

GETTING THE DEAL THROUGH

e-Commerce

in 31 jurisdictions worldwide

Contributing editor: Robert Bond

2009



**Published by
Getting the Deal Through
in association with:**

ABBC – Azevedo Neves, Benjamim Mendes, Bessa Monteiro, Carvalho & Associados, Sociedade de Advogados RL

Abdulai, Taiwo & Co

Altius

Barretto Ferreira, Kujawski, Brancher e Gonçalves – Sociedade de Advogados (BKBG)

Dimitrov, Petrov & Co

Foyen Advokatfirma AB

Froiep Renggli

García Magliona y Cia Ltda

Gatt Frendo Tufigno Advocates

George Charalambides & Co

Hankyul Law Firm

Heydary Hamilton PC

J Sagar Associates

Joyce A Tan & Partners

JUDr. Tomas Borec Law Firm

Jun He Law Offices

Karniol Malecki i Wspólnicy Sp k

Latournerie Wolfrom & Associés

LG@vocats

Loebl & Loebl

Lovells

Martí & Associats

Michalsons Attorneys

Minter Ellison Lawyers

Portolano Colella Cavallo Studio Legale

Preslmayr Rechtsanwaelte OG

Schjødt

Speechly Bircham LLP

SSW Schneider Schiffer Weihermüller

Yabuki Law Offices

South Africa

Lance Michalson and Jana van Zyl

Michalsons Attorneys

General

- 1** How can the government's attitude and approach to internet issues best be described?

During both the pre and post-apartheid periods, the South African government embarked on a mission to formulate information and communications technology policies. There have been multiple ICT-related policies and legislation since the 1994 democratic elections.

The end of the last century saw the emergence of a myriad of policies in telecommunications, postal, broadcasting, science and technology as well as ICT and trade policies. The new century dawned with important infrastructure policies under the auspices of the Department of Communications (DOC), manifesting themselves in, inter alia, the Electronic Communications and Transactions Act of 2002 (ECT Act) and relevant acts on postal and broadcasting matters and more recently the Electronic Communications Act of 2005 (EC Act). The passing of the ECT Act marked the end of a process initiated by the South African Government in 1999 to establish a formal structure to define, develop, regulate and govern e-commerce in South Africa.

Government policy has focused on initiatives that promote the use of tools and concepts associated with a global information society, with a view to achieving national, social and economic development goals. Consistent with this, the president has established three bodies, the Presidential International Advisory Council on Information Society and Development (PIAC), the Presidential National Commission on Information Society and Development, and the African Advanced Institute on ICT.

The minister of communications was mandated under chapter 2 of the ECT Act to formulate a national ICT or e-strategy, which is still in the process of being formulated. The vision of the e-strategy is to derive long-term benefits from the knowledge-based economy for South Africa by harnessing ICT to aid South Africa in meeting its development goals of job creation, economic growth, poverty alleviation and competitiveness within the knowledge-based economy.

Legislation

- 2** What legislation governs business on the internet?

The ECT Act introduced formal legal recognition of electronic commerce to South Africa. It provides for the facilitation and regulation of electronic communications and transactions, including issues relating to electronic signatures, electronic evidence and computer crimes. Its primary objective is to facilitate and to provide legal certainty on e-commerce and electronic records.

The Regulation of Interception of Communication and Provision of Communication Regulated Information Act 70 of 2002 (RICA) prohibits the interception of communications and makes it a criminal offence to do so. This follows on from the previous legal situation

under the Interception and Monitoring prohibition Act 127 of 1992, but the provisions have been made significantly more sophisticated and they apply to all form of communication, both direct (face-to-face) and indirect (including post and all forms of electronic communication or telecommunication, such telephone, fax, e-mail, network or internet messaging, etc). It is thus unlawful to monitor or intercept communications unless:

- you have a directive from a judge;
- you are a law enforcement agency in some other special circumstances);
- you are a party to that communication;
- one or more of the parties to that communication have consented;
- it is for a business purpose and you have gone through some important procedural steps;
- to determine location in emergencies; or
- in terms of another law.

Business agreements (including business conducted via the internet) will soon be regulated by the Consumer Protection Bill (the third draft is currently available from the Department of Trade and Industry), which will bring about considerable changes to the existing South African law of contract and will impact significantly on all website terms and conditions, which will have to be revisited.

Regulatory bodies

- 3** Which regulatory bodies are responsible for the regulation of e-commerce and internet access tariffs and charges?

E-commerce is regulated to a limited extent in South Africa in the four areas mentioned below by either the DOC or the Consumer Affairs Committee established under the Consumer Affairs (Unfair Business Practices) Act 71 of 1988.

- DOC: Registration of cryptography products and services: chapter 5 of the ECT Act requires that suppliers (not users) of cryptography services or products to register their names and addresses, and the names of their products with a brief description in a register maintained by the Department of Communications. Unless the (local or foreign) supplier has registered, they cannot provide their services or products in South Africa.
- DOC: The use of 'advanced electronic signatures': chapter 6 of the ECT Act provides for the establishment of an Accreditation Authority within the DOC, allowing voluntary accreditation of electronic signature technologies in accordance with minimum standards. Once accredited, these government-endorsed advanced electronic signatures can be used by parties who have to sign by means of an advanced electronic signature where required by law. In addition, the legislature has created a presumption of integrity where advanced electronic signatures are used – that is, they will

allow a party to place reliance on its authenticity by shifting the burden of proof onto the signatory to disprove its authenticity. It has also created a benefit in favour of those processes that have been accredited and are thus recognised as particularly reliable.

- Consumer Affairs Committee: Selling goods or services from a website: chapter 7 of the ECT Act requires that suppliers provide consumers with a minimum set of information, including the price of the product or service, contact details and the right to withdraw from an electronic transaction before its completion. A consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of chapter 7 by a supplier.
- Consumer Affairs Committee: Unsolicited communications (spam): consumers have the right not to be bound to unsolicited communications and the sender of the unsolicited communication must at the request of the consumer provide the identifying particulars of the source from which it obtained the consumers' personal information. A person who continues to send unsolicited communications to a consumer after having been advised that the unsolicited communications are not welcome, commits an offence. A consumer may also lodge a complaint with the Consumer Affairs Committee.

Tariffs and charges

The Independent Communication Authority of South Africa (ICASA) regulates certain internet access tariffs and charges. ICASA was established in July 2000 with the merger of the telecommunications regulator (Telecommunications Regulators Association of Southern Africa) and the broadcasting regulator (Independent Broadcasting Authority). ICASA was established in terms of the Independent Communication Authority of South Africa Amendment Act of 2000, later amended in 2005.

ICASA regulates the telecommunications and broadcasting industries in the public interest and issue licences to providers of telecommunication services and broadcasters.

The EC Act has, inter alia, the objective of ensuring the provision of a variety of quality electronic communications services at reasonable prices. It makes provision for internet services to public schools and public further education and training institutions at a minimum discounted rate of 50 per cent of the total charge levied by a licensee that provides internet services to such schools or institutions.

Jurisdiction

- 4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions (or contentions) in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The general principle for a court to justify exercising jurisdiction over a foreign defendant in internet-based transactions, is that there must be sufficient contact in addition to the accessibility of a website. The mere fact that a defendant has accessed a website is not enough to establish jurisdiction. In order to exercise jurisdiction, it needs to be shown that the defendant has taken further steps or actions.

In the case of defamation, a South African court's jurisdiction vests when a party in South Africa access the offending material published by the defendant.

Contracting on the internet

- 5 Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

Contracts can be concluded electronically.

In terms of South African law, a contract is concluded when one party accepts the offer made by another party. Accordingly a binding agreement will be concluded if one party offers a product or service via the internet and another party accepts the offer of the first party. The legal position is regulated by the common law and the ECT Act.

Section 23 of the ECT Act prescribes the deemed time of dispatch of a data message as being the moment when the data message enters an information system that is outside the originator's control. If the parties are within the same information system, then the message will be deemed to be sent as soon as the recipient can access the message. It provides that a message will be deemed to have been received when the complete message is accessible to the addressee at an address designated or used by the addressee. Messages are deemed to have been sent or received from the person's or entity's usual place of business or residence.

Section 24 deals with the legal recognition of declarations of will or other messages made by way of an electronic data message. This section makes it clear that an electronic signature is not the only means by which assent may be given, but that any action such as clicking on an icon will be sufficient.

Section 25 provides that a data message will be attributed to the originator if its agent or pre-programmed computer system (operating within operational specifications) sent the message.

Section 26 provides that there will be no general requirement to acknowledge receipt of a data message before such message will have legal effect, unless the parties have agreed that acknowledgement is necessary. The remainder of the section provides guidelines that will apply where the parties have agreed that acknowledgement is a prerequisite for legal effect.

E-commerce users frequently agree to the supplier's terms of business placed on its website by clicking on a link, which refers them to the terms (where no signature is involved). This is known as a 'click wrap' agreement. There is legal uncertainty as to whether this form of agreement is valid in South Africa, as there is no case law on the topic. The prevailing view is that the 'ticket cases' apply. These are cases based on a three-question test that makes the obtaining of a signature unnecessary. This description, for lack of a better one, covers all cases in which the supplier places before the customer a document that is not intended to be signed and contains or refers to terms on which the supplier is prepared to do business, whether or not the document is what is normally described as a ticket, because the basic principles are the same in all cases. This situation is mirrored in an online environment. In ideal circumstances, the customer reads and understands the document and, by his or her conduct in going ahead with the contract, becomes bound by the terms. This is either because the customer truly assents to the terms or the supplier is reasonably entitled to assume assent from his or her conduct. If it cannot be proved that the customer read the terms, the customer will nevertheless be bound by the terms if the supplier did what was reasonably sufficient and necessary to draw the customer's attention to the terms of the contract. The question is whether the supplier took steps to draw the attention of 'a reasonable customer' to the terms, so that the supplier is reasonably entitled to assume from the customer's conduct in going ahead with the contract that he or she either read or assented to the terms, or is prepared to be bound by the terms without reading them. What this translates into is the need

for suppliers to display their terms and conditions prominently and do what is reasonably sufficient to give customers notice of these terms and conditions.

- 6** Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

The ECT Act governs contracting on the internet. There are consumer protection provisions relating to business-to-consumer contracts. See question 3.

- 7** How does the law recognise or define digital or e-signatures?

The ECT Act defines an electronic signature as data attached to, incorporated in, or logically associated with other data and that is intended by the user to serve as a signature. The ECT Act recognises the contractual freedom of parties to specify whether electronic signatures are required, and if so, the types of electronic signatures. The Act does not prescribe what type of technology must be used and remains technology neutral. The Act also creates a special type of electronic signature, known as an 'advanced electronic signature'. Where a law (statute) requires a signature, only an 'advanced' electronic signature will be recognised. These signatures can only be provided by vendors whose electronic signature product has been accredited by the DOC. They involve face-to-face authentication. Some of these signatures rely on public key cryptography and to this extent, may be considered 'digital signatures'.

- 8** Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

This depends on whether or not the electronic contract is a 'record'. There is currently no definition of 'record' that is universally used by all organisations. The simple reason for this is that definitions serve the community that they are created by and each community has different needs.

While not in itself a law, the South African National Standard on Records Management (SANS 15489) defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. This definition therefore covers records which the law and the business require be retained.

All organisations in all industries are required to retain certain electronic and paper based records. The difficulty lies in giving practical effect to these laws as they focus on the need to retain the record based on its content and often do not focus on the specific medium that is used to transmit or house the record (eg, e-mail, word processing document or paper) or identify precisely what the actual record is as this is often not apparent from the statute.

Where the law requires an organisation to keep records, sections 14 (original) and 16 (retention) of the ECT Act allows the organisation to keep the record in electronic form, provided that it implements a reliable, auditable process. However, the ECT Act does not override laws where electronic retention is expressly precluded or where certain requirements for electronic storage are specified (eg, taxation laws).

An important point to note is that the ECT Act, unlike some foreign laws, does not provide procedural or technological standards that have to be followed in order to ensure that a record will be legally valid. It does not prescribe any technical functional requirements and leaves it up to the implementing technology companies to determine the best approach on their own.

Security

- 9** What measures must be taken by companies or ISPs to guarantee the security of internet transactions?

Section 43(5) of the ECT Act requires the supplier in an electronic transaction to 'utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned'. If a payment system is breached, the supplier must reimburse the consumer for any loss suffered. In most instances the supplier does not provide or operate the payment system and this obligation will shift to the provider who is sometimes the ISP.

Apart from the foregoing, while there is no specific law that imposes specific information security related obligations on companies and ISPs, both have a common law duty not to be 'negligent'. When South African courts consider whether an act was negligent or not, they will try to find out if a 'reasonable person' in the defendant's position (the ISP) would have acted differently if the damage was reasonably foreseeable and preventable. It may be argued that compromises to an organisation's information security is a foreseen risk which should be guarded against and that any omission to take preventative or remedial steps could be regarded as a negligent act which may lead to liability.

The concept of a 'duty of care' is also used by our courts to determine whether or not a party was negligent. One owes a duty of care only to persons to whom harm may be reasonably foreseen. Where a degree of skill and expertise is required in the rendering of certain services, such as information security services, the test for negligence is adapted to accommodate such situations. Here, not only must reasonable care be exercised, but it must measure up to the standard of competence of a reasonable person professing such knowledge and skill. In other words, the reasonable person is replaced by the reasonable expert.

Where, for example, a hacker gains access to an organisation's database and obtains the names, addresses and credit card numbers which it the uses for purposes of identity theft, the individual whose information was stolen might be able to institute legal proceedings claiming that in failing to use industry-standard security measures, such as firewalls or intrusion detection systems, the organisation or ISP failed to protect the victim's personal information and thereby caused it to suffer loss.

- 10** As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

Yes, private keys can be made available but only after having received a decryption direction from a judge in terms of section 21 of RICA.

Certification authorities are a type of authentication service provider whose activities are not regulated unless they provide advanced electronic signatures, in which case they must be accredited under chapter 6 of the ECT Act. Once accredited, their liability is determined by their Certificate Policy or Certification Practice Statement. This is regulated by the Accreditation Regulations pursuant to section 41 of the ECT Act.

Domain names

- 11** What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

The .za domain name space of the Republic of South Africa is managed by the .za Domain Name Authority (the Authority) established in terms of chapter 10 of the ECT Act. The Authority licenses

entities to manage and administer the various sub domains of .za. See www.zadna.org.za/slds.html for the various sub-domains and their respective statuses. The Authority can also accredit domain name resolution service providers to resolve disputes relating to domain names registered under certain portions of the .za name space. The current accredited service providers are the Arbitration Foundation of South Africa and the South African Institute for Intellectual Property Law.

Any person can register the second level sub-domains .co.za, .nom.za (corporate entities excluded), .tm.za (if the holder of a South Africa trademark) and .web.za (any person who wants to put up a web server).

12 Do domain names confer any additional rights (for instance in relation to trademarks or passing off) beyond the rights that naturally vest in the domain name?

No.

13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

Yes. See the alternative dispute resolution regulations at www.info.gov.za/gazette/regulation/2006/29405.pdf.

Advertising

14 What rules govern advertising on the internet?

The Advertising Standards Authority (ASA) governs and regulates advertising in South Africa. It is an independent body set up by the marketing communications industry to regulate advertising through a system of self regulation. The Code of Advertising Practice is the guiding document of the ASA. The Code binds the advertiser, the advertising practitioner and the medium involved in publication of the advertiser's message to the public.

The ASA does not distinguish between advertising on the internet and advertising through other mediums. The Advertising Rules of the ASA also apply to Internet advertising. However these rules only apply to Internet advertising on South African based websites.

The Wireless Application Service Provider's Association (WASPA) also regulates advertising via SMS and on websites. WASPA is an industry body which represents the interests of its members and consumers with its own Code of Conduct, and seeks to enforce good practices established by the Code.

Advertising Rules referred to as 'advertising guidelines' have been published pursuant to section 6 of the WASPA Code of Conduct. These Advertising Rules regulate the following aspects of advertising placed on websites:

- rules for cost and terms and conditions must be displayed in full;
- advertisements that have a subscription service component must include certain specified information; and
- adult content and age-restricted services must implement an adult verification process.

The Consumer Protection Bill referred to in question 2 will also regulate advertising (including advertising over the internet) once enacted. The provisions of the Bill seem to be based on the general principles of the ASA.

15 Are there any products or services that may not be advertised or types of content that are not permitted on the internet?

In terms of ASA, the following has been identified as unacceptable advertising:

- advertisements that play on fear (without justifiable reason);
- advertisements that contain anything that leads to or supports acts of violence;
- advertisements that contain anything that leads to or supports act of criminal activity;
- advertisements that contains anything that is discriminatory (without being justifiable in terms of the Constitution of South Africa 108/1996); and
- gender stereotyping or negative gender portrayal (without being justified as stated above) (Constitution of South Africa 74/1996).

It is a punishable offence in terms of the Films and Publications Amendment Act 34 of 1999 use children in pornographic publications on the internet, thus including such use in advertisements.

Financial services

16 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and if so by whom and how?

Financial service providers need to register with the Financial Services Board, from which they receive a financial service provider number (SFP Number). Online advertising of financial services or products is not regulated in any different manner than other advertising. The SFP number of a provider must be displayed in the advertisements of financial products or services.

The Financial Advisory and Intermediary Services Act 37 of 2002 makes provision for a code of conduct to be adopted with specific provisions relating to avoidance of fraudulent and misleading advertising, canvassing and marketing.

Defamation

17 Are ISPs liable for content displayed on their sites?

Chapter 11 of the ECT Act deals with the limitation of the liability of service providers or so called 'intermediaries' (such as ISPs) in cases where they may otherwise have been liable for third party data hosted on their servers. Chapter 11 thus creates a safe harbour for service providers who were previously exposed to a wide variety of potential liabilities by virtue of merely fulfilling their basic technical functions.

In order to receive the protection under this chapter, a service provider must be a member of a representative body recognised by the minister as such, in terms of the procedures of this Act. The minister has not yet recognised any representative bodies and the safe harbour is not yet available.

Because of the limited protection of the ECT Act (only applicable to members of recognised representative bodies which have not yet been recognised), several ISPs also exclude or limit their liability for content displayed on websites they host contractually in their terms and conditions with their subscribers.

18 Can an ISP shut down a web page containing defamatory material without court authorisation?

Yes. The ECT Act makes provision for take-down notifications to be addressed by a complainant to a service provider. These notifications must be in writing and must include certain specified information.

A service provider shall not be liable for the wrongful take down in response to such a notification.

Intellectual property

19 Can a website owner link to third-party websites without permission?

This is not expressly prohibited by any law, but may possibly amount to a contravention of the provisions of the Copyright Act 98 of 1978. Broadly speaking, copyright is the right given to the owner of a copyrighted work not to have that work copied (reproduced) without authorisation. Without law in the area of linking having been established, website owners who wish to exert strict control over linking (and framing) of their website content should prohibit third parties contractually from linking by incorporating online terms and conditions that exclude any implied licence and limit and restrict the use of the website content and provide, for example, that no linking may take place without the express content of the website owner.

20 Can a website owner use third-party content on its website without permission from the third-party content provider?

No. This would amount to a contravention of the Copyright Act 98 of 1978 if the content as the copyrighted work was first published in South Africa or made by a 'qualified person' (a South African or company registered and incorporated under the laws of South Africa). The responsible minister has, however, in regulations made in terms of section 37 of the Act, made provision whereby the Act applies also to works of foreign origin in the same way as it applies to those works first published in South Africa. In terms of these regulations, the Act will apply to those countries listed in a schedule to the regulations if the content is first published in that country listed in the schedule.

Website content, whether it be text, music or graphics, is a form of work subject to copyright protection.

21 Can a website owner exploit the software used for a website by licensing the software to third parties?

It depends on whether the website provider owns the software. If it owns the software it can license it to third parties on such terms as it deems appropriate. In South African law, software is formally defined as a 'computer programme' under the Copyright Act – the provisions of which apply to proprietary software and not 'open-source software'. The owner of a computer programme is the author, and the author is the person who exercised control over the making of the computer programme. Factors to take into account in determining who 'exercised control' would include whether the software was coded by an employee or a sub-contractor, who issued the detailed instructions for the computer programme, and who was responsible for checking the work, etc.

22 Are any liabilities incurred by links to third-party websites?

If the linking without a licence is held by a court to amount to a contravention of the provisions of the Copyright Act 98 of 1978, liabilities can be incurred.

Data protection and privacy

23 What legislation defines 'personal data' within the jurisdiction?

The Promotion of Access to Information Act 2 of 2000 (PAIA), enacted to give effect to the constitutional right to access information held by the state and information held by another person, has a definition of 'personal information'.

The Protection of Personal Information Bill (PPI Bill) which is currently before the South African Law Commission and which is not yet law (August 2008) also has a definition of 'personal information' that corresponds to the definition in PAIA but has been extended to include, so far as it is applicable, an identifiable, juristic person.

In terms of the PPI Bill a very extensive definition for personal information has been defined to include a large amount of information about identifiable natural and juristic persons (where applicable).

24 Does a website owner have to register with any controlling body to process personal data? May a website provider sell personal data about website users to third parties?

The processing of 'personal information' is not yet regulated by South African law, but will be soon when the PPI Bill is enacted. In terms of the common law, case law and Constitution, there is no specific prohibition on the sale of personal data and there is no controlling body that regulates the processing of personal data.

In terms of the PPI Bill, personal data will only be processed in very limited instances including where the person has given consent or where the processing is necessary in terms of the specified provisions of the Bill. This corresponds with the provisions of the National Credit Act 34 of 2005 (NCA), which provides for 'confidential information' (personal information) to be used only for a (limited) purpose permitted or for a purpose required by the NCA or other legislation.

25 If a website owner is intending to profile its customer base to target advertising on its website, is this regulated in your jurisdiction?

Profiling a customer base is not regulated in South Africa.

26 If an internet company's server is located outside the jurisdiction, are any legal problems created when transferring and processing personal data?

Not currently. However, the issue of trans-border data flows is dealt with in section 94 of the second draft of the PPI Bill. The third draft of the Bill introduces these provisions of section 94 as an information protection principle under chapter 3 of the Bill. It currently states that such personal information can only be transferred to someone in a foreign country if:

- the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles set out in the PPI Bill;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- all of the following apply: the transfer is for the benefit of the individual, it is reasonably impracticable to obtain the consent of the data subject to that transfer, and if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

Taxation

- 27** Is the sale of online products (for example, software downloaded directly from a website) subject to taxation?

South Africa previously had a predominantly source-based tax system but adopted a resident-based tax system some years ago. The sale of online products will accordingly be subject to income tax where income is derived from online sales by a resident as defined in the Income Tax Act 58 of 1962. In the event of income deriving from sales by a non-resident, the source basis that entails that income derived from a South African source would still be applied and the sales will be subject to Income Tax.

- 28** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Value-added tax (VAT) is only levied on supplies by a person who conducts an enterprise in South Africa. A supplier who supplies telecommunication services on a continuous or regular basis to any person, who utilises the service in South Africa, is deemed to conduct an enterprise in South Africa for purposes of VAT. This principle applies also in circumstances where the supplier is not a resident or does not have a permanent place of business in South Africa.

Where the management of an incorporated entity outside the jurisdiction are residents of South Africa, the income derived will still be subject to Income Tax.

From the definition of an enterprise it follows that where a server has been placed within the jurisdiction, an enterprise is conducted in South Africa and such company would be exposed to local VAT, even though the company is incorporated outside South Africa.

- 29** When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

Every person who carries on an enterprise, including all telecommunication service providers become liable to register at the Commissioner for Revenue Services at the end of any month where the total value of taxable supplies made by that person in the preceding 12 months exceeded 300,000 rand (approximately US\$38,200). Application must be made within 21 days from the end of that month.

If such person is not a resident of the Republic, such person must appoint a representative vendor as agent or person controlling the affairs of the enterprise in South Africa and open a banking account with any bank or other similar institution for the purposes of his enterprise carried on in the Republic. He or she must then furnish the Commissioner with the particulars of such representative vendor and bank account details.

In the domestic Internet sale of goods or services, the supply will be subject to VAT of 14 per cent (the standard VAT rate).

- 30** If an offshore company is used to supply goods over the internet, how will returns (goods returned in exchange for a refund) be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

In terms of the South African Value-Added Tax Act 89/1991, VAT is levied on the importation of goods by a South African resident from a supplier who resides or conducts business outside South Africa. VAT is only payable on goods or services for private use and not where it has been acquired for the purpose of making taxable supplies. The recipient of the imported goods or services is liable for the payment

of VAT. That VAT paid by a private consumer is a permanent cost and in the event of goods returned in exchange for a refund, the VAT paid to the commissioner will not be refunded.

There is no VAT implication where a customer returns goods to a local branch of an offshore company where the product was bought. The customer will be refunded in the local currency and any transfer pricing differences will be determined and handled between the two branches.

Gambling

- 31** Is it permissible to operate an online betting or gaming business from the jurisdiction?

Online gambling is not permissible under the current legislation, but will soon be once the National Gambling Amendment Bill is enacted. Currently gambling in South Africa is regulated concurrently by national and provincial legislation. The National Gambling Act 7 of 2004 (the National Gambling Act) governs all gambling activities in South Africa on a national basis. In addition, each of the nine provinces has its own act (Provincial Acts), which were promulgated under the National Gambling Act 33 of 1996.

Lotteries and sports pools are governed separately by the Lotteries Act 57 of 1997. Online sports betting will accordingly not be illegal, provided it is operated under a licence from the applicable provincial Gambling Board.

Of key importance to the whole question of the lawfulness of internet gambling and services related thereto is the question of where these activities occur. The provincial legislatures only have jurisdiction over their respective provincial territories.

In terms of the National Gambling Amendment Bill that has been approved by the cabinet, but still needs to be signed by the president before it becomes law, internet gambling will effectively be legalised by providing for the regulation of interactive gambling and the licensing of interactive gambling activities in terms of regulations to be promulgated. These regulations have not yet been drafted (August 2008).

In terms of the proposed legislation, software vendors that build interactive gambling platforms will have to be licensed. Conditions for awarding such licences would include a commitment to socio-economic uplift and compliance with broad-based black economic empowerment requirements. Further to this, a provider of interactive gambling facilities will have to ensure that participants are registered as players in terms of the Bill.

- 32** Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

The Supreme Court of Appeal (the highest authority on all cases except cases relating to constitutional rights), has held in the case of *Casino Enterprises (Pty) Ltd (Swaziland) v The Gauteng Gambling Board* (unreported) that 'the aim and object of the Act (referring to the Gauteng Gambling Act 4 of 1995) is to control gambling within the province, not elsewhere'.

Residents are accordingly permitted to use online casinos and betting websites where the actual betting will occur outside the jurisdiction.

Outsourcing

- 33** What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

When outsourcing certain services, an employer will have to follow the procedures in terms of the Labour Relations Act 66/1995 in order to retrench the current employees and employees will have to be paid

severance pay in accordance to the provisions of the Basic Conditions of Employment Act 75/1997 (see below).

The company rendering the outsourced service may be registered for VAT, in which event VAT of 14 per cent will be payable on the service.

- 34** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?

Where services are outsourced, employees' services are terminated due to 'operational requirements'. This entails that the economic, technological, structural or similar needs of an employer must have given rise to the employment being terminated and the services outsourced. Employers are bound by the provisions of section 189 of the Labour Relations Act 66/1995 to follow a process of consultation in such circumstances.

In terms of the Basic Conditions of Employment Act 75/1997, an employer must pay an employee who is dismissed for reasons of operational requirements severance pay equal to at least one week's remuneration for each completed year of continuous service with that employer, calculated in accordance with the provisions of this act. In the event of an unreasonable refusal by an employee to accept the employer's offer of alternative employment with that employer or any other employer, the employee is not entitled to severance pay.

These rules apply to all employees who work 24 hours or more per month.

Online publishing

- 35** When would a website provider be liable for mistakes in information that it provides online? Can it avoid that liability?

The general principle is that a website provider must ensure that the content on the website is accurate and will a provider run the risk of being sued for breach of contract or negligence in the event of wrong information being provided.

In terms of South African law, nothing prevents a provider from limiting or avoiding its liability contractually. In terms of the contract entered into between the provider and user of the website, a provider can contractually be indemnified against liability on the grounds of negligence or gross negligence.

Update and trends

An important change is the pending data protection legislation, to be enacted when the Protection of Personal Information Bill becomes law.

- 36** If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

Yes. A database is protected as a literary work under the Copyright Act 98 of 1978, while computer programmes are protected as a separate class (namely 'computer programmes').

Section 1 of the Copyright Act 98 of 1978 defines a computer programme as a 'set of instructions fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result'. It is thus important to check whether or not the source code contains a set of instructions which, when used on a computer, directs its operation to bring a result.

A database schema does not consist of a set of instructions. Rather it includes a table with a certain number of columns which may vary.

In the 2006 Appeal Court case of *Haupt t/a Soft Copy v Brewers Marketing Intelligence (Pty) Limited and Others* 2006 (4) SA 458 (SCA), the court distinguished between computer programmes and databases as separate categories of work eligible for copyright under the Copyright Act. In this case they held the bare database to be a computer programme and considered the database schema to be a literary work and not a computer programme. This was, however, always subject to the proviso that the database schema was first created by a person and not a computer (a person can use a computer to assist in the creation of a database in much the same way as a document is created using a word processor); otherwise the court ruled that it will be treated as a computer programme.

Michalsons Attorneys

Lance Michalson

lance@michalson.com

Po Box 32482
Camps Bay
Cape Town
South Africa

Tel: +27 21 423 3332
Tel: +27 11 327 4540 (Johannesburg)
Fax: +27 86 669 0400
www.michalson.com

Offices in Johannesburg and Cape Town