of part-time judge or some other court function. By creating this prohibition, the NOvA intended to prevent the impression created by advocates that they would have extra influence with the courts.

Germany

Advertising

This paper's remarks above regarding the European Code of Conduct also apply to the German situation.

The German Code of Conduct for *Rechtsanwälte* (lawyers) also contains a number of provisions on advertising. As some of these provisions correspond with provisions in the Dutch Code of Conduct, this section will only briefly touch on these points.

A *Rechtsanwalt* is allowed to provide information regarding him or herself and the services being offered, as long as the information concerns professional information and relates to the lawyer's business.[14]

In general, when mentioning specific areas of the law, a *Rechtsanwalt* is allowed to indicate areas in which his/her activities are concentrated (to a maximum of three areas) or in which he/she has a special interest, clearly specifying which area falls in which category.[15]

Naming an area of special interest requires the ability to prove specific knowledge in this area through study, experience, publications or otherwise. This requires a minimum of two years' active and substantial experience in the named area. Incidental experience is not sufficient.

In brochures, circulars and related advertising materials, however, the regulations do permit mentioning other areas than those discussed above.[16] The reason for this distinction is not clear. It does seem to imply, assuming that a website would be regarded as "related advertising materials", that there is no limitation on the (number of) areas of law the lawyer is allowed to mention.

A *Rechtsanwalt* is not permitted to advertise success rates or turnover figures. Mentioning a case or a client requires the client's prior, express consent.[17]

If the *Rechtsanwalt* is a qualified mediator, advertising this fact is permitted.[18]

A *Rechtsanwalt* may indicate that he/she practices law in co-operation with other lawyers, or that he/she is a member of a *Sozietät* (partnership).[19]

Rechtsanwälte that have formed a partnership or co-operation with other *Rechtsanwälte* are allowed to act under a common name (*Kurzbezeichnung*). If such law firm has more than one office, all offices are obliged to use the same name. This name may include the names of former partners or employees and it may also contain some brief information with regard to the practice.[20]

The *Rechtsanwalt* is not allowed to co-operate in a specific type of advertisement of his services by a third party, if the rules bar his or her advertising in that way.[21]

The United Kingdom

In the United Kingdom the legal profession comprises solicitors and barristers. The solicitors' deontological codes were not changed specifically with regard to website promotions and the like. Such promotions are caught by the language pertaining to publicity, which, in general, follows the European rules prohibiting false and misleading advertising.[22]

The code for barristers[23] was indeed adapted to the use of e-mail, websites and use of the Internet. The guidelines established in the code of conduct of the Bar Council of England & Wales offer an overview of the issues with which every barrister is confronted when sending an e-mail, advertises his or her services through the web or even provides advice through the web. These rules contain a specific paragraph about Internet publishing.[24] In particular these rules distinguish between four types of Internet publishing by barristers:

> "(i) information about Chambers, *e.g.,* on a Chambers' website;
>
> (ii) information about individual members of chambers;
>
> (iii) legal information in the form of books, articles, lecture transcripts or notes, case and statute commentaries and updates and procedural guidelines;

(iv) advice – generic, specific or interactive advice.

These may be published on the Internet by:

(a) open access, with or without a fee, or

(b) by password access – for a fee or under some other contractual or quasi-contractual arrangements".

In rule 10 the Bar Council highlights a number of issues that should be considered when advertising on the Internet:

In all Internet publishing it is important to consider the following questions:

(i) What is the published material? Is it business information or legal information that is capable of creating a liability for negligent misstatement?

(ii) If the information may be case-specific advice, is the recipient a client? If so is he a solicitor, foreign lawyer or within BarDIRECT?[25]

(iii) Is the activity in compliance with the Code of Conduct? If the activity is giving case-specific advice without a professional retainer it will be in breach of the Code.

(iv) Is the activity covered by BMIF?[26] BMIF does not cover liabilities arising out of legal authorship, and activities outside the scope of the Code may not be covered by BMIF as part of the Insured Practice.

(v) If the material constitutes advertising, does it comply with the Code, and is it legal, decent honest and truthful?"

The Bar Council warns that information posted on the Internet is available to anyone who chooses to access it, not just to U.K. barristers or solicitors who are familiar with the nature of chambers and should therefore carry an appropriate caveat:

"Chambers' publications are regarded as marketing. The web enables Chambers' publications to be available not just to English solicitors who are familiar with the concept of a set of barristers' chambers, but to the whole world - most people are unaware of the nature of a set of chambers. It is therefore very important to ensure that Chambers cannot be perceived by members of the public (or commercial entities) to be offering legal services or advice on which they can rely to order their affairs.[27]

A Chambers' website, or other Internet dissemination of information about Chambers should therefore explain:

(i) the legal status of Chambers;

(ii) the fact that services are provided by the members of chambers as individuals;

(iii) that the services of a barrister may only be obtained through solicitors, foreign lawyers, the BarDIRECT scheme or where Direct Professional Access applies.

(iv) if any page accessed through the website includes any articles, case notes or other legal information, as opposed to merely business information such as is found in the legal service directories, then it should include a disclaimer".

Rule 12 refers to Individual Barrister's websites and stresses that:

"The crucial point is that a Barrister may only give advice to a professional client; the guidance above in relation to a Chambers website applies. If he or she advises a person who is not a professional client as defined by the Code of Conduct he or she will be in breach of the Code. Hitherto the publication by a barrister of legal information, case summaries or commentaries or other legal authorship has tended to be indirect, through a legal publisher in an article or book. Internet publishing creates a direct relationship with the individual recipient.[28]

Conventional legal authorship falls outside the scope of "Legal Services" as defined by the Code, and any liability arising therefrom is not covered by BMIF. Care must be taken to ensure that any such authorship cannot give rise to the assumption of responsibility towards the reader. If any legal information given on a website could be taken to be advice – for example a commentary which gives examples which may be similar to an accessor's case – then a disclaimer such as suggested above should be used".

In connection with the linked websites, the Bar Council points out that if Chambers' or individual barrister's website may be accessed through a link (for example from a firm of solicitors), care should be taken to ensure that liability to that site visitor (for example the solicitor's client) is not created. (It is also contrary to the Code to take money for a referral, or introduction fee, which may arise from a link).

The Bar Council also describes three example situations to which English barristers should pay special attention:

"(i) A CPR alerting service.[29] A Barrister might have a personal website with a password area giving an alerting service on new developments, cases etc with commentary on the CPR. Because it is 'passworded' he knows who uses it and sends them e-mail updates. If he did this through a conventional publisher they would charge for it, and pay him a fee as an author. If the consumers are not professional clients and are able to interact so as to receive advice on specific issues, then this would be in breach of the Code. Moreover, if a fee is charged to access the site then a contractual relationship is created which may attract stricter liability rules than a negligence claim, and it is unlikely that any disclaimer would assist. If the information is incomplete, inaccurate or out of date this may give rise to a claim in relation to which the barrister may wish to arrange insurance as an author, independently of his cover with BMIF.

(ii) A questioning interactive website. A barrister may have an interactive website which asks questions of the person entering the site. A general advice is provided at the end of the session,

depending on the answers given by the individual accessing the site. This is very likely to be case specific, and therefore in breach of the Code.

(iii) Bank Internet service with legal advice. A bank offers a subscription Internet service where subscribers have an account. Part of the material is legal information written by barristers who write a synopsis and a detailed guide. The synopsis is free, but when the detailed guide is downloaded the bank collects a fee, part of which is passed on to the Barrister author. If this is advice and not to a professional client, then it is in breach of the Code. There will also be a contractual liability to the Bank if it is sued by the consumer. In both cases claims may fall outside the scope of BMIF cover".

All this is without prejudice of honoring the general rules on advertising and publicity set forth in Article 710.1 and following of the Code of Conduct of the Bar Council.[30] Barristers may engage in any advertising or promotion in connection with his practice which conforms to the British Codes of Advertising and Sales Promotion and such advertising or promotion may include:

"(a) photographs or other illustrations of the barrister;

(b) statements of rates and methods of charging;

(c) statements about the nature and extent of the barrister's services;

(d) information about any case in which the barrister has appeared (including the name of any client for whom the barrister acted) where such information has already become publicly available or, where it has not already become publicly available, with the express prior written consent of the lay client."

According to Article 710.2, an advertising promotion must not:

"(a) be inaccurate or likely to mislead;

(b) be likely to diminish public confidence in the legal profession or the administration of justice or otherwise bring the legal profession into disrepute;

(c) make direct comparisons in terms of quality with or criticisms of other identifiable persons (whether they be barristers or members of any other profession);

(d) include statements about the barrister's success rate;

(e) indicate or imply any willingness to accept instructions or any intention to restrict the persons from whom instructions may be accepted otherwise than in accordance with this Code;

(f) be so frequent or obtrusive as to cause annoyance to those to whom it is directed."

France

France, and in particular the Paris Bar association ("Barreau de Paris"), has also issued new guidelines with regard to the advertising of the legal profession and contains one provision that explicitly refers to advertising legal services through the Internet.

French lawyers are prohibited from engaging in certain types of advertising. There is a distinction between *publicité fonctionnelle* (functional publicity) that refers to the publicity the object of which is to inform about the legal profession and *publicité personnelle* (personal publicity). The latter is allowed to the extent that it provides to the public "necessary information".[31]

In France, certain marketing activities are not allowed. In particular, Rule 10.2 prohibits door-to-door selling (*démarchage*)[32] and soliciting (*sollicitation*).[33] The activities here described refer to the offer of services and the "personalised rendering of services performed by any means of distance communication", including over a website.

Publicity with a view to provide advice, draft legal acts by way of letters, posters, films, radio or television is also forbidden.

The following marketing activities are not forbidden:

- organisation of seminars and the like; and
- participation of lawyers in professional fairs.

The French deonthologic code contains very specific directions on what can be printed on the firm's stationary, plaques and so forth and these might also be applied to the firm's website.

Announcements (including press releases) may only be the object of punctual and technical information such as lawyers moving from one location to another; the venue of a new associate; the participation to an authorised group; or the opening of a secondary office (branch).

The rules on information that may be published in brochures are also applicable with regard to publicity through the Internet. Rule 10.11 deals specifically with this issue: This type of publicity must conform the prescriptions of Article 161 of the decree dated November 27, 1991, and decree no. 72-785 of August 25, 1972. Any lawyer who intends to set up an Internet page must inform the Bar Association, including information about the references of the site and how to access it.

Contents of the website: (the code refers here to the contents of the brochures): the code distinguishes between compulsory information, authorised information and prohibited information.

Compulsory information: the site should contain all the information that is required to be mentioned in the letter paper and any other useful information with regard to presenting the activity of the firm.

Authorised information: the site may refer to the years of experience of the firm's lawyers; the internal organisation of the firm; the professional activities of the firm; foreign languages spoken; fees and how they are fixed; if prior consent has been obtained. The site may also refer to lawyers that regularly and significantly contribute to the firm's practice; teaching activities of lawyers, lists of secondary offices and partners abroad (see rule 10.8).

Prohibited information: the site may not refer to names of clients, however the rule on brochures provides for an exception which is that clients having provided their

prior consent may be made public in foreign countries where disclosing clients' names is allowed. In addition, the site may not refer to activities which are not linked to the professional activities of the firm.

Conclusion

As noted here, a number of lawyers' associations have already adapted their rules of conduct for the Internet. The degree of thoroughness of each of these regulations varies one to another. This variation underscores the dangers of relying (exclusively) on information plucked from the Internet when seeking legal advice or advice for consumers.

Apart from the limitations described above with regard to the information about lawyers and the firms themselves, in general there are no boundaries as to the nature of the content that a law firm may post on its Internet website other than the identification of the lawyers, expertise, and so forth.

What should be clear is that the use of proper warnings and guidelines for consumers and potential clients at such websites should become standard practice.

1 Westermeier, J T, *Ethics and the Internet*, 2003, p. 1.
2 Code of Conduct for Lawyers in the European Union, originally adopted October 28, 1988, amended November 28, 1998 (and later amended December 6, 2002), Art. 2.6.1, *www.ccbe.org/doc/En/code_en.pdf* (European Code).
3 European Code (2002), Art. 2.6.1, *www.ccbe.org/doc/En/code2002_en.pdf*.
4 See footnote 2.
5 "*Verordening op de Publiciteit*", November 25, 1988, last amended September 14, 2001 ("Dutch regulation"), *www.advocatenorde.nl/index.html*.
6 Dutch Regulation, section 2.
7 Dutch Regulation, section 3.
8 Dutch Regulation, section 4.
9 Dutch Regulation, section 5.
10 Dutch Regulation, section 6.
11 Dutch Regulation, section 2.
12 Dutch Regulation, section 9.
13 Dutch Regulation, section 12.
14 German Code of Conduct for Lawyers, para 6(1), *www.brak.de/seiten/01.php*, ("German Regulation").
15 German Regulation, para 7(1).
16 German Regulation, para 6(2).
17 German Regulation, para 6(3).
18 German Regulation, para 7a.
19 German Regulation, para 8.
20 German Regulation, para 9.
21 German Regulation, para 6(4).
22 See "The Guide to the Professional Conduct of Solicitors" (eighth ed. 1999, and as amended thereafter) at *www.guide-online.lawsociety.org.uk/*. A section in the online guide entitled "Ethics and IT" is indicated as not yet being available.
23 The 'Bar Council' is the regulatory and representative body for barristers in England and Wales. It deals with the qualification and conduct rules governing barristers and those wishing to become barristers. Those rules of conduct are codified in the Code of Conduct of the Bar of England and Wales (7th Edition) and its Annexes ("Barristers' Code"). The Code implements the Access to Justice Act 1999 and includes the extension of full rights of audience to employed barristers and changes to the Pupillage Regulations. See, *www.barcouncil.org.uk/text.asp?404; www.barcouncil.org.uk/2003/111/document.asp*.
24 Barristers' Code, Rule 9 of Guidance on E-Mail Security, Websites and Use of the Internet, published in *www.barcouncil.org.uk* (as accessed on July 28, 2003).
25 BarDIRECT is a scheme whereby organisations or individuals who are suitable to instruct barristers because they have particular areas of legal expertise can apply to the Bar Council to be licensed to instruct barristers directly in those areas. See, *www.barcouncil.org.uk/document.asp?languageid=1&documentid=208*.
26 The Bar Mutual Indemnity Fund Ltd., a company established by the Bar Council. Barristers are required to have a specified amount of professional indemnity insurance, which this company provides.
27 *www.barcouncil.org.uk/document.asp?documentid=917&languageid=1&highlight=Internet*, Rule 11.
28 *www.barcouncil.org.uk/document.asp?documentid=917&languageid=1&highlight=Internet*, Rule 12.
29 CPR refers to the Chambers Performance Report.
30 Barristers' Code, Pt. VII, Art. 710 *et seq*.
31 Code of Conduct, Paris Bar, p. 25, Rule 10.1 ("*Règlement Intérieur du Barreau de Paris*", *http://195.212.162.216/public/profession/RIHP_vigueur_030408.PDF*, hereinafter "Paris Bar Code").
32 "*Tout acte de démarchage ou de sollicitation est interdit à l'avocat*" (Rule 10.2, Paris Bar Code). Door-to-door selling is understood here as offering an advocate's services principally by approaching possible clients personally or sending someone else to their domicile, where they work, or in any public place.
33 Soliciting is defined as a personalised proposition of lawyer services, effected by a lawyer without having been previously invited to do so. See footnote 32.

The Impact of New Technologies on Business in India

By Sandeep Parekh, a Partner at P.H. Parekh & Co, New Delhi, India. Mr Parekh is admitted to practice in New York and New Delhi and is a visiting faculty at the Indian Institute of Management, Ahmedabad.

The positive impact of Information Technology on the world economy hardly needs to be stated. Technologies have streamlined processes, improved communications and have been instrumental in dis-intermediating intermediaries in the chain of trade and services. For instance, with the use of dematerialised shares in India, an entire industry which processed transfers of shares and debentures has been rendered dysfunctional. Today, shares, debentures and exchange-traded derivatives are traded and transferred instantaneously, without the use of physical papers. The risk of loss or theft is low, with virtually no requirement for an intermediary, except for a depository and an electronic exchange. Living in India over the past decade, it has been exciting to see the country rapidly adopting and using technology to its advantage. India's edge in software and back office leadership worldwide has been possible in spite of, and not because of the legal regime in the early 1990s.

The use of old laws in the changing face of technology sometimes produces amusing results and often, disastrous implications. For instance, the 1872 Indian

Contract Act ("ICA") does not even envisage a telex or a telephone as a means of communication. Court made law has often stepped in to avert obvious absurdities as would result from applying old law to a new scenario. For instance, the application of the common law postbox rule to telephonic contracts created such absurdities that the courts stepped in to make the postbox rule inapplicable to phone based contracts.[1] The use of telephones in the first half of the century did not spur the legislature to enact amendments to various statutes, but the use of more contemporary technology has resulted in the passing of the Information Technology Act, 2000 ("the Act", "IT Act" or "ITA") which *inter alia* deals with various new modes of proof, evidence and contracts. The Act has been timely in helping to reduce the large gap between commercial reality and the law.

Scope of the IT Act: Extra-territorial Effects

Under Article 246 of the Constitution, Indian laws may have extra-territorial effect. The Act extends itself to offences committed outside India and by virtue of the Article would withstand a challenge of unconstitutionality. Thus Indian courts, constitutionally, have the power to enforce the application of the Act even if the party committing an offence resides outside India, or if the offence is committed outside the territorial limits of India but has some iota of connection with India or Indian residents.

When an Electronic Contract is Complete

The Act only prescribes the time when a document is deemed to be dispatched or received. It does not specifically deal with when exactly the acceptance is complete. This gives rise to the question of whether the use of e-mail is a form of instantaneous communication similar to the use of the telephone, or is it more akin to the use of regular mail? E-mails *usually* reach the recipient instantaneously. However, it is not unusual for an e-mail to take several hours to reach the addressee. This poses a peculiar problem, since until now "modern" technology was either instantaneous or not, *i.e.*, not a mixture of the two. The postbox rule was essentially inserted into the Contract Act as a reflection of the common law rule of convenience, that it was easier to prove that a letter had been posted and practically impossible to prove that a letter had been received. With the Internet regime, it is possible to track the route and time of an e-mail message; therefore there is no necessity for the rule of convenience to be applied in an e-mail communication. We are of the opinion that since e-mails are in most cases instantaneous communications and it is possible to request an automatic acknowledgement that the mail has been received by the recipient, the law laid down for immediate communication should lead. The acceptance would be complete therefore, when and at the place where, the receiver receives the message. *Chitty's* on Contracts[2] asserts that

> "the effects of unsuccessful attempts to communicate should depend on whether the sender of the message knows (or has the means of knowing) at once of any failure in communication".

The other issue that arises is, can an acceptance be complete even though a message never reaches the offeror? There can be three answers to this question:

- First, when the system (of the sender, the receiver or a third party Internet Service Provider (ISP) fails to deliver the e-mail to the recipient. In such a case, as argued above, the contract would not have been completed. This view is reinforced if the acceptor uses an acknowledgment request available with most e-mail programs.[3]
- Secondly, an e-mail address is not delivered because the acceptor typed in the wrong address. The law is well established on the point, and the acceptor cannot rely on his own mistake to allege a completed contract.
- The third scenario poses a problem however, and that is where the offerer himself provides a wrong e-mail address to the acceptor. Under the law as pronounced for postal communications, when the offerer himself provides a wrong address, the acceptor's communication will bind the offerer. The law should not be different for e-mail. Where the acceptor is under notice that the e-mail did not reach the intended recipient, he should not be permitted to bind the offeror. For example, where the acceptor sends an e-mail to the wrong address provided by the offeror and the e-mail bounces back or if the person who receives it writes saying that the mail was wrongly sent to him, then the acceptor should not be able to bind the offeror to the contract.

Also at issue would be whether actual receipt is determinative or not. As in the example of a telex, a message is taken to have been received by the addressee when the message is received by the telex machine and not when the addressee's attention is drawn to it. However the issue is settled by the express words of the IT Act, which prescribes the time when a message is deemed to have been received.[4]

Determining the Place of Contract

When dealing with international contracts, one more issue beside the time of the contract must be determined and that is the place of the contract. This gains significance in view of the fact that under international law, the law of the place where the contract was signed may govern future disputes. To answer this question, one would need to go back to *when* the contract was completed. The place of contract would be determined by the time of the contract. Thus to determine the place, one would need to analyse the time and simply note the place when the contract became valid and binding.

Digital Signatures

A digital signature is an electronic algorithm or formula applied to a message or electronic record. It is not an unalterable code attached to the end of a document. A digital signature is actually a formula, which will change the original document with a "key" so that it

may be read only with the help of another "key". Without the help of the second key it is impossible to read the document. Further, if any alteration is attempted on the signed document, the document loses its seal of digital signature, therefore making it tamper-proof. The two keys used are provided by a Certifying Authority, which provides the digital certificate. The Certifying Authority is in turn regulated by a Controller of Certifying Authorities, which is a government body set up under the Act.

However, messages attached with digital signatures need to be proved unless they are attached with *secure* digital signatures.[5]

For a digital signature to be secure it must:[6]

- be unique to the person using it;
- have capacity to identify such person;
- be in the exclusive control of the sender; and
- linked to the record/document in such manner that any alteration would render the certificate invalid.

Once it satisfies these conditions, the digital signature is considered "secure".

The presumptions created when a digital signature is secure are:

- that the person who is purporting to send the message is the actual sender; and
- that the message sent has not been tampered with. The digital signature therefore, authenticates and binds the person sending the message to a contract or obligation.[7]

> **"Presumptions as to electronic records and digital signatures**
>
> **85B**.[8] (1) In any proceedings involving a secure electronic record, the court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.
>
> (2) In any proceedings, involving secure digital signature, the court shall presume unless the contrary is proved that:
>
> (a) the secure digital signature is affixed by the person who will sign or approve the electronic record;
>
> (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or a digital signature".

Implications for International Contracts

The Act only envisages a certifying authority certified with the Indian government. This is obviously a part of the Act, which does not contemplate international contracts and is unfortunately inward looking. Even if international contracts were contemplated, the legislature refused to give its *imprimatur* to all certifying authorities worldwide. This makes foreign digital signature not attracting the presumptions of the Act. However, the foreign digital signatures would be valid – they would just need to be proved in a court of law as being 'secure'.

E-mail Messages

Similarly, an e-mail message is ordinarily presumed to be received in the same condition as it is sent without there being a presumption as to the sender's identity unless the e-mail is sent with a digital signature.

> **"Presumptions as to electronic messages**
>
> **88A**.[9] The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed, corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent."

This provision is similar to the presumption under the Evidence Act for a telegraph.

> **"88**. The Court may presume that a message, forwarded from a telegraph office to the person to whom such message purports to be addressed, corresponds with a message delivered for transmission at the office from which the message purports to be sent; but the Court shall not make any presumption as to the person by whom such message was delivered for transmission."

Encryption

Encryption is usually effected by the use of public keys and private keys, using a method not dissimilar to the one used in a digital signature. These keys are nothing but mathematical algorithms. Each user has a pair of these, a private one, which is confidential and a public one, which is open to other users. Thus when a sender sends the message he will encrypt the message with the receiver's public key. Then the message can be decrypted by the receiver using his private key. If any other persons intercept the message he will only be able to read junk characters. It is thus a means of sending documents which only the intended recipient can read.

Difference between Digital Signatures and Encryption

The chief difference between a digital signature and an encrypted message is that a message which uses a digital signature can be read by any person but cannot be tampered with (both as to origin and substance of the document); a message which uses encryption cannot be read by any person except the intended recipient but provides no guarantee of its origin. Of course it is possible to use both technologies together and get the benefit of both.

The flip side of the problem is that anti-national persons may send messages to each other using encryption technology and these messages cannot be read by the police agencies of the government. The IT Act therefore provides for making all private keys

available to the government. However, most keys are not generated by Indian companies and therefore, the regulation is really not effective unless it is co-ordinated across countries.

Original Document

An electronic record which accurately reproduces the original will be admissible as the original if the terms mentioned in Section 65B of the Evidence Act, as modified by the IT Act, are satisfied.

The law also creates a presumption as to records over five years old, which are affixed with digital signatures.

> **"Presumptions as to electronic records five years old**
>
> **90A**. Where any electronic record purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him on his behalf.
>
> Explanation: Electronic records are said to be in proper custody if they are in the place in which and under the care of the person with whom they naturally belong; but no custody is improper if it is proved to have had a legitimate origin, or in the circumstances of the particular case are such as to render such an origin probable."

The Problem of Originality

The word 'original' is alien in cyberspace because a duplicate is as good as the original. Therefore, it would be easy to duplicate records or electronic forms of money. Such duplicated records or money would be indistinguishable from the original making it difficult to establish that one is original, and the other is not.

Conclusion

The Indian law has progressed substantially in the field of Information Technology. However, the law needs to be altered a little to accommodate recognition of reputed foreign Certifying Authorities. Though little case law has developed since the passing of the Act in the fields of evidence and contracts, IP related cases have mushroomed under the provisions of the Act. Thus one will need to wait until either some case law is developed in the field, or until the legislature amends the Act to accommodate more international transactions.

1 See *Bhagwandas v. Girdharilal* (1966) 1 SCR 656.
2 H.G. Beale, Chitty on Contracts, Sweet & Maxwell, *28th Ed, Vol 1*.
3 MS Outlook, Netscape Messenger and Eudora mail support e-mail acknowledgement. However services like Hotmail and Yahoo do not yet have this feature available.
4 See above at "When is an offer made?"
5 Section 67A, Indian Evidence Act.
6 Section 15.
7 Section 85B.
8 All references to sections in this part of the paper refer to the relevant sections of the Indian Evidence Act.
9 Indian Evidence Act.

A Practical Guide to the New Information Duties for E-Commerce in Germany

By Dr. Axel Freiherr von dem Bussche, Taylor Wessing, Düsseldorf. The author may be contacted on tel.: +49 211 8387-284; or at: e-mail: a.bussche@wessing.com

Introduction

Since the beginning of 2002, all companies offering Internet services have been required to comply with new information duties. The new duties were introduced to protect the Internet user, as well as to enhance the legal and economic framework of e-commerce in Europe. The information duties were implemented by conversion of Directive 2000/31/EC ("the E-Commerce Directive")[1] into German Law at the end of 2002 and are now part of various German statutes. The most relevant information duties are implemented in the Teleservices Act *(Teledienstegesetz TDG)* and in section 312(e) of the German Civil Code *(Bürgerliches Gesetzbuch BGB)*.

These information duties are relevant for e-commerce contracts, mailing lists, online-banking and also for the running of a company's homepage. Thus, every company established in Germany with a homepage has to comply with the new rules; failure to do so means a possible fine of up to EUR50.000.

The following article provides a practical guide for those companies required to make changes but which have yet to make the necessary amendments.

Teleservices Act

The purpose of the Teleservices Act is to establish uniform economic conditions for the various applications of electronic information and communication services. The provisions apply to all electronic information and communication services that are designed for the individual use of combinable data such as characters, images, or sounds and are based on transmission by means of telecommunication (teleservices). This includes, in particular, services offered in the field of individual communication (*e.g.*, telebanking, data exchange, web updating services).

Providers of commercial teleservices shall ensure that the following information is given as a minimum requirement:

- the name and address under which they are established; legal persons shall identify their authorised representative,
- information that allows the user rapid electronic contact and direct communication with the provider, including the provider's e-mail address;
- if the teleservice is offered or rendered as part of an activity requiring government licensing, information on the responsible supervisory agency must be provided;
- the commercial register, register of associations, register of partnerships, or public register of co-operatives listing the provider, along with the corresponding registry number;
- to the extent that the teleservice, in the exercise of a profession as defined under Article 1 Letter d of Council Directive 89/48/EEC[2] or as defined in Article 1 Letter f of Council Directive 92/51/EEC,[3] is offered or rendered, information on:
  - (a) the chamber to which the provider belongs;
  - (b) the legal designation of the profession and the country in which the occupational designation was issued;
  - (c) the designation of the professional regulations and how these may be accessed;
- the turnover tax identification number under section 27a of the Turnover Tax Act, if the provider has been assigned such a number.

Further duties to provide information – laid down in the Act on distance selling (*Fernabsatzgesetz*); the Act on distance learning (*Fernunterrichtsschutzgesetz*); the Act on part-time residential rights (*Teilzeit-Wohnrechtegesetz*); the Acts on the Information on Prizes and the Act on the Rules for Prizes, as well as the Ordinance on the Information on Prizes (*Preisangaben- und Preisklauselgesetz und Preisangabenverordnung*); the Act on the Supervison of Insurances (*Versicherungsaufsichtsgesetz*) – remain unaffected although they must still be taken into consideration, especially the Act on distance selling, which requires important information duties to be taken into account for every B2C transaction via Internet.

The information must be easily recognisable, directly accessible, and constantly available. Hence, Internet users will usually find the required information under the click through heading "Impressum" or "company information" accessible from every single page.

The Teleservices Act also stipulates, that providers of commercial communications which constitute a teleservice, for example, a banner, shall fulfil the following conditions as a minimum requirement:

- commercial communications shall be clearly recognisable as such;
- the natural or legal person on whose behalf commercial communications are transmitted must be clearly identifiable;
- promotional offers such as discounts, premiums, and gifts must be clearly identifiable as such and the terms of compliance must be easy to access and clearly and unambiguously outlined;
- contests or sweepstakes of a promotional nature must be clearly recognisable as such and the terms of participation must be easy to access and clearly and unambiguously outlined.

The Teleservices Act also contains important regulations concerning a provider's responsibility (liability) and the newly introduced and controversially debated "Country of Origin Principle", which says that Internet service providers only have to take into account the laws of their country of origin and not the laws of every European Member State in which they offer their services.

Section 312(e) German Civil Code

The new section 312(e) of the German Civil Code provides duties for Internet contracts; for B2C as well as B2B contracts. If a businessperson uses a television or media service for the purpose of concluding a contract for the delivery of goods or the supply of services (electronic contract), he must:

- provide the customer with appropriate, effective and accessible technical means allowing the customer to identify and correct input errors, prior to sending his order;
- in good time before the sending of his order, communicate to the customer clearly and comprehensibly the information specified in the Regulation under Article 241 of the Introductory Act to the Civil Code
- acknowledge to the customer the receipt of his order without undue delay and by electronic means; and
- enable the customer to retrieve and save in reproducible form the conditions of the contract including standard business terms incorporated in it upon conclusion of the contract.

The information duties with respect to the mentioned Regulation under Article 241 of the Introductory Act to the Civil Code, the so-called Regulation of Information Duties (*Informationspflichtenverordnung InfoV*) are also newly introduced. This special regulation requires that a businessperson must inform a customer (both consumer and/or businesspersons):

- about the single technical steps which lead to a conclusion of a contract;
- if the words of the contract will be stored by the businessperson after conclusion of the contract and are accessible to him;
- how he can, with the technical means provided pursuant to section 321(e) para 1, sentence 1, No. 1 of the German Civil Code, find and correct mistakes after entering but before sending an offer;
- about the languages provided for the conclusion of the contract; and
- about all relevant rules of behaviour which the businessman is subject to as well as about the possibility of electronic access to the respective rules.

Finally, as already mentioned the Act on distance selling (Fernabsatzgesetz) requires even more information for B2C contracts. But those information duties

are not newly introduced by the E-Commerce Directive and are therefore, not subject to this guide.

It is not very difficult to comply with these new rules, but many Internet service providers are still unaware of their new duties. Consequently, they are not only risking a fine but also might be subject of an injunction of competitors.

1 Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

2 Council Directive 89/48/EECof December 21, 1988 on a General System for the Recognition of Higher-Education Diplomas Awarded on Completion of Professional Education and Training of at Least Three Years' Duration (Official Journal L 019, p. 16).

3 Council Directive 92/51/EEC of June 18, 1992 on a Second General System for the Recognition of Professional Education and Training to Supplement Directive 89/48/EEC (Official Journal L 209, p. 25) amended most recently by Commission Directive 97/38 EC of June 20, 1997 (Official Journal Nr. 184, p. 31).

News

INDIA

Government Proposes Introduction of Electronic Reporting

The Department of Company Affairs, (DCA) of the Government of India, is proposing to introduce electronic interaction with all companies registered in India and computerisation for its record keeping of their filings with its offices. India's 1956 Companies Act currently requires companies registered under the Act, to file various detailed returns and forms as part of their disclosure obligations. Hard copies of the filings and reports are maintained by the DCA for public inspection at its offices in key locations throughout India. However, each office maintains such records only in relation to the companies that fall within its jurisdiction.

The new system, when introduced and implemented, will enable companies to file their reports and returns electronically. The automation plan, which will be implemented and managed by a private firm on a build-operate-transfer model, is based on plans drawn up by the Government's Department of Information Technology and the National Institute of Smart Governance.

The DCA plans to pay some part of the filing fees accompanying company filings to the private agency concerned, for the management services to be rendered. The DCA currently earns approximately 3000 million Indian Rupees (Rs) per annum from such fees and various services rendered to companies registered under the 1956 Companies Act.

The DCA had originally planned to create a special purpose vehicle with participation by banks and infrastructure finance companies. The current plan for the automation project development and implementation is based on an outsourcing model.

By Subramaniam Vutha, Subramaniam Vutha & Associates, Mumbai

INDIA

Update on the National Internet Exchange

India's key Internet service providers (ISPs) will join the government in forming the National Internet Exchange of India, to facilitate the exchange of Internet traffic among service providers, reducing costs of bandwidth access and allowing quicker access to the net for users (see *World Internet Law Report*, October 2002).

The government plans to provide the initial seed capital of about Rs.50 million. On-going operations of the exchange will be sustained, it is anticipated, by revenues earned by it, from services involving the linking of Indian websites to each other thus providing faster surfing for customers.

The exchange will obviate the current need to route traffic from customers of an Indian ISP seeking to access any other Indian website, through international carriers with servers outside India. Indian ISPs will save on the international bandwidth costs bringing down the down the costs of operations for the ISPs and lowering surfing costs for customers.

The four exchange points planned at the four major cities of Delhi, Mumbai, Chennai and Kolkata will carry inter ISP traffic but will not be permitted to carry any intra ISP traffic.

The new exchange will have an executive board with representatives of the Ministry of Information Technology and industry associations and will be a "not for profit" company under the Indian 1956 Companies Act.

By Subramaniam Vutha, Subramaniam Vutha & Associates, Mumbai

Case Reports

UNITED STATES

■ NEW STANDARD FOR DEFAMATORY/OBSCENE SPEECH

Batzel v. Cremers, No. 01-56380

Court of Appeals, Ninth Circuit, June 24, 2003

In a profound decision with application to business defamation lawsuits and technology usage policies, the U.S. Court of Appeals for the Ninth Circuit articulated a new standard which exempts operators and users of computer networks from liability when the party merely re-transmits defamatory or obscene material with a reasonable belief the author intended to publish the material through a computer network, in *Batzel v. Cremers*, No. 01-56380 (June 24, 2003). This decision also marks a case of first impression under the Communications Decency Act in which the claims arose from a single defamatory e-mail communication that was transmitted in private, moved onto a public listserv and later published without express permission from the author of the communication. For these reasons, *Batzel* is likely to influence future claims that involve the Communications Decency Act.

Batzel is intrinsically noteworthy on its facts. The plaintiff-appellee, an attorney licensed to practice law in California and North Carolina, owns a home in North Carolina which contains "hundreds of older European paintings on [its] walls, all with heavy carved wooden frames." (*Batzel*, at 8432). A handyman, whom the plaintiff-appellee employed to paint a room in the house and repair her truck, suspected "these paintings were looted during WWII and are the rightful legacy of the Jewish people". (*Batzel*, at 8434). He transmitted a private e-mail communication which reported his suspicions, and included plaintiff-appellee's address, to the Museum Security Network in Amsterdam, The Netherlands.

The e-mail communication was received by the head of the Museum Security Network, who operated the organisation's computer networks and also served in a position of authority as Director of the internationally renowned Rijksmuseum in Amsterdam. Hundreds of museum security officials, insurance investigators and law enforcement personnel around the world subscribed to the Museum Security Network website and listserv mailings, relying on the information made available there to assist with investigations of stolen artwork and antiquities. Minor wording changes were made to the message and it was published via the Museum Security Network listserv and website. In addition, the organisation head posted a "moderator's message" which announced the matter had been forwarded to the FBI.

Once the handyman learned his e-mail communication was published, he contacted the organisation head and complained "that if he had thought his e-mail 'message would be posted on an international message board [he] never would have sent it in the first place.'" (*Batzel*, at 8434). In response, the organisation acknowledged "[y]ou were not a subscriber to the list and I believe that you did not realize your message would be forwarded to the mailinglist [sic]." (*Batzel*, at 8434-35). Regardless, publication of the handyman's e-mail communication resulted in the North Carolina Bar Association investigating the plaintiff-appellee and it damaged her personal and professional reputations according to the court documents.

The plaintiff-appellee filed a complaint in the U.S. District Court for the Central District of California in which she alleges the handyman defamed her as retribution for refusing to forward his screenplay to plaintiff-appellee's contacts in Hollywood. She denies the artwork at the house in North Carolina is illicit. The head of the Museum Security Network was named as a defendant and responded with a motion to strike pursuant to Cal. Civ. Proc. Code § 425.16, the California Anti-SLAPP statute ("Strategic Lawsuits Against Public Participation"), arguing the lawsuit lacks merit. The District Court denied this motion, ruling that the plaintiff-appellee was likely to succeed on her claims, in part because the Museum Security Network head did not qualify under the Communications Decency Act, 47 U.S.C. § 230(c), as "an interactive computer service" provider or user which would have exempted him from liability for publishing the handyman's allegedly defamatory e-mail communication through the organisation's listserv and website facilities. The organisation head appealed this decision.

On June 24, 2003, the Ninth Circuit sided with the organisation head. The court vacated the Central District of California order and remanded with instructions for additional proceedings consistent with a new "reasonable belief" standard. Assuming *Batzel* remains undisturbed, the decision will operate to exempt computer network operators and users from civil claims that are based on alleged circulation of defamatory or obscene material if such persons establish they held a reasonable belief the author intended to publish the material to a computer network.

The pertinent statutory text, 47 U.S.C. § 230(c)(1), provides that

> "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". (*Batzel*, at 8441).

The Ninth Circuit determined that § 230(c)(1) should control disposition of all claims against the organisation head, since the Museum Security Network's listserv and website facilities utlized the Internet and thus they comprised an "interactive computer service". It did not matter whether the organisation head actually was a "provider" of the Museum Security Network computer networks, since he certainly had used these facilities at the time he published the allegedly defamatory e-mail communication from the handyman. Accordingly, he was at least a "user of an interactive computer service" and § 230 immunity could obtain.

The Ninth Circuit turned its analysis to the § 230(c)(1) phrase "information provided by another information content provider". (*Batzel*, at 8449). The handyman qualified as an "information content provider," the court ruled, given that he authored the original message, and § 230 defines information content provider broadly as

> "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service", § 230(f)(3).

However, as the Ninth Circuit noted, the Museum Security Network head had modified the original e-mail communication, and this required the court to examine the ultimate message that got published through the organisation listserv to determine which of the parties actually contributed the allegedly defamatory content. The Ninth Circuit decided the issue in favour of the organisation head, observing that a central purpose of the Communications Decency Act "was to protect from liability service providers and users who take some affirmative steps" to review and edit potentially defamatory or obscene material disseminated through computer networks. In addition, the court reasoned

> "[t]he scope of the immunity cannot turn on whether the publisher approaches the selection process as one of inclusion or removal, as the difference is one of method or degree, not substance". (*Batzel*, at 8452).

The Ninth Circuit's § 230(c)(1) analysis gravitated to the term "provided", which the court deemed relevant solely on the basis of the handyman's contention that he had never anticipated his e-mail communication would be published to an international listserv or website. The Ninth Circuit rejected an argument by the Museum Security Network head that the handyman's subjective intention was irrelevant for purposes of § 230 and, therefore, immunity attached automatically once the organisation head retransmitted the handyman's e-mail. The court concluded this interpretation could lead to "nearly limitless immunity for speech never meant to be broadcast over the Internet". (*Batzel*, at 8454). The Ninth Circuit followed with a discussion of the policy underpinnings for the § 230 legislation, observing that "[i]mmunizing providers and users of 'interactive computer service[s]' for publishing material when they have reason to know that the material is not intended for publication [would contravene] the Congressional purpose of encouraging the 'development of the Internet' " since this would tend to chill protected First Amendment speech propagated through computer networks (*Batzel*, at 8455).

To address the issue, the Ninth Circuit articulated its new standard:

> "[A] service provider or user is immune from liability under § 230(c)(1) when a third person or entity that created or developed the information in question furnished it to the provider or user under circumstances in which a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other 'interactive computer service' " (*Batzel*, at 8456).

Then the court remanded the case with instructions for the Central District of California to conduct additional proceedings and determine what the head of the Museum Security Network should have reasonably concluded at the time he received the allegedly defamatory e-mail communication from the handyman. The court ruled that if the organisation head did hold a reasonable belief the handyman transmitted his message with the understanding it might be published through a computer network, then the alleged defamatory content was indeed "provided" within the meaning of § 230, and the organisation head must be found immune from the plaintiff-appellee's civil claims under the Communications Decency Act. In the event no such belief existed, however, the new standard will strip away § 230 immunity and the usual defamation tests control the liability of the organization head.

A lone judge dissented against the majority standard based on his conviction this improvidently will shift the pertinent court analysis away from a publisher's conduct since the standard compels a trier of fact to delve into a publisher's perception of an author's state of mind. The dissenter proposed an alternative § 230(c)(1) standard which, it argues, better conforms with the original legislative intent to foster "self-policing" of computer networks on the part of operators and users. Under this strict proposed standard, the Communications Decency Act only would immunise a publisher if the party "took no active role in selecting the questionable information for publication". (*Batzel*, at 8463). The alternative standard is founded upon a distinction drawn between communications published automatically across a computer network, on the one hand, which should be immunised by § 230 it is urged, and those communications by which the publisher has made a deliberate choice to publish the information irrespective of the means. In support of this proposed standard, the dissenting opinion cited the belief that the majority decision will lead to unpredictable consequences for operators and users of computer networks, who "may not grasp that their tort liability depends on whether they reasonably should have known that the author of a particular communication intended that it be distributed on the Internet". (*Batzel*, at 8462).

In dicta, the majority rejected the alternative § 230 standard, concluding the standard rests upon an artificial and illogical distinction between a publisher's decision to include certain content and its corresponding decision to exclude identical content. Content which was transmitted to an operator or user of a computer network and labelled "for consideration for inclusion on your website" automatically would not qualify as "information provided by another" under § 230(c)(1) in any instance where a receiving party chose to publish it through a computer network. This result, the majority argued, does not square with the original legislative intent for the Communications Decency Act. In turn, however, the dissent criticised this interpretation, advancing a separate legislative analysis, and positing that

"[a] person's decision to disseminate the rankest rumor or most blatant falsehood should not escape legal redress merely because the person chose to disseminate it through the Internet rather than through some other medium", which in certain instances will obtain if a court applies the majority's reasonable intentions standard. (*Batzel*, at 8466).

From corporate counsel's viewpoint, *Batzel* may necessitate rethinking company policies which govern an organisation's computer networks and communications practices. Counsel may, for example, wish to advise management that all sensitive internal communications are to be disseminated solely by hardcopy and with an appropriate legend indicating the communication is "not to be transmitted via computer network". Under *Batzel*, adopting a simple practice such as this may strip away immunities claimed by a disgruntled employee, or by a third party computer operator, in the event that either later redistributes the sensitive content through the Internet. Furthermore, counsel may have to contend with a situation where the organisation is being subjected to defamatory e-mail, listserv or electronic bulletin board attacks, and the emergency court denies temporary injunctive relief because the defamatory communications are being published via a computer network, the company cannot immediately identify the author, and some reasonable basis exists for the accused publisher to have believed the author intended to publish by computer network. Under *Batzel*, a judge would be compelled to grant § 230 immunity to the publisher and deny emergency relief. It remains to be seen whether other circuits will choose to apply the *Batzel* reasonable belief test with future Communications Decency Act claims.

By D. James Nahikian, Avendia Law Group, Ltd., Chicago, Illinois. The author can be contacted by telephone on: tel. +1.312.329.5700; or by e-mail at: jnahikian@avendialaw.com

UNITED STATES

■ ARE DOMAIN NAMES PROPERTY? THE SEX.COM CASE

Controversy surrounds *sex.com*, but not just because of its name or the pornographic content of the site at the address. The saga of *sex.com* has opened up a debate as to whether a domain name is a property right, and in particular, whether a registrar should be liable to pay damages to a registrant if it fails to uphold that right.

The story began in 1994, when, in the fledgling days of the Internet, Gary Kremen spotted a lucrative opportunity to register *sex.com*. The name was registered with Network Solutions, in the name of Kremen's business, Online Classifieds. Convicted fraudster Stephen Cohen subsequently forged a letter from Online Classifieds, which confirmed that *sex.com* should be transferred to Cohen. The letter purportedly authorised Cohen to effect the transfer with Network Solutions because, in spite of its name, "Online" Classifieds did not have an Internet connection. This misnomer was not spotted by Network Solutions, and *sex.com* was transferred to Cohen without further checks being made. Cohen went on to build a highly lucrative online porn empire.

In 1998 Kremen sued Cohen to reclaim the name, and was awarded $65 million in damages, as a reflection of Cohen's profits from the purloined domain name. Cohen fled to Mexico and secreted all his money in off-shore accounts. Despite offering a $50,000 reward to anyone bringing Cohen to justice (which allegedly led to gunfights between Mexican authorities and bounty hunters), Kremen has failed to recover any damages.

As a result, Kremen sued Network Solutions (now known as Verisign) for mishandling the domain name. This tactic was initially dismissed by the courts, but the decision has now been overturned by the federal appeal courts. Kremen argued, unsuccessfully, that Network Solutions had breached an implied contract with him. This argument was dismissed because Kremen had not paid for the name, so no valid contract was formed. Kremen's argument that Network Solutions breached the government contract making Network Solutions the *.com* registrar was also dismissed. That contract did not intend to confer rights to domain name registrants.

However, the court accepted that domain names could be considered to be property rights belonging to the registrants, and that *sex.com* was such a right, which had been wrongfully disposed of by the registrar. The judge said that

> "Exposing Network Solutions to liability when it gives away a registrant's domain name on the basis of a forged letter is no different from holding a corporation liable when it gives away its shares under the same circumstances".

Network Solutions' conduct was found to be unreasonably careless. Policy reasons for finding in favour of registrants, such as stifling the domain name registration system and increasing registration fees, had been relied upon by the district court in its earlier decision. These were rejected by the appeal court, which did not consider that special rules should apply to the regulation of the Internet.

Verisign claimed that the decision, if upheld, heralded the crippling of the Internet. Whilst this overstates its significance and implies that the Internet is inherently unstable, the decision will be crucial to every re-seller of

domain names, affecting the way they handle claims over ownership. However, it needs to be considered in its context. Few, if any, domain names comprised of generic words can be as inherently valuable as *sex.com*. The popularity of pornography on the Internet was anticipated by few in 1994. Had Cohen complied with the judgment, it is also possible that the case against Network Solutions would have been unnecessary. Also, subsequent changes to the registrar's contracts with registrants mean that the decision is unlikely to apply to any other registrant. However, it remains to be seen whether the increased regulatory burden on registrars, and the increased registration fees heralded by Network Solutions will, in fact, be implemented if the decision is upheld.

By Katie Withers, Eversheds; KatieWithers@eversheds.com

DOMAIN NAME DISPUTE RESOLUTION REPORTS

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

PepsiCo, Inc. v. Amilcar Perez Lista d/b/a Cybersor

Domain names: pepsix.com, pepsixxx.com

Dispute resolution provider: WIPO (Case No. D2003-0174)

Panelist: Dimitris Oekonomidis

Identical or confusing similarity: Domain name confusingly similar to registered trademark even with addition of extra letters to end of mark.

Rights or legitimate interests: Failure to submit a response; acceptance of all reasonable allegations and inferences in Complaint as true.

Registration and use in bad faith: Facts which support finding that Respondent does not have a legitimate interest in the domain name are relevant to the inquiry of registration and use in bad faith.

Result: The domain name was ordered transferred.

Decision date: April 22, 2003

Diners Club International Ltd. v. SPS aka DCS aka ADC

Domain names: aboutdinersclub.com, dinersclubsucks.com

Dispute resolution provider: NAF (Case No. FA 0303000149414)

Panelist: Tyrus Atkinson, Jr.

Identical or confusing similarity: Respondent's domain name incorporated trademark in its entirety with the addition of suggestive generic words.

Rights or legitimate interests: Failure to submit a response; all reasonable inferences made by Complainant to be regarded as true.

Registration and use in bad faith: Registration of domain name with prior knowledge of Complainant's famous trademark.

Result: The domain names were ordered transferred.

Decision date: April 21, 2003

Cases cited in decision:

Arthur Guinness Son & Co. (Dublin) Ltd. v. Healy/BOSTH (WIPO Case No. D2001-0026)

Sony Kabushiki Kaisha v. Inja, Kil (WIPO Case No. D2000-1409)

Rollerblade, Inc. v. McCrady (WIPO Case No. D2000-0429)

Do the Hustle, LLC v. Tropic Web (WIPO Case No. D2000-0624)

Vertical Solutions Mgmt, Inc. v. webnet-marketing, inc. (NAF Case No. FA 95095)

Canadian Imperial Bank of Commerce v. D3M Virtual Reality Inc. (eResolution Case No. AF-0336)

Boeing Co. v. Bressi (WIPO Case No. D2000-1164)

Wal-Mart Stores, Inc. v. Stork (WIPO Case No. D2000-0628)

Skipton Bldg Soc'y v. Colman (WIPO Case No. D2000-1217)

Tercent Inc. v. Lee Yi (NAF Case No. FA 139270)

Compagnie de Saint Gobain v. Com-Union Corp. (WIPO Case No. D2000-0020)

Vivendi Universal v. Sallen (WIPO Case No. D2001-1121)

G.D. Searle v. Martin Mktg. (NAF Case No. FA 118277)

Samsonite Corp. v. Colony Holding (NAF Case No. FA 94313)

Victoria's Secret v. Hardin (NAF Case No. FA 96694)

Cruzeiro Licenciamentos Ltda. v. Sallen (WIPO Case No. D2000-0715)

Educ. Testing Serv. v. TOEFL (WIPO Case No. D2000-0044)

E. & J. Gallo Winery v. Hanna Law Firm (WIPO Case No. D2000-0615)

Phat Fashions LLC v. Kruger (NAF Case No. 96193)

Alitalia-Linee Aeree Italiane S.p.A. v. Colour Digital (WIPO Case No. D2000-1260)

Australian Airlines Limited, Qantas Airways Limited and AAL Aviation v. Joint Adventure

Domain name: australianairlines.com

Dispute resolution provider: WIPO (Case No. D2003-140)

Panelist: David Perkins

Identical or confusing similarity: Domain name identical to registered trademark.

Rights or legitimate interests: Failure to demonstrate rights and legitimate interests in domain name.

Registration and use in bad faith: Attempt to sell domain name; no possibility to conceive of any use of the domain name that would not be illegitimate.

Result: The domain name was ordered transferred.

Decision date: April 22, 2003

Cases cited in decision:

Telstra Corp. Ltd. v. Nuclear Marshmallows (WIPO Case No. D2000-0003)

Westfield Corp. Inc. v. Hobbs (WIPO Case No. D2000-0227)

Harrods Limited v. Coupon Corporation Inc.

Domain name: harrodscoupons.com

Dispute resolution provider: WIPO (Case No. D2003-0105)

Panelist: Keith Gymer

Identical or confusing similarity: Addition of purely descriptive term to registered trademark implied association with Complainant.

Rights or legitimate interests: No submissions to justify claim to legitimate use; no legitimate non-commercial or fair use of domain name found.

Registration and use in bad faith: Registration for purposes of taking unfair advantage of famous mark.

Result: The domain name was ordered transferred.

Decision date: April 14, 2003

Cases cited in decision:

Harrods Ltd. v. Wieczorek (WIPO Case No. DTV2001-0024)

Harrods Ltd. v. AB Kohler & Co. (WIPO Case No. D2001-0544)

Harrods Ltd. v. Harrod's Closet (WIPO Case No. D2001-1027)

Harrods Ltd. v. Vineet Singh (WIPO Case No. D2001-1162)

British Telecommunications Plc v. One in a Million Limited [1998] 4 All ER 476 (CA)

United States Olympic Comm. v. MIC (WIPO Case No. D2000-0189)

Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale (WIPO Case No. D2000-0662)

Harrods Ltd. v. Pierre (WIPO Case No. D2001-0456)

Ansell Healthcare Products Inc. v. Australian Therapeutics Supplies Pty Ltd. (WIPO Case No. D2001-0110)

Christie's Inc. v. Tiffany's Jewelry Auction Inc. (WIPO Case No. D2001-0075)

Arthur Guinness Son & Co. (Dublin) Ltd. v. Steel Vertigogo (WIPO Case No. D2001-0020)

Veuve Clicquot Ponsardin, Maison Fondée en 1772 v. The Polygenix Group Co. (WIPO Case No. D2000-0163)

Arturo Salice S.p.A. v. Izzo & Co. (WIPO Case No. D2000-0537)

Petland, Inc. v. COM.sortium, LLC (WIPO Case No. D2001-0430)

Feinstein v. PAWS Video Productions (WIPO Case No. D2000-0880)

Empresa Brasileira de Telecomunicações S.A.–Embratel v. McCarthy (WIPO Case No. D2000-0164)

Cellular One Group v. Brien (WIPO Case No. D2000-0028)

British Telecommunications plc and Others v. One in a Million Ltd. and Others, CA [1999] ETMR 61

Quiksilver Inc. v. Official Site Builders

Domain name: veronicakay.com

Dispute Resolution Provider: NAF (Case No. FA0303000147308)

Panelist: Carolyn Marks Johnson

Identical or confusing similarity: Individual can hold common law rights in his/her name if a reputation is established; no common law rights held by Complainant in its name.

Rights and legitimate interests: No legitimate non-commercial or fair use of domain name.

Registration and use in bad faith: Registration of famous trademark was for the purpose of taking unfair advantage of the famous mark.

Result: The domain name is to remain with Respondent.

Decision date: April 16, 2003

Cases cited in decision:

TotalFinaElf E&P USA, Inc. v. Farnes (NAF Case No. 117028)

Estate of Tupac Shakur v. Shakur Info Page (eResolution Case No. AF-0346)

Lush Ltd. v. Lush Environs (NAF Case No. 96217)

PRL USA Holdings, Inc. v. Polo (WIPO Case No. D2002-0148)

Loris Azzaro BV, SARL v. Asterix & De Vasconcellos (WIPO Case No. D2000-0608)

America Online, Inc. v. Anytime Online Traffic School

Domain names: aoltrafficschool.com, aoldefensivedriving.com, aoldriverimprovement.com

Dispute resolution provider: NAF (Case No. FA0302000146930)

Panelist: Petter Rindforth

Identical or confusing similarity: Domain name incorporated entire mark with addition of descriptive terms that did not add any distinctive features; finding of confusing similarity.

Rights and legitimate interests: Finding of use of domain name in connection with a bona fide offering of services.

Registration and use in bad faith: Failure to prove that domain names were registered and used in bad faith.

Result: The domain names to remain with Respondent.

Decision date: April 11, 2003

Cases cited in decision:

Arthur Guinness Son & Co. (Dublin) Ltd. v. Healy/BOSTH (WIPO Case No. D2001-0026)

Realmark Cape Harbour LLC v. Lewis (WIPO Case No. D2000-1435)

Al-Anon Family Group Headquarters, Inc. v. Reid (WIPO Case No. D2000-0232)

LEGISLATION & GUIDANCE

Mauritius Enacts the Computer Misuse and Cybercrime Act 2003

By Mouammar Oozeer, a practising barrister at the Office of the Mauritian Attorney General. The views of the author in this article are strictly his and do not bind the Attorney General's Office. The author can be contacted at amarooz@intnet.mu

Presently, one of the most important activities in Mauritius is its transformation into a "*cyber island*", an ambitious undertaking but an attainable one. The project began with the Electronic Transactions Act 2000 and on July 15, 2003 the Mauritian National Assembly voted unanimously to pass the Computer Misuse and Cybercrime Act ("the Act").

The Computer Misuse and Cybercrime Act is based on the European Cybercrime Convention 2001. A close reading of the Act also shows that the provisions of the 1990 U.K. Computer Misuse Act and the Singapore Computer Misuse Act have also been taken into account.

Prior to the passing of the Act, the Criminal Code was amended in 1998[1] to provide for the offences of "data protection and security" and "computer misuse". The new Act repeals sections 369 and 369A of the Criminal Code. Nine different computer related offences are created and consequential amendments are made to the offences of "forgery" and "dealing in obscene matter" as contained in the Criminal Code and Criminal Code (Supplementary) Act. Part II of the new Act deals with the new offences.

Section 3 provides that any person who causes a computer system to perform a function, knowing that the access he intends to secure is unauthorised, shall commit an offence. The objective of this section is to dissuade deliberate unauthorised access. It is aimed at insiders who try to access parts of a system where they know they should not be. The word "knowing" is the key element. It will be necessary for the prosecution to establish both the intention of securing access and the knowledge that the access is without authority. Indeed, it would be wrong to seek to catch the person who gains access to a system simply because he or she is careless. From the employers' point of view, it will be advisable that their employees are left in absolutely no doubt about what they are entitled to do. If the employee is authorised, this offence of "unauthorised access" would in no way attempt to penalise him or her, unless he or she has "hacked" into the system of a third party.

Sections 3 and 4 are inter-related. Section 4 deals with the offence of unauthorised access with intent to commit another offence. It is provided that any person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system,[2] with intent to commit an offence under any other enactment, shall commit an offence.[3] The use of the words "under any other enactment" makes it possible to catch the offender who uses a computer system to, for instance, transfer funds which directly or indirectly represent the proceeds of any crime.[4]

Sections 3 and 4 reflect the particular nature of computer crimes and the speed with which crimes involving computers can be carried out. One has in mind the English case of *Re Levin [1997] QB 65*, where the perpetrator used his computing skills to obtain access from his computer in St Petersburg to Citibank's Computer System in New Jersey. This unauthorised access allowed the hacker to monitor customers' accounts and make transfers from their accounts into other bank accounts maintained by an accomplice.

Section 5 deals with the offence of "unauthorised access to and interception of computer service". The Act makes it an offence for any person who, by any means, knowingly secures access to any computer system for the purpose of obtaining a computer service, for instance data processing. "Computer service" is defined in the Act as including data processing and the storage or retrieval of data.

Besides, it is also an offence to intercept a function of a computer system, unless the person acts in accordance with a statutory power, or has obtained the consent of both the person who has sent the data and the intended recipient of the data.

Unauthorised modification of data held in computers or computer storage media is dealt with in Section 6. The section is not intended to cover physical damage to a computer or to disks which would remain within the ambit of Section 369 of the Criminal Code, which deals with "damaging goods and chattels".

Section 7 addresses the offence of "damaging or denying access to a computer system", in computer jargon, "denial of service ('DOS') attacks". Denial of service attacks attempt to overload webservers or Internet Service Providers with automatically generated or artificial messages and thereby deny or reduce legitimate access to the computer system. One would recall that from February 7 to February 9, 2000 a number of major e-commerce companies' websites (*e.g.*, amazon.com, Buy-com, E-Trade) were so inundated with requests for data that the sites' servers were overloaded and could not deal with legitimate requests for information for a number of hours. These DOS attacks were widely reported in the media with some concern.

This kind of attacks leads not only to economic damages but also to intangible damage to reputation. Increasingly companies rely on the availability of their websites for their business and those companies that

depend on it for "just in time" supply are particularly vulnerable. Given the serious consequences which this type of attack might have, a heavy penalty is provided for in the Act. Anyone convicted under that section shall be liable to a fine not exceeding 200,000 rupees to penal servitude not exceeding 20 years.

The offence of "unauthorised disclosure of passwords" is dealt with in Section 8. Where a person discloses a password to another person for a wrongful gain, or for any unlawful purpose where the disclosing party knows that by so doing, prejudice will be caused to a third party, he commits an offence. It was argued during the course of debates at the National Assembly as to whether "mere" disclosure of passwords should be rendered unlawful. Arguably, such an approach is too stringent, as any employee disclosing his password to another colleague so that they might log on to his personal computer to check his incoming e-mails, would be committing an offence.

Section 9 deals on the one hand, with the unlawful possession of devices designed or adapted primarily for the purpose of committing an offence under sections 3 to 8; and on the other hand, with possession of data or programs which can be used in the commission of a crime – one such example would be someone in possession of a "program fraud" to commit electronic fraud.

The offence of electronic fraud is dealt with in section 10 deals. With the advancement in technology, the opportunities for committing economic crimes such as fraud, including credit card fraud are increasing.

Financial institutions face unprecedented threats in the current global environment. The threats faced by financial institutions stem from a variety of factors; one factor being the increasing use of electronic commerce. The increasing interconnectivity of the networks of financial institutions means that they are vulnerable, not only to costly new viruses and worms, but also to economic frauds, like credit card frauds. Only this year, a massive credit card fraud was discovered in Mauritius involving foreigners with the complicity of the local criminals.

Some fraud-related offences are already contained in the Mauritian Criminal Code. Examples are "issuing cheques without provision", "embezzlement", and "swindling". The offence of swindling is a type of fraud in which the gain is obtained by, for instance making use of false pretences. However, there is another type of fraud in which the gain is obtained neither by deception nor false pretence: this is the kind practised on machines. A machine has no mind, so it cannot believe a proposition to be true or false and therefore cannot be deceived. A person who dishonestly obtains a benefit by giving false information to a computer cannot be guilty of any "deception" or "false pretence".

Section 10(a) of the Act provides that any person who fraudulently causes loss of property to another person by any input, alteration, deletion or suppression of data with intent to procure an advantage for himself or another person, commits an offence. With a view to ensuring that all possible manipulations are covered, paragraph (a) is supplemented by the general "act of interference" with the functioning of a computer system. Interference with the functioning of a computer system will cover acts such as hardware manipulations or acts affecting the recording of data or the sequence in which programs are run.

Further, the term "property", is defined as including money, tangibles and intangibles with an economic value. The general intent element of the offence refers to the manipulation or interference, causing loss of property to another person. The offence also requires a specific "fraudulent" intent to gain an advantage for oneself or another.

The offence of "forgery" in the offline world is dealt with in the Criminal Code. The purpose of consequential amendment to the Criminal Code, more specifically by enacting a new section "105A – Electronic document or writing" is to create a parallel offence to the forgery of tangible documents. The relevant sections of the law in the Criminal Code criminalising forgery do not apply to electronically stored data. Manipulations of such data may have the same serious consequences as conventional acts of forgery. A "document or writing" is defined as including "any disc, tape, sound track or other device on or in which data is recorded or stored by mechanical, electronic or other means".

Section 86 of the Criminal Code (Supplementary) Act, which deals with the offence of "Dealing in obscene matter" defines "obscene matter" in relation to "tangibles" only. Subsection (2) defines "obscene matter" as meaning any "obscene writing, drawing, print, painting, printed matter, picture, poster, emblem, photograph, cinematograph film, video tape, slide, or any other obscene object".

The consequential amendment to the Child Protection Act and section 86 of the Criminal Code (Supplementary) Act seeks to remedy deficiencies and "loopholes" which arise primarily as a result of technological developments and advances.

Whilst no precise definition of the term "computer pornography" appears to exist, it might be described as a use of electronic means by which indecent, obscene or pornographic images may be stored, transmitted and viewed. Still photographs, films and videos can all be stored on computer disc, and using current technology, photographic images can be converted into digital form. This process can be reversed so that a photographic image, comparable in quality with the original photograph, can be produced on screen and printed as a physical copy. Material stored in this way can be distributed electronically; or by being recorded on floppy disc or a CD-ROM which can be transported and used on another computer.

It is arguable whether material thus stored can be said to constitute a "photograph" for the purposes of section 86. To remove any doubt, section 86 is amended so that "obscene matter" is defined as including "data stored on a computer disc, or by any other electronic means capable of conversions into a photograph".

In addition to amending the Criminal Code (Supplementary) Act, the Child Protection Act is amended by adding a new section 15. Section 15 of the Child Protection Act criminalises various aspects of the electronic production, procession and distribution of child pornography. Whilst it is a moot point on the international scene as to whether "pornography" is to be rendered illegal; there is a unanimous consensus that "child pornography" is to be considered illegal.

Section 15 is borrowed from U.K. law. It makes it an offence for a person to take, to permit to be taken, to distribute or show, or to have in his possession with a view to its distribution or showing, an indecent image of a child. In order for a person to be charged under section 15, the prosecution must prove the existence of a photograph, that this photograph is of a child and that the photograph is indecent. The word "photograph" is, for the purpose of the Child Protection Act defined as including –

> "(a) the negative as well as the positive version; and
>
> (b) data stored on a computer disc or by other electronic means which is capable of conversion into a photograph".

This makes it clear that data stored, whether on computer disc or by "other electronic means" (which term is wide enough to include CD ROM as well as other technological developments which may take place in the future for storing computer data), can be regarded as a photograph even if not reproduced as the visual image. The term "pseudo-photograph" is intended to deal with composite or "manipulated" photographs.

Whilst it remains necessary to established that the photograph is of a "child", as defined in Section 2 of the Child Protection Act,[6] for pseudo-photographs, it is sufficient if the *predominant* impression conveyed is of a child as defined.

Part III of the Act deals with "Investigations and Procedures". The object of section 11 to 17 of the Act is to obtain data and information for the purpose of criminal investigations or proceedings. All the sections in Part III referred to "investigatory authority" which is defined pursuant to section 2 as meaning the police or any other body lawfully empowered to investigate any offence.

Any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system where there are reasonable grounds to believe that such data is vulnerable to loss or modification.[7] "Data preservation" is considered to be a very important investigative technique in the field of computer crimes, especially those committed through the Internet.

Because computer data is not static, it is easily subject to manipulation. Evidence can be "lost" through careless handling or intentional deletion. Secondly, transmissions through the computer system may contain illegal content, such as viruses, child pornography or evidence of the commission of other offences such as drug offences and money laundering. Indeed, section 56 of the Mauritian Dangerous Drugs Act empowers the Judge in Chambers, upon being satisfied by information on oath that there are reasonable grounds to suspect that an offence has been committed, to issue an access warrant to a police officer. The warrant authorises the police officer to have access to the computer systems used by persons suspected of participation in the offences and to place them under surveillance. A preservation order in the present instance will be very important in assisting the police to gathering evidence for the purpose of criminal investigations and prosecution.

Section 14 of the Act which deals with access, search and seizure for the purposes of investigation, aims at modernising Mauritian criminal procedural law in relation to the search and seizure of tangibles. In the offline world, investigators search recorded data, and seize or physically take away the tangible record. With respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure in the traditional search environment. Data being an intangible form, it can be read with the use of computer equipment – it cannot be seized and taken away as a paper record.

The term "computer system" is defined as meaning a "device or combination of devices, including input and output devices". Section 14 of the Act also concerns the related components of a computer system that can be considered together as forming one distinct computer system (for example, a computer together with its storage devices). Indeed, investigation of computer crimes requires both the search of the computer system and any other related storage medium which is in the neighbourhood of the computer system. Section 2, which defines the term "data" as including "representations of facts, information and concepts held in any removable storage medium", encompasses this situation.

Section 14(2)(d) provides the possibility of rendering data inaccessible. This can include encrypting data or otherwise technologically denying anyone access to the data. This measure can be applied where the data or their content are illegal, such as child pornography. By the term "removal", it is meant that the data is removed or rendered inaccessible, but not destroyed. The perpetrator of the offence is temporarily deprived of the data, pending the outcome of the criminal investigation or proceedings.

Section 15 governs the real time collection and recording of traffic data for the purpose of criminal investigations or proceedings. The collection of traffic data, as opposed to content data is often crucial for the investigation of some offences such as those involving unauthorised access to computer systems, distribution of viruses and child pornography. The Act provides that where the investigatory authority has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under the Act, it may apply for a court order:

> (1) allowing the collection or recording of traffic data, in real time, associated with specified

communications transmitted by means of any computer system; or

(2) compelling a service provider, within its technical capabilities, to –

(a) effect such collection and recording referred to in subsection(1); or

(b) assist the investigatory authority, to effect such collection and recording.

Under section 15, the traffic data concerned must be "associated with specified communications". The investigatory authority is not allowed to go on "fishing expeditions" where criminal activities are hopefully sought to be discovered; as opposed to specific instances of criminal activities. The court order permitting the real-time collection of traffic data must specify the communications to which the "collection or recording of the traffic data" relates.

One peculiar feature of our information and communication technologies legislation, is that no legal obligation is imposed on communication service providers to build in technical capabilities to collect or record traffic data or, to assist the investigatory authority. The service providers are not legally required to acquire or develop new equipment to engage in the costly re-configuration of their systems. However, it is understood that if their systems and their personnel have the existing technical capability, they would be required to take the necessary technical measures.

However, where a service provider does not have the technical ability to collect or record the traffic data, then the investigatory authority can undertake the task itself. The service provider will be obliged to assist the authority to effect such collection and recording.

Section 16 of the Act aims at giving the Judge in Chambers the power to order that any indecent photograph of children which exists in any computer system or in any other information and communication technologies medium, be deleted or destroyed; or to be no longer stored on and made available through the system or medium. The question that arises is whether incriminating materials posted on websites can be subject to such deletion order. It seems that the answer should be in the affirmative. The terms "information and communication technologies" are defined in the Act as meaning

"technologies employed in collecting, storing, using or sending out information and include those involving the use of computers or any telecommunication system".

The Act also provides in Section 17 for the limited use of disclosed data and information. Any data or information obtained in respect of any computer related offences can only be used for a purpose for which it was originally sought. The exceptions to this principle are where the data is sought in accordance with any other enactment or in compliance with an order of a court or Judge.

Finally, the offences relating to indecent photographs of children and computer related offences (excluding the "unauthorised disclosure of password" offence) are made extraditable offences for which extradition can be granted, or obtained under the Extradition Act.

Conclusion

With the forthcoming launch of the Mauritius Online portal and the ongoing work of the eGovernment Task Force, the country sets the objective of working with the private sector to ensure a safe and secure Internet environment for the provision of online public services, electronic commerce and to help build trust in B2C and B2B transactions. Mauritius is not only providing the necessary infrastructure to attract renowned foreign and local investors to its "*cyber island*" programme; but is also putting into place the legal framework required. The Electronic Transactions Act is already in force and a Data Protection Bill will be introduced shortly.

However, enacting legislations is not an end in itself. Organisations that rely on networked computer systems must take proactive steps to identify and remedy their vulnerabilities, rather than wait passively for an attack to occur. Information technology security audit must be an ongoing activity.

1 The Information Technology (Miscellaneous Provisions Act) 1998.

2 A "computer system" is defined as meaning "a device or combination of devices, including input and output devices, but excluding calculators which are not programmable, and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

3 This type of offence is considered as an aggravated offence for it is not 'merely' an 'unauthorised access' offence. The penalty provided is a fine not exceeding 200,000 rupees and a penal servitude for a term not exceeding 20 years.

4 Section 3(1)(b) of the Financial Intelligence and Anti-Money Laundering Act 2002 provides that

(1) Any person who –

(a) …

(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

where he suspects or has reasonable grounds for suspecting that the property is derived or realised, in whole or in part, directly or indirectly from any crime, shall commit an offence.

5 'Child' is defined as 'any unmarried person under the age of 18.'

6 Section 11 of the Computer Misuse and Cybercrime Act 2003.

7 See footnote 2 above.

News

GERMANY

New Youth Protection Law has Implications for the Gaming Industry

Recent changes to youth protection laws in Germany, which come after national pressure for tougher regulations and censorship to protect minors, are set to impact the gaming industry. The move comes following

a national tragedy in April 2003, the so-called "Erfurt massacre", where a pupil at the Johann Gutenberg high school in the town of Erfurt shot dead sixteen people before turning the gun on himself. The pupil was said to be a heavy user of the PC-game "counterstrike" in which players act out the role of terrorist or counter-terrorist and plot assassinations with the aid of virtual firearms.

Legal Situation

At federal level, German Youth Protection law was regulated in the Act to Regulate the Dissemination of Writings and Media Contents Harmful to Young Persons (*Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte, GjSM*) and in the Youth Protection Act (*Jugendschutzgesetz, JÖSchG*). In light of recent technical developments in the field of multimedia, both Acts were considered outdated and were to be summarised in one uniform Youth Protection Act. This Youth Protection Act was officially announced on July 26, 2002 and came into force recently, when the supplementary States Contract was signed on April 1, 2003. The States Contract for Youth Media Protection (*Jugendmedienschutz-Staatsvertrag, JMStV*) also supersedes the individual regulations previously in force in different German states.

The new law distinguishes between telemedia (*Telemedien*) and content carrying media (*Trägermedien*). Telemedia are those media, which can be transferred or are accessible electronically, *e.g.*, online-games. Content carrying media are those which are accessible offline, such as books, CDs, video cassettes, cassettes for PC-games, *etc.* Telemedia are addressed in the States Contract, while content carrying media are regulated at federal level in the new Youth Protection Act.

Implications for the Gaming Industry?

It is important to distinguish between both PC-Games and Online-Games, though both products will be effected by the new Youth Protection Rules.

PC-Games (content carrying media)

The most important change is, that *PC-games now explicitly fall into the scope of the Youth Protection law,* a move which has been long-awaited by youth authorities.

One significant change is for PC-games to be labelled with a minimum age requirement for players. To enable this to work in practice, the law suggests co-operation between the computer games industry and the highest regional authorities (in the same way that the authorities co-operate with the film industry). With respect to online-distribution of PC-games, the respective offer must provide a clear reference to existing labelling.

Furthermore, the Youth Protection Act distinguishes between various levels of regulation:

- Content carrying media, which may have a negative influence (*jugendbeeinträchtigende Trägermedien*) are not allowed for their intended age group.
- Content carrying media, which are likely to endanger youth (*jugendgefährdende Trägermedien*) shall be put on the Official List (*Liste der jugendgefährdenden Medien*) of the Federal Authority for endangering media (*Bundesprüfstelle für jugendgefährdende Medien*) to be subject to various other restrictions and sanctions.
- Content carrying media, which are considered to particularly endanger minors (*schwer jugendgefährdende Trägermedien*) shall not be labelled at all but reported to the criminal prosecutors. Restrictions are already in place in this regard, without the requirement to be on the above-mentioned Official List.

Online Games (Telemedia)

Telemedia, which may have a negative influence on youth (*entwicklungsbeeinträchtigende Angebote*) are also restricted.

- The content provider is responsible for ensuring that children or youth of the respective age group – under usual circumstances – shall not gain access to content, which falls under this classification . The provider can comply with the latter duty with the help of technical restrictions or hourly limitations. The required technical restrictions can be provided by installing a pre-approved youth protection program (all protection programs have to be checked by a special authority and approved ("positive rating").
- Furthermore, there are several kinds of offers which are not permitted to youth (propaganda, pornography *etc.*). New to that list is the prohibition of the "performance of children or youth with unnatural, sexual posture", *e.g.* in fashion advertisements.
- Also, providers of telemedia which are deemed to have a negative influence on or endanger youth must appoint a named person (*Jugendschutzbeauftragter)* who's job it is to be responsible for the firm's youth protection policy. The *Jugendschutzbeauftragter* will act as a contact person for users and as an advisor for the provider, to ensure compliance with the youth protection duties.
- Finally, provider of telemedia must also comply also with the respective age labelling of games or products.

Against this background, both the national and foreign gaming industry with business in Germany will have to comply with the new rules.

By Dr. Axel Freiherr von dem Bussche, Taylor Wessing, Düsseldorf. The author may be contacted on tel.: +49 211 8387-284; or at: e-mail: a.bussche@wessing.com

INDIA

Plans for a Comprehensive Cybercrime Law

The Indian Government has announced that it plans to create a comprehensive law for cybercrimes. This is in anticipation of the increasing use of electronic means in corporate and public governance, e-commerce and education. The development of the new law will

involve consultations between the Ministry of Law & Justice and the Ministries of Defence, Home Affairs, Finance and Communications & Information Technology. The aim is create a legal framework to tackle growing concerns about cybercrimes and threats to national security, commerce and other areas of national significance.

The new law will address apprehensions that India's Information Technology Act 2000 (which recognises electronic documents and digital signatures) does not take into consideration all forms of cybercrime, which is assuming "very sophisticated and menacing forms".

The IT Act provides for penalties for unauthorised access to computer systems, introduction of viruses, damage to computer systems, disruption of computer networks, denial of access, wrongfully diverting the charges payable by one person to another and assisting in unauthorised access. The Act also deals with intentional tampering with computer source code, hacking with the intent to cause damage and publishing obscene material electronically.

There has been no significant debate in India as to whether there is a need for a special and comprehensive law to address cybercrime. The new law when introduced into parliament is likely to trigger such a debate. One alternative to a comprehensive law for cybercrime is to amend and supplement India's Penal Code and the Criminal Procedure Code to give these laws an Internet dimension. That may be simpler and less unsettling for courts and legal practitioners. In fact, the IT Act recognises its own limitations by providing specifically that for the time being, no penalty imposed under the Act shall prevent the imposition of any additional punishment attributable under any other law currently in force.

Stepping Up Cybersecurity

Attacks on Indian websites and the growing perception that India's Internet and web-based infrastructure is vulnerable to subversion and attempts at espionage, have prompted the Indian government to step up its efforts to police the Internet and raise security levels.

The Minister for Information Technology and Communications, Mr. Arun Shourie, announced the government's intentions in response to queries on the functioning of the Information Technology Ministry during a parliamentary session.

While no specific measures have been indicated, such security measures could include the establishment of a computer emergency response scheme for monitoring the national Internet infrastructure and facilitating responses in emergencies. The Government will also examine various proposals to provide better protection for IT infrastructure facilities that are identified as being critical to the functioning of the Internet in India. An encryption policy may be framed to protect critical messages from interception and misuse.

Various sub-groups in India's Department of Information Technology are working on specific plans for the tightening up of security in the IT infrastructure.

By Subramaniam Vutha, Subramaniam Vutha & Associates, Mumbai

UNITED STATES

Passage of Drug Import Bill Benefits Internet Pharmacies

On July 25, 2003 the U.S. House of Representatives voted by 243–186 to approve legislation that will allow importation of lower-cost prescription drugs from certain countries, including Canada. The *International Prescription Drug Parity Act*, which faces significant opposition from the U.S. pharmaceutical industry still has to pass the Senate to become law.

It is illegal for Americans to import into the United States, prescription drugs that are ordered by phone, Internet or bought in person. However, according to the Canadian International Pharmacy Association, U.S. regulators traditionally have not enforced the law against individual purchasers.

The new U.S. law will allow for the importation into the U.S., by retailers and distributors, of medicines that are made in foreign facilities, and which are approved by the U.S. Federal Drug Administration.

For a copy of the legislation visit:

http://thomas.loc.gov/cgi-bin/query/D?c108:1:./temp/~c108X8Msuw

By Richard Venerus, Allstream (formerly AT&T Canada)

News

AUSTRALIA

New Cybercrime Code of Practice for ISPs

Following 18 months of development the Australian Internet Industry Association (IIA) released a draft Cybercrime Code of Practice (Code) in relation to cybercrime on July 21, 2003.

While the Internet can deliver enormous efficiencies for business, cybercrime is proving to be an escalating cost for Internet Service Providers (ISPs), government and businesses. Crime involving computers and electronic communications is a big challenge facing organisations as crimes such as Internet based fraud, hacking, card skimming and electronic money laundering are difficult to detect.

The 2003 Computer Crime and Security Survey, run in conjunction with the Australian Federal Police, Queensland Police, Western Australia Police and South Australia Police highlighted the extent of electronic crimes. This survey found that:

- total losses for organisations surveyed in 2003 were estimated at $12 million, more than double the losses for 2002;
- 42 per cent of organisations experienced one or more computer attacks which harmed network data or systems;
- financial fraud, laptop theft and virus, worm and Trojan infections were the largest source of losses.

Improving the safety and security of the Internet depends on early detection of criminal activity. The Code attempts to balance differing concerns including the law enforcement agencies' need to identify, investigate and prosecute offences, the privacy of end users and costs to the industry in complying with the Code.

The objectives of the Code are to:

- facilitate co-operation between ISPs and law enforcement agencies and establish clear policies and procedures for investigations;
- provide a transparent mechanism for the handling of law enforcement agency's investigations for the Internet industry and ensure both ISPs and law enforcement agencies understand the procedures;
- promote positive relationships between law enforcement agencies and the Internet industry;
- ensure that the privacy of users of the Internet will be protected from unlawful intrusion by law enforcement agencies.

The Code stipulates that customer information collected by ISPs, must be retained for six or 12 months, depending on the type of information. Personal information such as a customer's name, username, e-mail address, phone number, credit card details and address details, must be retained for the greater of six months from the date a customer ceases to be a customer or 12 months after the creation of the record. Operational data, such as dynamic IP allocations records, dates and time of log-ins and the total data transferred, must be retained for six months from the date of creation. ISPs, however, are not required to capture subscribers' phone numbers via caller line identification.

The Code was delayed in its release due to privacy concerns. However, after consultation with the Privacy Commissioner it was determined that some ISPs might not be bound by the National Privacy Principles which were introduced on December 21, 2001 under the Privacy Act 1988 (Cth) (Privacy Act).

As a consequence, the Code requires all ISPs wishing to be a party to the Code to be bound by the Privacy Act, if necessary by voluntarily but formally agreeing to be bound. This means the Privacy Commissioner can exercise his power against ISPs bound by the Code who breach the National Privacy Principles.

The Code also reminds ISPs that if they disclose customer information to anyone other than law enforcement agencies, they are at risk of breaching the Telecommunications Act 1997 (Cth) and exposing themselves to the possibility of criminal penalties and up to two years imprisonment.

The IIA has also drafted an Industry Code of Practice for Internet Privacy.

A full copy of the draft Code is available from *www.iia.net.au/cybercrimvt.html*. A 30-day Public Consultation Period in relation to the draft code has commenced during which time public input is welcome. Comments can be e-mailed to the Internet Industry Association at cybercrimecode@iia.net.au. The deadline for submissions is August 21, 2003.

By Elizabeth Levinson, Senior Associate and Natalie Ceola, Articled Clerk, Freehills, Melbourne; e-mail: elizabeth.levinson@freehills.com

How is information privacy being regulated worldwide?

WORLD
DATA PROTECTION
REPORT

Volume 3, Issue 6 June 2003

Monthly news and analysis of data protection and privacy issues from around the world

BNA International Inc., London
INTERNATIONAL INFORMATION FOR INTERNATIONAL BUSINESS

Every month, keep track of global developments in data protection.

From storing and transferring customer and employee data to unsolicited commercial e-mails — **World Data Protection Report** is a monthly journal which gives you an insight into how these and other areas are being regulated worldwide.

In theory, the Internet has meant that national boundaries are no longer an obstacle to the flow of digital communications. But national and international regulators are focusing on privacy as one of the key areas of e-commerce requiring legislation. In the United States alone, there are currently dozens of bills dealing with Internet privacy.

Use **World Data Protection Report** to gain an insight into how legislators throughout the world are overhauling their laws in response to growing capabilities in electronic data storage and transfer. Coverage will include: protection of databases; privacy of individuals' data — employees and customers; privacy from electronic intrusion; the extension of telephone privacy laws to the Internet and other forms of mobile communication media; the practicalities and implications of "safe harbours"; and whether imposing standards of privacy can be viewed as barriers to trade.

BNA International, 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England.
Telephone: (+44) (0)20 7559 4801 Fax: (+44) (0)20 7559 4840
E-mail: marketing@bnai.com Website: www.worldtaxandlaw.com