Legal Aspects of Electronic Commerce

Only study guide for LML411Q

Compiled by
Prof T Pistorius
Prof TB Floyd
Prof GTS Eiselen

Department of Mercantile Law
University of South Africa, Pretoria

Printed and published by the
University of South Africa
Muckleneuk, Pretoria

LML411Q/1/2010–2012

98547992

3B2

Sections of the Green Paper on Electronic Commerce have been reproduced in this study guide with the permission of the Department of Communications.

A4 Icon style

Contents

STUDY UNIT 1

Introduction to legal aspects of electronic commerce

Tana Pistorius

OVERVIEW

In this study unit we shall explain the legal challenges that are posed by electronic commerce. We shall introduce you to the subject matter of this module and we shall explain to you how to use the study guide.

LEARNING OUTCOMES

After completing this study unit you should be able to do the following:

- understand the legal challenges that are posed by e-commerce
- understand the role and function of the Green Paper on Electronic Commerce

SETTING THE SCENE

In this study guide, we shall tell you an ongoing story in each study unit, and sometimes before a set of activities, we shall provide you with the necessary details as we go along. Although this is just a story, the answers to the activities are based on South African law and court decisions.

The main story line, as set out below, briefly provides the issues that will be discussed in the different study units. The function of the ongoing story is to involve you in the practical application of the legal aspects of e-commerce in a concrete manner.

The three main role players in our story are three friends, Tim, Vuzi and Sina. Tim studied literature and plans to earn his living by writing contemporary stories. Sina is an artist and up to now has sold her metal artworks, called ''METALLINKS'', at informal craft markets. Vuzi is a qualified mechanic. Tim, Vuzi and Sina have decided that they should trade on the Internet.

They are of the opinion that the Internet offers vast business opportunities. Vuzi has had some computer training and enjoys surfing on the Internet by using the facilities offered by the local Cybernet café. Tim and Sina do not have any computer-related experience. They are not sure of how to launch their ''Internet ventures''. They approach Thieu, a computer ''whiz kid''. Thieu offers to launch their Internet-trading activity by designing their websites for the friends. Our ongoing story will tell you about the threesome's ensuing electronic-commerce activities. The friends will also approach you for legal advice when difficulties arise.

1.1 GLOBALISATION OF BUSINESS

electronic frontier

The Internet is a global network of computers that all speak the same language, a ''digital Esperanto'' of zero's and ones (Gringras 1). This giant network has given birth to an electronic frontier, namely a virtual world in which cyber citizens enter into cyber contracts. One of the phenomena of globalisation and the development of information technology is the advent of global business.

globalisation

What until very recently took place over long distances, has now shrunk to instant transmissions through communications and the convergence of technologies. Conventional time and place have been replaced by **any moment**, **any place**, in the world. At the very least, globalisation is a process that affects all aspects of social, political, and economic activity. The world is thus shrinking, and we are — irresistibly — moving toward a world of increased communication, common markets, and shared culture.

The digitisation of information and the rapid growth of the Internet have had a marked influence on society. The Internet is changing the way we communicate and do business. These changes have dramatically and irrevocably altered the needs of business and industry.

1.2 THE LEGAL CHALLENGES

novel legal problems

The Internet has revolutionised international commerce. However, definite answers to several complex legal questions have not yet been found. The continuing development of the Internet and its associated applications has created a variety of new situations in which traditional legal principles should be applied. It may not be easy to apply the traditional principles of commercial law to e-commerce as some of them have been rendered obsolete by modern communication techniques.

What is electronic commerce?

Electronic commerce, or e-commerce, is simply trading electronically. The technologies that can be used for electronic commerce include the Internet and the World Wide Web, electronic mail (e-mail), EFTPOS, and the common fax machine. A website can continue taking orders 24 hours a day, as business hours occur in different time zones. The fundamental benefit of electronic commerce is enhanced communication, which allows for simplicity, flexibility and new ways of doing business.

Commerce over the Internet differs from traditional commerce, in that, traditionally trading was developed in a paper based society. E-commerce takes place in an anonymous borderless society, and many of the rules which were developed for trading in a real environment is inappropriate for this new virtual environment.

Intellectual-property law faces the biggest challenge yet as on-line services, the Information Highway and the age of multimedia have become realities. Furthermore, the heated ''dot.-com'' domain-name disputes and the transmission of digitalised information products necessitate a re-examination of current intellectual-property laws.

security

The big question is whether **security** is needed in the Internet. The Internet presents security challenges. The Internet, comprised of millions of interconnected computers, allows nearly instantaneous communication and transfer of information, around the world. People use e-mail to correspond with one another. The World Wide Web is used for online business, data transmission, research, learning, personal communications, transfer of payments and a myriad of other activities. The perpetual increase of information transmitted electronically has lead to an increased need for secure transmissions.

legal issues

On-line service providers are experiencing a number of issues of concern namely privacy, liability, content restrictions, security, intellectual-property protection, consumer protection, electronic authentication, and electronic-payment mechanisms. Other issues are also affecting the consumer, including access to global telecommunications networks and the myriad of issues affecting access. The creators of website shopping malls are faced with the challenge to design their sites in order to effectively contract with customers (see Davies *Communications law* 82; Barlow 169).

1.3 INTERNATIONAL TRENDS IN LEGISLATION AND REGULATORY REGIMES

uniform trade laws

The economic argument is as simple as it is persuasive: if people in business trade in a number of countries, their lives would be made much easier and their effectiveness in business would be greatly enhanced *if* their dealings were to be subject to similar legal regimes no matter where they happen to trade. This is not a new idea, of course: it is exactly what has underpinned the notion of *lex mercatoria* or law merchant during the Middle Ages.

International efforts are under way to tackle the most important policy issues regarding telecommunications deregulation, the unified treatment of paperless commercial transactions, intellectual-property protection, security and privacy and customs and taxation. Laws providing for data protection, digital and electronic signatures, privacy and access to information have become imperative.

UNCITRAL Model Law

It is against this background of increasing legal uncertainty that the UN Commission on International Trade Law established a working group to draft legal rules on electronic commerce. The UNCITRAL Model Law on Electronic Commerce (1996) aims to create a more secure legal environment for what has become known as ''electronic commerce'' by providing a tool for states to enhance their legislation regarding paperless communication and storage of information. The Model Law is expressed in a technologically neutral manner; so that it can apply not only to existing, but also to future, technology.

examples

Numerous jurisdictions that have adopted legislative measures to facilitate e-commerce based their enabling instruments on the Model Law (see, eg, in the US, the draft Uniform Electronic Transactions Act (hereafter referred to as ''the UETA'' (1999). This Act has been closely modelled on articles 2(a) and (f), 4, 5, 6, 7, 8, 9, 10, 11, 14 and 15 of the Model Law; see also the Australian Electronic Transactions Act 1999; and the Canadian Uniform Electronic Commerce Act 1999 (available at <http://www.law.ualberta.ca/alri/ulc/acts/eueca.htm>) (assented to on 13 Apr 2000); see Ontario's Act with Respect to Electronic Information, Documents and Payments (Bill 70 2000); Singapore has adopted the Electronic Transactions Act 25 of 1998, based on the Model Law. International organisations have also played an important role in policy formulation (see the Global Business Dialogue on Electronic Commerce, available at <http://www.gbde.org>)).

1.4 SOUTH AFRICA'S GREEN PAPER ON ELECTRONIC COMMERCE

1.4.1 The Discussion Paper on Electronic Commerce

The Discussion Paper on Electronic Commerce (Jul 1999) served as a starting point for discussions concerning the development of a national policy on e-commerce for South Africa. The Discussion Paper pertained to the building of trust in e-transactions (viz the security of data transmissions, privacy protection, digital signatures, certification and certification authorities, consumer protection and consumer fraud), the establishment of ground rules for e-commerce (including issues such as taxation and duties, intellectual-property rights and domain names), enhancing information and telecommunications-technology infrastructure and maximising benefits for the South African society as a whole.

1.4.2 The Green Paper on Electronic Commerce

The Green Paper on E-Commerce ''Making it your business'' was a further step in the evolution of a South African policy on E-commerce. It was published in November 2000. The Green Paper was a very important policy document.

1.5 THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 (ECT ACT)

The ECT Act was promulgated on 25 August 2002. The overall objective of the ECT Act is to enable and facilitate electronic transactions by providing for its enforceability and thus creating public confidence in electronic transacting.

1.6 OVERVIEW OF STUDY UNITS

In **study unit 2**, the way in which the Internet operates is explained and an exposition of the major role players involved in e-commerce is given. In **study unit 3**, the rules of consensus are applied to establish whether, where and when an electronic contract has been concluded. Also, the formalities and different ways in which payment may be made over the Internet are dealt with. Consumer protection is also touched upon.

In **study unit 4**, copyright infringement on the Internet is dealt with. Also, the effects of digitisation on copyright works, forms of infringement in the network environment and service-provider liability are dealt with.

Study unit 5, protection of electronic databases is dealt with. In **study unit 6**, the use of trade marks on the Internet and the registration of domain names are discussed. **Study unit 7** deals with the implication of e-commence on income tax.

1.7 USE OF THE STUDY GUIDE

This tutorial letter is your primary tutorial matter for the module Legal Aspects of Electronic Commerce (LML411Q).

The activities are important, as they will give you the opportunity to apply the theoretical material to a practical situations. We shall try to help you to evaluate the material in a critical manner and to seek new solutions to old problems. Feedback is provided for every activity. Do not refer to the feedback before you have completed the activity. You will be able to reach the critical outcomes listed at the beginning of each study unit only if you complete each activity **before** turning to its feedback.

The tutorial matter contains technical terms of reference — for example, ''hosting'', ''hyperlink'' and ''ccTLD''. We have thus included a glossary of terms as an appendix to the study guide. Students who have not yet enjoyed extensive exposure to cyberspace terminology will find this glossary useful.

Please use the glossary if you are unsure of the precise meaning of a term (see appendix I of the study guide). Students who wish to broaden their knowledge on legal aspects of e-commerce are referred to the myriad of sources in the on-line and off-line bibliography cited at the end of the Green Paper on Electronic Commerce.

1.8 CONCLUSION

We hope that you will enjoy this new and exciting module.

STUDY UNIT 2

Introduction to the Internet: overview and major role players

Sieg Eiselen and Tana Pistorius

OVERVIEW

This study unit contains an introduction to the Internet. The way in which the Internet operates is explained, and an exposition of the major role players involved in cyber trading or e-commerce is given. Also, the difference between entities that provide access and Internet services to Internet users (service providers) and entities that provide and operate the actual electronic commercial sites (content providers) is explained. Furthermore, the various contractual relationships that are created or that exist between the various parties are explained.

LEARNING OUTCOMES

After completing this study unit you should be able to do the following:

- explain what the Internet is, and how it operates
- explain what a network is, and distinguish it from the Internet
- identify the different role players involved on the Internet
- distinguish between Internet service providers, access providers and content providers
- describe the various services offered on the Internet
- explain the various contractual relationships that may be created between service providers, access providers, content providers and customers
- explain the relationship and communication between the customer and the content provider

SETTING THE SCENE

As indicated in study unit 1, Tim, Vuzi and Sina have decided to launch their Internet venture, as they believe that it will open up

new markets and possibilities for them. Tim, Vuzi and Sina, acting on your advice, have formed a close corporation called ''TVS Enterprises CC'', through which they wish to conduct their business. Thieu, who offered his services to design and launch their Internet trading site, has also approached them. TVS has now concluded a contract with Thieu to develop the site on its behalf.

Thieu has introduced TVS to Netlink, an Internet service provider, and has concluded a contract with TVS on behalf of Netlink. In terms of the agreement, Netlink will provide space on its computer (server) on which TVS can develop its site, and which will ultimately be linked to the Internet, giving consumers worldwide access to TVS's products and services. Thieu has an independent contract with Netlink in terms of which he will earn 5 percent commission on every customer introduced to Netlink by him. However, he is not employed by Netlink.

The site which Thieu has developed consists of a home page describing the various products and services it sells in general terms, a page containing TVS's standard terms and conditions of contract, a page describing the various types of product and service that TVS sells, and an order page on which the products and services can actually be ordered by a customer. TVS also has an e-mail facility with Netlink, as well as access to a chat line. Thieu has also developed and installed an internal network for TVS, linking the computers of Tim, Sina, Vuzi and their secretary to one another, and providing access to the Internet via Netlink.

2.1 INTRODUCTION TO THE INTERNET

origin of the Internet

The Internet is a global network of computers that all speak the same language, a ''digital Esperanto'' of zero's and ones. The Internet is made up of a shared infrastructure — namely a network of networks that all use the same protocols. The ''TCP/IP'' protocol is used in the United States, and the ''Open Systems Interconnection'' (OSI) protocol is used in Europe.

The Internet came into being in the United States in 1969, for strategic military purposes. The development of ARPAnet — the first interlinked network of 40 computers — enabled the American Defence Department to simultaneously dispatch orders to all ballistic missile bases. The basic principles that guided the development of the first network in the 1960's still apply today.

These networks link computers throughout the world through several means of telecommunication, such as telephone and coaxial cables, fibre-optics and satellites. The best-known category of communication over the Internet is the World Wide

WWW

Web. The World Wide Web (WWW) is at the moment the most popular way of gaining entry to the Internet. The Internet consists of a world wide association of computers and infrastructure that makes communication possible. The WWW is a part of the Internet consisting of interlinked data that makes communication on the web possible by using a specific Internet protocol called HTTP.

In order to access information on the *WWW* a user needs an Internet browser like *Netscape Communicator* or *Internet Explorer* which provides the means for finding and reading information on the web. Each website has a unique web-address where the information hosted on that site may be found. In order to find information, the user therefore needs to have or find the correct address. Search engines, like *Google* (*http://www.google.com)* provide a quick and efficient way to find relevant addresses on the Internet. An address will usually look as follows: *http://www.msn.co.za*. Several other communication applications are also available to the user, namely e-mail (electronic mail), Telnet, FTP (File Transfer Protocol), Gopher, Mailing Lists, Discussion Groups (such as Newsgroups) and Internet Relay Chat.

core infrastructure

The core infrastructure of the Internet consists mainly of routers (computers designed to receive and transmit data), hosts (computers which store programs and data), and pipes (telecommunication links between the routers and hosts). A typical arrangement of the Internet is provided in figure 2.1.

ACTIVITY 2.1

DISCUSSION

- Describe what the Internet is, who owns it, who operates it, and how it works.
- Distinguish between the World Wide Web, e-mail, newsgroups, bulletin boards, Internet chat, intranets and extranets.

FEEDBACK

If you are unsure of any answer, refer back to the study material, in which you will easily find that particular answer.

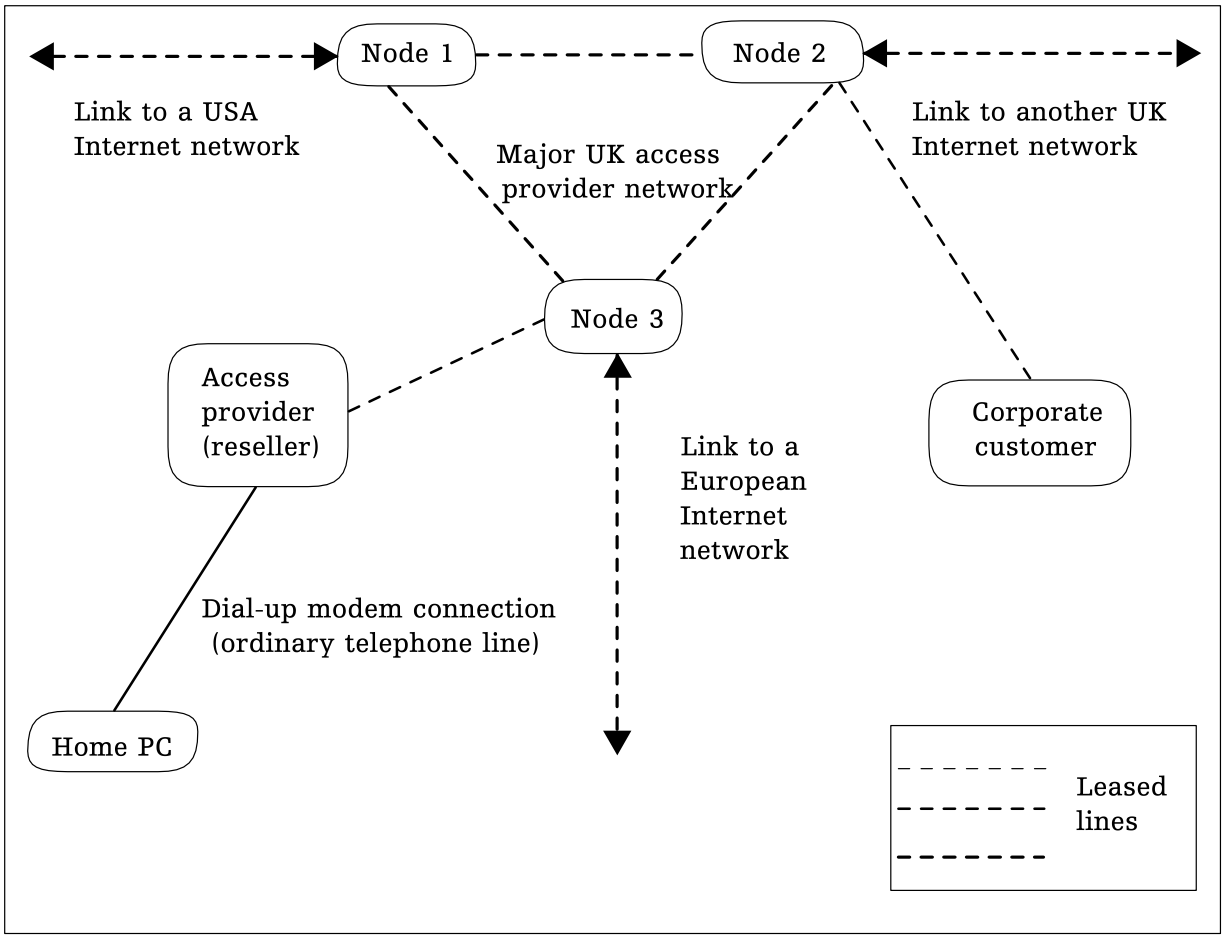
Have you also considered the following:

- how users and sites are identified, and who controls the protocols for naming and identification

- how difficult it is to exercise any kind of control over the flow of information, types of service offered and tracking down of individual sites
- whether there are any legal differences among the various services that are offered on the Internet and the relationships resulting from them

FIGURE 2.1

The Internet — a typical arrangement



Source: Smith GJH *Internet law and regualtions* (1996) p 2

2.2 INTERNET ROLE PLAYERS

main players

The main players in the Internet context are infrastructure and network providers, content providers, administrators, access providers (commonly, and perhaps less accurately, known as Internet Service Providers (ISPs), or, more accurately, as Online Service Providers (OSPs)), navigation providers, and transaction facilitators.

2.3 CONTRACTUAL RELATIONSHIP BETWEEN PARTIES

A number of contractual relationships may be created by and between parties using the Internet, ranging from agreements to provide infrastructure, to provide access to the web, hosting material to commercial agreements between users. In each instance it is important to establish who the contractual parties are and what the nature of their agreement is in order to determine what the rights and obligations of the parties are.

Infrastructure providers. These entities provide the basic infrastructure which makes communication on the Internet possible. The first type of infrastructure needed is communication lines such as telephone or data lines which link the various computer systems to one another. These services are usually provided by world-wide telecommunication companies such as Telkom. The agreement is a composite agreement including lease, service and a contract for the use of the infrastructure.

Internet service providers. These entities provide a number of services to the users of the Internet ranging from Internet access, e-mail facilities and hosting of websites. These agreements are mainly service agreements (*locatio conductio operis)* in terms of which the service provider provides the services agreed upon at a price agreed upon. Sometimes these agreements may contain an element of lease where specific equipment is leased to the client.

Internet content providers. These entities provide information on the web to users of the Internet. There are a great variety of content providers, some charging fees for access or use of their sites, whereas others provide free access but make their money from selling advertising space on their websites. Many entities simply provide information free of charge as a public service, or provide information to market their goods or services. Where fees are charged the contract will usually be a contract for services, (ie access to the website), or it may be a sales contract (ie for information products).

Internet businesses. Today there are a host of websites where transactions can be concluded online between the Internet business and clients. A wide range of agreements, ranging from simple sales contracts, agreements for financial services, such as banking services, to agreements for the provision of services (such as online legal services or providing medical advisory services). The rights and duties flowing from the contract concluded between the business and client will be determined by establishing the *naturalia* for that contract as well as the agreement itself. Many sites also make use of standard terms and conditions which are included by reference or through so-called click-wrap.

Any relationship between Internet role players will be deter-

mined by the contractual relationship between them. In the law of contract, relationships between contractual parties are determined first and foremost by the agreement between the parties themselves. However, there are certain specific con-

naturalia

tractual types and relationships for which the common law has developed a number of specific rules — *naturalia* which will apply to the relationship of a specific contract type unless the parties have made another arrangement in their agreement. It is therefore important to establish what kind of contractual relationship one is dealing with.

freedom of contract

In the South African law of contract, the principle of freedom of contract plays a fundamental role in the flexibility and adaptability of this part of the law. This principle means, *inter alia*, that the parties have a large degree of freedom in structuring any contractual relationship according to their wishes and needs. This also holds true for the contractual relationships that may be concluded in respect of Internet services and cyber trade.

residual rules

The common law, however, also makes provision for certain residual rules which will apply in respect of certain types of contract unless the parties have made an alternative arrangement in their agreement. This is to ensure that if parties fail to provide for commonly occurring events in their agreement, the agreement will nonetheless be valid and enforceable. For instance, in a contract of sale there are certain common-law warranties that will apply if the goods suffer from latent defects even though the parties have not agreed to such warranties. The parties are, however, free to change or exclude these warranties if they so wish.

These *naturalia* apply to certain identified types of contract such as sale, service (*locatio conductio operis*), agency or hire. These contracts can be identified according to the common-law principles set out below. If a contract cannot be classified as one of these specific contracts it is called an ''innominate'' contract, and no *naturalia* will apply. Regarding cyber trade and the various relationships, it is important to distinguish between contracts of service, hire, sale and agency:

sale

Sale can be described as an agreement for the delivery of goods against the payment of a certain price. The distinguishing feature of this type of contract is that the seller provides the goods to the buyer on a permanent basis, in that the seller guarantees to the buyer that the buyer will not be disturbed in its possession by someone with a stronger right or vested interest. In most cases, the aim of sale is to provide ownership of the goods, although this is not an essential requirement for an agreement to be classified as ''sale''.

hire

Hire can be described as an agreement for the temporary delivery of goods against payment of an agreed sum for a certain

period of time. The feature that distinguishes hire from sale is the fact that in hiring, the use of the goods is provided to the hirer only on a temporary basis, whereas sale is aimed at providing free and undisturbed possession to the buyer on a permanent basis.

locatio conductio operis

Agreement for work and services (*locatio conductio operis)* can be described as an agreement whereby the one party will complete certain work or render certain specified services in exchange for the payment of an agreed sum of money. The agreement for work and services should be distinguished from the employment contract. In an employment contract, the employee agrees to make his or her services available to the employer on an ongoing basis and under the control of the employer.

Although the dividing line between these two types of contract is not always easily established, the usual test for determining whether a particular relationship is one of employment or one of work and services, is found in the amount of control the employer/*mandator* is entitled to exercise over the employee/ contractor. Usually, the contractor who performs work and services retains a high degree of independence regarding when and how the work is to be done, as long as the required end result is achieved within the agreed time. The employee, on the other hand, is normally under the control of the employer, who is entitled to lay down requirements about when and how the employee is to render specified work.

agency

Legal representation or **agency** is a relationship established by a contract of mandate in terms of which an agent is authorised by the principal to perform certain juristic acts on behalf of the principal. For instance, the agent may be authorised to conclude an agreement with a third party on behalf of the principal, which will bind the third party, and the principal, but not the agent. The agent does not become a party to such an agreement even though he or she physically negotiated and concluded the deal. An agent may act in terms of an independent agency agreement, or as an employee in terms of an employment contract, or, in certain instances, as a result of his or her legal status (*ex lege*), such as the parent of a minor or the curator of an insolvent.

ACTIVITY 2.2

Tim approaches you for legal advice. He wishes to know what type of legal relationship exists between TVS and Thieu, between TVS and Netlink, between Thieu and Netlink, and between TVS and any potential customers.

FEEDBACK

- Have you considered that Thieu plays a double role in his dealings with TVS in that he acts as an agent in effecting the agreement between TVS and Netlink, but that he also operates as an independent contractor in developing the site and its content on behalf of TVS?
- Have you considered how the relationships between TVS, Thieu and Netlink would change if Thieu were an employee of Netlink, and not an independent consultant?
- Have you considered that the normal common-law rules of South African law regarding agency, *locatio conductio operis* and sale would apply in the various situations described above?

All the above legal relationships of course have their origin in contract. The following specific contracts were concluded between the various parties:

- TVS and Thieu concluded a contract of mandate
- TVS and Netlink concluded a contract for work and services
- Thieu and Netlink concluded a contract of mandate to represent Netlink

2.4 CONCLUSION

You should now fully understand the global-network structure and the functional role played by different parties. You should also be able to describe the various services offered on the Internet and understand the various contractual relationships that are created between service providers, access providers, content providers and customers.

STUDY UNIT 3

Internet contracts

Tomas Floyd, Tana Pistorius and Sieg Eiselen

OVERVIEW

In this study unit, we shall discuss in detail several aspects of contracts concluded on the Internet. Specific provisions have been enacted in the ECT Act to provide for electronic contracting. In this study unit, we shall explain how the rules of consensus are applied to establish whether a contract has been concluded, and if so, where and when that contract came into existence. We shall also deal with the formalities that are, or may be, required to conclude legally valid and binding agreements, as well as the way in which such agreements may be amended. We shall then discuss the different ways in which debt may be paid over the Internet.

LEARNING OUTCOMES

After completing this study unit, you should be able to do the following:

- apply the rules regarding offer and acceptance to contracting on the Internet
- explain why the rules regarding ticket cases may be applicable to Internet contracts
- explain what a ''click-wrap contract'' is and whether such a contract will be valid
- determine when and where an Internet contract was concluded
- explain whether an Internet contract can comply with the formalities of writing and signature
- explain how an Internet contract can be amended
- discuss the international developments on consumer protection
- draft a standard Internet contract

SETTING THE SCENE

TVS has now launched its Internet trading site. The following products and services are offered on the site:

- Sina's current artworks, of which pictures can be seen on the Internet, may be bought on-line. She also offers to create artworks on commission. Interested parties are requested to negotiate with her by e-mail.
- Tim's short stories and novel, which may be ordered on-line.
- Vuzi's advice on mechanical matters, which may be ordered at R50 per request.
- A mechanical device developed and manufactured by Vuzi which reduces fuel consumption, called the ''Petrosaver''.

Thieu, who has no legal background, has posted an adapted standard contract of sale on TVS's website. He found this contract on an American commercial website. Tim, Vuzi and Sina are not sure whether these standard terms will bind their potential customers.

A study of this study unit presupposes a sound knowledge of the general principles of the law of contract. **We recommend that you refresh your memory on offer and acceptance, consensus, mistake, the ticket cases, the time and place of the formation of contracts, formalities and amendment of contracts, by referring to your study material on the general principles of the law of contract.** Failure to do so, can have the following negative consequences:

- You will not understand, or fully understand, what you are learning. This will lead to rote learning, and you will not fully benefit from this study unit.
- You will be unable to apply, or fully apply, what you have learnt when, inter alia, drafting a binding and workable contract for a website or advising someone on how to set out the contract on a website.

3.1 INTRODUCTION

economic growth

The Internet has become a vehicle for tremendous economic growth through the development of electronic commerce (e-commerce). Simple retail purchases made through cyber shopping malls are the most common Internet-based transactions. Participation in on-line auctions of goods and airline tickets has become extremely popular. The banking and insurance industries are further industries that make use of e-commerce on a large scale. The use of e-mail in international trade transactions has been increasing rapidly and will continue to expand. At present it seems unlikely that major and complex transactions will be concluded on-line. The negotiating and sending of drafts by e-mail can speed up the process of concluding more complex transactions. Such on-line negotiations will usually be supplemented with a final written contract.

e-commerce

E-commerce on the Internet is only a segment of e-commerce as a whole, which also includes transactions concluded through electronic data interchange (EDI), telex and even fax. We will

primarily focus on Internet commerce. The international initiatives on e-commerce and foreign legislation cover all forms of electronic transactions.

woes of Internet commerce

Internet commerce has currently become less popular because of the sharp drop in IT share prices on the stock market, and also in view of the fact that, until now, few commercial websites have succeeded in making a profit. The growth potential of Internet commerce nevertheless remains enormous.

3.2 LEGAL ASPECTS OF E-COMMERCE

sound business practices

The use of technology is no substitute for sound business practices. The commercial website should therefore be well-designed and the standard contract skilfully drafted. It is extremely important to carefully draft the Internet contract which will regulate the relationship between the merchant and the customer and to set it up on the website in such a way that a valid contract will be concluded between the parties.

problems

Internet commerce differs primarily from conventional commerce in that electronic transactions are largely impersonal and anonymous in nature. This new way of trading creates the following problems:

- The traditional model of offer and acceptance becomes questionable in light of modern technology that is now being used. The question is whether the new way of concluding contracts is different from, or similar to, existing ways of concluding contracts over a distance.
- The virtual world of e-commerce is a paperless world, but formalities such as writing and signature are sometimes legal requirements.
- The possibility of transnational transactions has led to the problem of determining the applicable national legal system that regulates contracts. The Internet has created a virtual borderless world in which cyber contracts are entered into by cyber citizens, but which are still subject to different national laws.
- The actual identity of the other party is uncertain in a virtual world, and must be verified.
- The parties may be located in different parts of the world, which raises the problem of consumer protection and the right to redress.
- The existing systems of payment are ill-suited to a virtual world.
- There is a lack of trust on the part of consumers regarding matters such as confidentiality, security and information about payment.

See generally: Eiselen:
<http://www.cisg.law.pace.edu>

requirements for cyber trade

These problems contribute to a lack of confidence on the part of consumers and business in Internet commerce. Internet commerce requires an accessible, predictable, safe and transparent trading environment, which operates worldwide across territorial borders and jurisdictions. Legal, procedural and technical means have to be employed to ensure the existence of such an environment which will allow e-commerce to flourish.

applicable law

Commercial-law developments have traditionally lagged behind new commercial practices, and here Internet commerce is no exception. Law always redefines contemporary developments in its own terms. Regardless of how revolutionary the Internet is and how inappropriate the application of current legal processes and laws may be, existing legal rules must be applied to this global networking of communities.

3.2.1 The ECT Act: Facilitation of electronic transactions

The Act is applicable to all transactions except those which are specifically excluded in the Act or the Schedules to the Act (see s 4 of the Act).

Chapter 3 of the Act is aimed at facilitating electronic transactions by creating legal certainty about electronic communications and transactions. Part 1 deals with the legal requirements for data messages and Part 2 deals with the communication of data messages and the requirements for the validity thereof.

data message

The term 'data message' is defined in very wide terms: — **data message** means data generated, sent, received or stored by electronic means and includes: (a) voice, where the voice is used in an automated transaction; and (b) a stored record. Data messages includes all messages generated, sent, received or stored by electronic means. It *specifically includes* any Internet messages, e-mail but is wide enough also to include telefax, fax, SMS on a cellphone and instances where voice is used in conjunction with a voice recognition system on a computer. What is clearly excluded is purely voice messages such as telephone conversations, even where the messages is stored as a voice message.

Validity electronic messages

Section 11(1) clearly states that no data message is invalid merely because it is in the electronic format, thereby removing any uncertainty about the legal differences between electronic messages and conventional paper messages.

3.3 CONSENSUS (AGREEMENT)

offer and acceptance

An agreement is reached when two or more parties consent to be bound to each other through contractual obligations. The main components of a valid contract are usually those of offer and acceptance.

express or tacit contract

An express contract may be concluded in writing or orally, or in the form of a mixture of the two – for example, the offer may be made in writing, but may be accepted orally. A tacit or inferred contract is concluded partly or wholly through the conduct of the parties — here the agreement is inferred from the actions of the parties.

If the party through his or her actions accepts a written or oral offer, some commentators are of the opinion that a tacit agreement is concluded, whereas others are of the opinion that an express agreement is concluded. Christie (89–94) argues that such a contract is perhaps best described as partly express and partly tacit. The only difference of any consequence between these two types of contract lies in the manner in which the conclusion of the contract is proved (Christie 94; *Bremer Meulens (Edms) v Bpk v Floros*).

four Internet contracts

The following four ways of concluding an Internet contract have been identified:

- offer and acceptance by e-mail
- an offer made on a commercial website which is accepted by clicking on a button or by doing a specified act (sometimes, the owner of the commercial website merely extends an invitation to do business, and the customer makes the offer by ordering goods or service, which in turn is accepted by the Internet trader)
- an electronic offer and acceptance displayed on the monitors of the offeror and the offeree during an Internet relay chat
- a verbal offer and acceptance during a video conference or Internet voice link

The offer and acceptance can also be a mixture of the above. The offer or acceptance can furthermore be made by more traditional means: orally in each other's presence, by letter in the post, fax, telex or telephone.

3.3.1 Offer

requirements

The requirements for a valid offer are as follows:

- The offer must be definite and complete.
- The offer must contemplate acceptance and (a) resultant obligation(s).
- The offer must come to the attention of the offeree (addressee).

- An offer must as a rule be directed at (a) definite person(s), although it may also be directed at undefined persons.
- The offer must comply with any formalities set by law.

invitation to do business

When one examines the validity of an Internet contract, the first question is whether the contents of a website or electronic mail constitute an on-line ''offer'' or merely ''an invitation to do business''. It is important to note that a true offer must be made with the intention to form a binding contract. An advertisement is therefore usually regarded as a mere invitation to do business, and not as an offer *(Crawley v R)*. This applies to the displaying of goods in a shop, or the placing of advertisements in the press or in circulars (Sharrock 47). The prospective customer who comes forward is deemed to make an offer to buy, and only upon acceptance of his or her offer by the advertiser does a contract come into existence (Sharrock 47–48). An advertisement may, depending on its wording, qualify as an offer if there is a clear indication that the advertiser intended it to be as such *(Carlill v Carbolic Smoke Ball Company)*.

commercial website

A commercial website may serve both as ''shop displays'' and as ''shop sellers'', and may constitute a fusion of advertising and selling. An advertisement or digital image of products for sale on a website is generally directed ''to the world'', and may, depending on its wording, constitute an offer. However, it may also be only an invitation to the world at large to do business in that the electronic order by a prospective client is regarded as an offer subject to acceptance by the Internet trader. The exact intention should be clearly stipulated in the standard terms of the Internet merchant.

From the point of view of the Internet trader it is usually preferable to structure the Internet site in such a way that orders by customers are regarded as offers rather than acceptances. It may happen that the interest in a specific product is oversubscribed by buyers worldwide to the extent that the Internet merchant is unable to fulfil its obligations or that it receives orders from parts of the world to which it does not wish to ship or send its goods or services. In such cases, unwanted orders can merely be rejected by the trader without further legal consequences.

If the Internet merchant wishes to make an offer for the sale of goods to the general public his or her offer should be made with an express statement that the offer is subject to ''first come, first serve'', or ''as long as stocks last'' if stocks are limited. Such a clause is, of course, not necessary if stocks are unlimited. The merchant should also expressly limit the area of delivery in his or her offer.

3.3.2 Acceptance

Prescribed article: Pistorius ''Click-wrap and Web-wrap Agreements'' (2004) 16 n4 *SAMLJ* 568-576

requirements

The requirements for a valid acceptance are the following:

- The acceptance must be unconditional and unequivocal.
- The offer must be accepted by the person to whom it was addressed. Usually, an offer on the Internet is made to the public in general, and any member of the public may accept it. If the offer is made by e-mail, however, it is usually directed at a specific person, and only that person will be able to validly accept the offer.
- The acceptance must be a reaction to the offer — a person cannot accept an offer of which he is not aware.
- The acceptance must comply with any formalities set by law or by the offeror.

manifested

A binding contract is created upon the acceptance of an offer. The acceptance must be manifested through some unequivocal act from which acceptance can logically be inferred.

communicated

The acceptance must also be communicated to the offeror — that is, it must come to the attention of the offeror. The offeror may expressly dispense with communication of the acceptance.

waiver

The need to communicate the acceptance of the offer may also be waived impliedly, by requiring the offeree to signify his or her acceptance by some specified act. The offeror may thus prescribe that the offer could be accepted tacitly by the purchaser by performing a certain act. This act then evidences the purchaser's acceptance of the terms of the contract, and as such is equivalent in law to the signing of a contract.

silence

If the offeror indicates the mode of acceptance, the offeree should adhere to it *(Bloom v The American Swiss Watch Co)*. However, the offeror may not force the contract onto the offeree by stating that the offeree's silence will be construed as acceptance — for example, by sending unsolicited goods through the post (Christie 73; *Collen v Rietfontein Engineering Works*).

application to cyber contracts

In the case of Internet contracts, the traditional model of offer and acceptance becomes questionable in view of the modern technology that is now being used. In most cases, the Internet trader will set up its cyber-trade site from which business will be conducted. In cases in which the site constitutes an offer to

website an offer

be accepted by clients, the traditional model requires subjective knowledge of the acceptance by the offeror before the agreement will come into existence, unless such knowledge has, expressly or impliedly, been waived. In most cases of Internet trade, it will be difficult to tell whether knowledge of the acceptance ever reached the attention of the offeror or, if it is a company, came to the knowledge of a person authorised to contract on behalf of the company.

website an invitation

Conversely, if the site works with the model that it only invites business and that the order by the client constitutes an offer, the contract will come into existence only once the client receives subjective notice of the acceptance by the cyber trader. The trading site should therefore be able to confirm the order to the client. However, there is a danger that the client may never receive notice of the confirmation, in which event no contract will have come into existence.

3.3.3 The ECT Act

Section 22 of the ECT Act puts it beyond doubt that electronic contracts will be regarded as valid and binding.

Acknowledgment of receipt

Section 26 provides that no acknowledgment of receipt is necessary to provide legal validity to any message, unless of course the parties have agreed to such a requirement. A contract will become final and binding once the acceptance is received. It is not necessary that the offeror acknowledge receipt of the acceptance.

3.3.4 Acceptance of standard terms

contracts of adhesion

Standard terms of agreement constitute a modern phenomenon in the law of contract. A party to a prospective contract may include or insist on including its standard terms of agreement as part of the eventual contract. Standard contracts are by nature contracts of adhesion, since the possibility of negotiations is excluded — one simply declares one's acceptance of the standard terms, or one goes without. These contracts are used extensively in almost all economic activities today — from insurance policies, bills of lading, banking, and consumer finance to transport of goods.

''ticket cases''

The rules devised for ''ticket cases'' may be applied to all cases in which the supplier places before the customer a document (or ticket) which is not meant to be signed and which contains the terms on which the supplier is prepared to do business or refers the customer to a document which contains the terms on which the supplier is prepared to do business. These principles were adopted to dispense with the need to obtain every customer's signature, and are therefore used to prove that the customer is bound by the contract.

test

In terms of these principles, the following three-pronged test may be applied to determine whether these standard terms have become part of the contract or not:

- Did the person who received the ticket know there was writing or printing on the ticket?

- Did the person who received the ticket know that the writing or printing referred to terms of the contract?

  If both the above questions can be answered in the affirmative, the terms referred to form part of the contract, but if either of them is answered in the negative, a further question is posed, namely:

- Did the party who issued the ticket take the steps which were reasonably necessary to bring reference to the terms to the notice of the other party?

  If this was done, the terms form part of the contract. If not, the other party is not bound by the terms.

nature of document

Whether the necessary steps were taken is, for the purposes of this last question, a question of fact. The nature of the document is also material to this question: the more contractually obscure or incidental the document is, the less it can be expected to contain contractual terms and the more specific and positive the steps must be to bring these terms to the attention of the customer *(Bok Clothing Manufacturers (Pty) Ltd v Lady Land Ltd).*

was the document actually read

Of course, if it can be proved that the customer has read the document, he or she is bound by its terms, and no enquiry regarding his or her understanding of the document needs to be made. By reading the document and by going ahead with the contract, the customer accepts the offer (through his or her action), and a valid contract is concluded.

website with notice

The rules regarding ''ticket cases'' can find application on commercial websites. These websites then only contain a notice that the use of the website or the placing of an order will be subject to the standard contract of use of the site or of sale. If after application of the three-pronged test it is found that the client is not bound by the standard contract, it does not follow that he or she is not bound by a contract at all. The client will through his or her acts have concluded a tacit contract, which will be regulated by the *naturale* of that specific type of contract that the parties have concluded. The terms of the standard contract will, however, not be binding.

click-wrap contract

''Click-wrapped'' contracts have been specially developed for commercial websites. Basically, they will entail that a client who wishes to register at a website in order to make use of its services or who wishes to purchase goods offered through the ''electronic shop'' will be instructed to ''click'' on a certain icon, thereby indicating his or her acceptance of the terms of the contract. There will usually also be a link to the standard contract, which will be displayed when the client ''clicks'' on that link.

validity

Although these ''click-wrap agreements'' have as yet not been

tested in court, there appears to be no reason why they should not be enforceable. Unlike in the ticket cases, in which the customer is not necessarily aware of the existence of contract terms, the customer in the ''click-wrap'' agreement actually is aware of the existence of contractual terms before he or she makes a commitment to make use of the site or to acquire the goods or services, due to the design and layout of such a website. Furthermore, the ECT Act also makes provision for incorporation by reference through click-wrapped agreements.

3.3.5 ECT Act: Incorporation by reference

Section 11(2) deals with incorporation by reference. It stipulates that information will have legal force and effect even though it is only referred to in a data message even though that information is not actually part of that data message. For instance, an order form may refer to the standard terms and conditions of the trader without being part of the page accessed by the buyer. The mere reference suffices. However such incorporation will only be valid if the reference is such that a reasonable person would have noticed it and where it is accessible to the buyer in a form which is readable, retrievable and capable of being stored. These provisions are in line with the common law position as developed by the courts. Thus, where a website clearly refers to the standard terms of the seller in an obvious place, or where the buyer is required to click on an accept button, the first requirement will have been met. Secondly, the terms must be accessible to the buyer, even if it is on another web page and the buyer must be able to download those terms onto its own computer for future retrieval.

ACTIVITY 3.1

On 25 February 2001, Johnson, the managing director and sole shareholder of MK Motors (Pty) Ltd situated in Maputo, Mocambique, while surfing the net, came across TVS's homepage. He was interested in the Petrosaver that was advertised on this site. After surveying the site, he clicked on an icon that said ''Ordering Petrosavers.'' He was taken to a page that stipulated that the standard terms of agreement of TVS would apply to any transaction between TVS and a customer ordering Petrosavers through the site. Johnson was then faced with two icons containing the following wording: **''Display standard terms and conditions''** and **''Order Petrosavers''**. Johnson was in a hurry, and clicked on the second icon without reading the standard terms. He was taken to a page containing an order form. He ordered 300 Petrosavers at $10 a Petrosaver from TVS via the Inter-

net site. Ten seconds later he received a confirmation of his order, requesting him to confirm the order. He clicked on the icon that designated the correctness of the order. On the same day, TVS dispatched the Petrosavers by container to MK Motors.

The standard terms of agreement, *inter alia*, contain the following terms:

(1) The agreement will become final and binding only upon receipt by TVS of the confirmation of the order by the client.
(2) TVS is entitled to reject any order for any reason whatsoever.
(3) The Petrosavers will be shipped within one week of the conclusion of the agreement.
(4) The Petrosavers will carry a three-month guarantee against any defects, which guarantee will replace all other guarantees against latent defects.
(5) The client is not entitled to reject the Petrosavers for any reason whatsoever, whether they comply with international standards or not, and whether they are defective or not.
(6) No variation of or discharge from the contract will be valid and binding unless confirmed in writing by TVS.

Based on the facts given above, advise TVS on whether its standard terms of agreement will become part of the agreement and whether all of these terms are valid and enforceable or not.

FEEDBACK

Have you also considered the following:

- that the standard terms form the framework against which the actual agreement for the sale of the Petrosavers is to be interpreted
- Section 11(2) of the ECT Act provides that information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message
- Section 11(3) provides that information is regarded as having been incorporated into a data message if such information is (a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and (b) accessible in

a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

- That the fact that Johnson failed to read the standard terms may not be fatal to their inclusion, but that it should also be considered whether Johnson had actual knowledge of their existence, or whether TVS took reasonable steps to bring them to Johnson's attention and that a reasonable client would have noticed them? In other words, the answer will depend on whether the icon ''Display standard terms and conditions'' would be noticed by the reasonable person and whether the standard terms and conditions were accessible as provided for in section 11(3)(b).
- that under the above circumstances, MK Motors makes the offer which is subject to acceptance by TVS, but that the contract is not binding until TVS has received confirmation of the order from Johnson

FURTHER COMMENTS

- The contract between the parties is a contract of sale which would normally be subject to the *naturalia* of the sales contract, unless the parties have agreed to the contrary or have made alternative arrangements. The standard contract contains additional terms, some of which change the *naturalia* of the contract — for instance, the liability for latent defects is changed by the guarantee term (4) and the exclusion clause in (5) above. If, however, the standard terms for some reason do not apply, the *naturalia* will apply.
- Regarding the question whether TVS took reasonable steps to bring the existence and inclusion of the standard terms to the attention of potential customers, one should determine whether the fact that potential customers are taken to a page that clearly refers to the standard terms and are forced to make a choice either to read the terms or to order the goods constitutes, under the circumstances, sufficient and reasonable notice. Therefore, in this case the standard terms will apply.
- If the choice of icons had been between **''Display standard terms and conditions''** and **''Accept standard terms and conditions''**, it would have meant that a click-wrap agreement was concluded. In such an instance, an action by the customer would also have led to the inclusion of the standard terms.

- In both instances, there was no actual consensus, because Johnson failed to read the standard terms and conditions. This is a case of quasi mutual assent. The liability is based on the reliance theory regarding consensus.

3.3.6 Automated transactions

In certain instances a party will communicate with the world through an automated website which requires a minimum of actual human input, but where the system will automatically generate responses to messages received from customers. For instance a website may be programmed to receive orders which have been electronically completed by customers. Once received, the system will generate an acknowledgment of receipt of the order, check the levels of stock, check the payment details of the buyer (for instance with the credit card company) and if sufficient stock is available and payment is cleared, generate a message to the dispatch department to send the item to the buyer.

electronic delivery

Human intervention will only take place where the goods are physically removed from the store and sent to the buyer. Where electronic goods are ordered this may not even be necessary as the goods can be sent electronically without human intervention. For instance if you buy software on the Internet, the software is usually sent without any human intervention. In terms of section 20 where electronic agents are used, the offer or acceptance generated by the electronic agent will be regarded as a declaration of will of the party on whose behalf that computer and electronic agent has been programmed.

definition: automated transaction

An automated transaction therefore is a transaction where one or both of the parties make use of automated systems, i.e. a program that communicates with or responds to third parties without any human intervention. The offer or acceptance is made by the computer program without referring any decision for actual human input. In this case the computer and computer program constitutes an electronic agent.

opportunity to review

Section 20 also contains some protection for natural persons dealing with electronic agents. A natural person will not be bound to a contract concluded with an electronic agent unless the natural person had an opportunity to review the entire transaction before confirming it in order to rectify any mistakes it may have made. However, to be entitled to this protection it is required that a natural person must notify the other party of any mistakes as soon as such mistake is noticed.

ACTIVITY 3.2

Imagine the following scenario: Johnson made a mistake when keying in his order and instead of ''300'' keyed in ''800''. When asked to confirm his order, he did not notice this mistake. A week later, Johnson became aware of his mistake and immediately e-mailed TVS, informing them about it. By then, TVS had already dispatched the goods. Now advise TVS on whether there is consensus between them and MK Motors and on whether MK Motors is entitled to resile from the agreement, either partly or totally.

FEEDBACK

Have you considered the following:

- that actual consensus is not always necessary for a contract to be binding on the parties, but in cases in which there is apparent consensus, although one of the parties is operating under a mistake, the contract will nonetheless be valid and binding if the act of the one party (Johnson, on behalf of MK Motors) induced a reasonable belief in the other party (TVS) regarding his intention, in which case the contract will be binding on the former, despite his mistake
- If, however, an electronic agent acted on behalf of TVS, it will be an automated transaction. In this case Johnson will be protected by the provisions of section 20 of the ECT Act. If there was no opportunity to review the order before submitting it, Johnson will not be bound to the order for 800 Petrosavers. As he notified TVS of the mistake as soon as he became aware of it, (a week later), MK Motors can resile partly from the agreement.

3.4 THE TIME AND PLACE OF FORMATION OF THE CONTRACT

simultaneously determined

The time and place of formation of a contract are determined simultaneously. The time of contracting is the time when the last step which is required for the completion of the contract was taken. The place where the last step was taken is the place of contracting.

purpose

A discussion of the current legal position regarding the time and place of the formation of contracts will help us understand the approach of our courts in this matter. This, in turn, will help us understand how the time and place of the formation of Internet contracts should be regulated.

theories

As you know, there are four possible jurisprudential theories regarding if, when and where a contract is concluded:

- the **declaration theory**, in terms of which the agreement is concluded once the offeree has expressed his or her acceptance
- the **expedition theory**, in terms of which the agreement is concluded as soon as the offeree has sent off his or her acceptance
- the **reception theory**, which holds that the agreement comes into being when the offeror receives the offeree's acceptance, or has access to it
- the **information theory**, in terms of which the agreement is concluded only when the offeror has been informed of the acceptance

3.4.1 Summary of the approach of the South African courts

approach

The approach of the South African courts can be summarised as follows:

- In general, the information theory applies, whether the parties conclude their contract in each other's presence or over a distance.
- The offerer is allowed to expressly or inpliedly deviate from the general rule.
- Mere geographical separation of the parties is not regarded as sufficient indication that the offeror has impliedly dispensed with the general rule. However, such an indication may exist if other factors are also present. In the case of postal contracts, the commercial inconvenience caused by the general rule, the application of a different rule in other legal systems and the trade usage that is generally observed have been regarded as sufficient indications of implied dispensation with the general rule.
- The courts, through analogy, have extended the rules applied in certain methods of communication to other, similar, methods of communication.

3.4.2 Internet contracts

3.4.2.1 Video conferencing, Internet relay chat or Internet voice link

relay chat/voice link

Internet relay chat, or Internet voice link are communication services that are ''full duplex'' and in real time. (Full duplex involves the transmission of data in two directions simultaneously — a telephone is a full-duplex device, whereas a walkie-talkie is a half-duplex device because only one person can transmit at a time see <http://e-comm.webopedia.com>). Communication between the client and the server over the

World Wide Web, is ''instantaneous'' in nature, and will place parties in a conversational situation. In both instances, the information theory should apply.

Video conferencing

Video conferencing over the Internet is the method of communication which comes closest to the parties actually contracting in each other's presence. The information theory should also apply to video conferencing.

3.4.2.2 Communication over the World Wide Web

Acceptances over the World Wide Web differ from acceptances by e-mail as the digital data are transmitted with a ''checksum'', which allows the receiving computer to check that the correct information has been received (Gringras et al 26). Communication between the client and the server over the World Wide Web is also simultaneous in nature, and has the quality of a telephonic conversation, but between two computers, rather than between humans. Either ''party'' will immediately be aware if the other party ''goes off-line''. Many writers are of the opinion that the reception theory should apply to Internet contracts concluded over the World Wide Web (Gringras et al 23; *Cyberlaw* 168).

technicalities

3.4.2.3 E-mail

technicalities

When a message is sent by e-mail the message will first travel to the sender's server. This server acts as a central point for the collection and dispatch of messages from a number of computers. This server then breaks the message into chunks and sends the chunks as a collection of packets, each with an address for the recipient, over the Internet. When the chunks reach the recipient's server the message is reassembled and placed in the recipient's mailbox, where it awaits retrieval. If the e-mail does not reach the addressee, the sender receives a message from his or her service provider, informing him or her that the e-mail could not be delivered. E-mail is **noninstantaneous** in nature and can be even slower than the post.

comparison post

E-mail is unlike the post, for the following two reasons:

- Acceptance of e-mail is far more reliant on the recipient than on the sender. Some e-mail users are permanently connected to their service provider, while others are notified only when an e-mail arrives for them. There will therefore be a lapse of time if a person is not present or if the service provider does not notify the user of a new e-mail. Other users are not connected and have to log in to their service provider on the off chance that there is e-mail for them.
- If the e-mail does not reach the addressee, the sender receives a message from his or her service provider, informing him or her that the e-mail could not be delivered. The sender will

know about this only when he or she reads the message. The sender can also find out if his or her e-mail has been delivered, and when.

comparison telephone

E-mail also differs from telephone communications in the following two respects:

- No ''direct line of communication'' exists between the sender and the receiver of e-mail, as the message is broken into ''chunks'' in the process of delivery. These chunks can even follow different paths to the recipient, through different computers on the Internet. Some of these chunks can be lost, so that the e-mail will be garbled.
- In the case of e-mail, it is impossible to check if an unequivocal acceptance was received. E-mails are sent by means of protocols (ie the agreed format for transmitting data between two devices), which allow computers to pass information to each other. Sometimes, when the protocols are used incorrectly, the e-mail may arrive entirely garbled, and sometimes there may be even a few important characters, such as zeros, missing.

remote logins

It should be remembered that mobile communications with the Internet are possible via a mobile phone or a notebook computer. It is thus naïve to assume that e-mail accepting an offer from *company@plc.uk* was actually sent from the United Kingdom. Such e-mail could have been sent by mobile communications from a plane crossing the Atlantic, or from a beach in Hawaii, or from an Internet café anywhere in the world.

Prior to the enactment of the ECT Act, writers and academics offered widely divided solutions to the vexed question of which theory should be applied in the case of electronic communications.

opinions

The following views are held on the question of which theory is applicable to e-mail:

- The information theory, as the general rule, should apply (Bagrain 51; Van der Merwe *JBL* 141).
- The expedition theory should apply, because e-mail is similar to the post (Gringras et al 23).
- The reception theory should apply (Pistorius *SA Merc LJ 290; Cyberlaw* 168). E-mail is very similar to the electronic communications discussed in the previous section, and the same arguments regarding the reception theory discussed there would apply here.

3.4.3 Emerging international-trade practices regarding the time and place of contracting

importance

International developments are important to us, for the following reasons:

- Internet commerce has the potential of being international in nature. Our solution to the problem of determining the time and place of the formation of Internet contracts by the courts or legislator adapting the common law must therefore be internationally acceptable.
- One of the factors which our courts take into account when determining whether the offeror has impliedly deviated from the information theory is trade usage. In this case, the international trade usage would be important.

3.4.3.1 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

importance

The Model Law (see: < *http://www.un.or.at/uncitral/texts/electcom/m1-ec.htm* >) contains the following two important solutions for Internet communication by e-mail and the World Wide Web:

- The Model law fits in with the reception theory, the expedition theory or even the solution of the EU Directive (see the discussion in the next section), because it explains when a message is dispatched and when it is received.
- The description of the place of dispatch of a message as the place of business or residence of the sender, and the place of acceptance as the place of business or residence of the receiver, constitutes a very realistic solution to the problem of determining the place of formation of the contract. A website is sometimes hosted on a remote server, and the question arises whether receipt of an acceptance is deemed to take place upon its arrival at the remote server, or upon arrival at the local server. Also, mobile communications with the Internet are possible via a mobile phone or a notebook computer, or by logging in from a remote terminal. In all these instances, the places of dispatch and of acceptance will be the places of residence or business of the parties involved.

despatch

Article 15(1) of the Model Law provides that unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator. An information system outside the control of the originator may be the information system of an intermediary or an information system of the addressee (the Guide par 101). ''Information system'' should be

interpreted broadly, as referring to any technical means, and would, therefore, include the communication link between the sender and, for instance, his or her service provider (Glatt 59).

receipt

Article 15(2)(a) provides that if the addressee has designated an information system for the purpose of receiving data messages, the time of receipt of a data message is determined as follows: (1) at the time when the data message enters the designated information system; or (2) if the data message is sent to an information system of the addressee that is not the designated information system at the time when the data message is retrieved by the addressee. ''Designated information system'' refers to a system that has been specifically designated by a party, for instance in the case in which an offer expressly specifies the address to which acceptance should be sent. A data message enters an information system at the time when it becomes available for processing within that information system (the Guide, par 103).

Article 15(2)(b) provides that if the addressee has not designated an information system receipt occurs when the data message enters an information system of the addressee. It seems that an information system would include a mailbox stored on the service provider's computer (Glatt 59).

presumption

Article 15(4) provides that a data message is deemed to be dispatched at the place where the originator has his or her place of business, and is deemed to be received at the place where the addressee has his or her place of business. If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction, or if there is no underlying transaction, the place of business where the principal place of business is. If the originator or the addressee does not have a place of business, reference is to be made to his or her habitual residence.

3.4.3.2 EU Electronic Commerce Directive

contract concluded

The European Union adopted a Directive on Electronic Commerce on 8 June 2000 (see *< http://europa.eu.int/)*. Article 11 contains express provisions regarding the time when an electronic contract is deemed to come into effect. Article 11 provides that an order by a consumer made by technological means must be acknowledged by the service provider without undue delay. The order or the acknowledgement is deemed to be received when the party to whom it is addressed is able to access it.

3.4.4 ECT Act: Time and place of contract formation

Time and place of dispatch and receipt

general rule: information theory

reception theory

According to common law principles a contract comes into being at the time and place where the offeror receives *subjective notice* of the acceptance if the general rule is applied, or where the offeree posts the letter of acceptance if the postal rules apply. The Act takes a third option, namely the receipt approach as its point of departure. The contract comes *into* being at the time and place that the acceptance is deemed received by the offeror, unless the parties have specifically come to another agreement. It is open to the parties to agree when and where the contract will come into being. This agreement takes precedence over all the residual common law principles or the provisions of the Act.

time message sent

time message received

In respect of the time of dispatch section 23 determines that a data message is deemed sent when *it* enters an information system (computer or network) outside the control of the sender. It is deemed received when the complete message enters an information system (computer or network) designated by the receiver or used for that purpose by the receiver.

It is important that the message must reach the recipient intact and complete. If the complete message of acceptance is not received intact on the relevant information system, it is ineffectual and no contract comes into being.

place of receipt/ despatch

Section 23 furthermore determines that a message is deemed sent or received at the usual place of business of the sender or receiver respectively, or if there is no place of business, from the usual place of residence. The description of the place of despatch of a message as the place of business or residence of the sender, and the place of acceptance as the place of business or residence of the receiver, constitutes a very realistic solution to the problem of determining the place of formation of the contract. A website is sometimes hosted on a remote server, and the question arises whether receipt of an acceptance is deemed to take place upon its arrival at the remote server, or upon arrival at the local server. Also, mobile communications with the Internet are possible via a mobile phone or a notebook computer, or by logging in from a remote terminal. In all these instances, the places of despatch and of acceptance will be the places of residence or business of the parties involved.

This provision ensures that the place of dispatch or receipt is linked to a physical place and is not artificially linked to some place such as the location of a server which has no real link to the sender or receiver. This is important in respect of issues such as jurisdiction and the applicable legal system. The Act does not make any provision in respect of jurisdiction or the applicable legal system.

3.4.5 Conclusion

Our courts will apply the reception theory to contracts concluded with data messages. But it is uncertain whether they will apply the information, expedition, or reception theory to contracts concluded by use of both data messages and other traditional communication methods such as post or telephonic conversations.

The offeror may expressly indicate in her offer when the contract comes into being. By doing so she makes sure that a solution acceptable to her applies to the contract that is eventually concluded.

ACTIVITY 3.3

TVS's business is situated in Pretoria and their Internet service provider, Netlink, in Cape Town. MK Motors (Pty) Ltd is situated in Maputo, Mocambique. TVS is not sure where the contract of sale with Johnson was concluded. Advise TVS.

FEEDBACK

Have you considered the following:

- that this is a similar case to the placing of an order over a distance which is accepted by carrying out the order
- that the contract was concluded by means of data messages and section 22(2) of the ECT Act provides that an agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror.
- It is important to note that section 21 provides that the provisions of the ECT Act on time and place of contracting only applies if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for therein.
- When MK Motors ordered Petrosavers it made an offer to purchase Petrosavers and that the terms of the standard contract formed the terms of the offer
- that the standard contract contains an indication when the offer would be accepted and the contract would be concluded
- that the terms of the standard contract should therefore be examined in this regard

TVS has indicated how the offer which the customer makes should be accepted in clause (a) of the standard contract. It

reads as follows: ''The agreement will only become final and binding upon receipt by TVS of the confirmation of the order by any client.'' The place where the contract will be deemed to have been concluded is the place where the last step was taken to conclude the contract. MK Motors makes an offer to buy *Petrosavers* which is subject to acceptance by TVS, but the contract is not yet binding until TVS receives confirmation of the order from Johnson. The standard terms provide that the place where the contract will be concluded will be where TVS receives confirmation of the order. The contract will not be concluded by despatch of the goods nor by reception of the offer by TVS, but upon receipt of the confirmation of the order.

When and where did TVS receive the confirmation of the order? Section 23(b) provides that a data message must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee; and section 23(c) provides that a data message must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence. The contract will thus be concluded when the message confirming the order enters Netlink's information system and when TVS is capable or retrieving the message from its mailbox. Where will this be? TVS's usual place of business in Pretoria.

3.5 FORMALITIES AND SIGNATURES

3.5.1 General

freedom of form

In *Conradie v Rossouw* the Appellate Division (as it then was) accepted the principle that a serious and deliberate agreement to create binding obligations is sufficient to bring a contract into existence, and hence that no special form is required for the formation of a binding agreement. Simple oral agreements are therefore valid and binding unless the law or the parties themselves prescribe formalities such as writing and signature as prerequisites for the agreement to be binding. Contracts which are required to be in writing and signed include the following: any alienation of land, suretyship, donations that still need to be carried out, and credit agreements. Although credit agreements are valid even if they are not in writing, there are other legal consequences that follow if they are not in writing.

types of formality

As far as contracts are concerned, there are usually three types of formality that may be required, namely writing, signature

and some kind of third-party authentication or involvement, such as notarial execution. As far as international sales contracts for movables are concerned, only the first two requirements are relevant. These formalities are required for two purposes, namely legal certainty (writing) and authentication (signature), and may be required either by statute or by the parties themselves.

problems

These two formalities may cause problems in the case of electronic contracts. Many written contracts contain a standard clause which states that no amendments to the contract will be valid or binding unless reduced to writing and signed by both parties, which makes the use of those formalities mandatory in nature.

3.5.2 Writing

solutions

The issue whether e-mail, fax and EDI messages which are not printed out constitute writing, especially in the context of statutory formality requirements, is dealt with differently in different jurisdictions. In many jurisdictions, electronic messages in whatever form are also regarded as writing, provided that a human being can read them in some form or other, even if only on a computer screen or other similar form of display. In the United States, this progressive and realistic attitude seems to prevail. In other jurisdictions, however, there is doubt about this issue.

In South Africa, for example, a statutory requirement of writing was prior to the enactment of the ECT Act deemed not to be fulfilled if the 'document' is in electronic form only. For example, a fax must have been printed out before it would have constituted writing. Once it had been printed out, it was regarded as a document, usually a copy of the original that had been faxed.

3.5.3 ECT ACT: Formalities of writing

Section 12 of the Act ensures that data messages are recognised as writing even where such a formality is required by statute. Formalities may be required either by the parties themselves (the contract must be in writing) or by statute (for instance in the Credit Agreements Act or the General Law Amendment Act of 1950). If information is contained in a data message (see the definition above) and it is stored in a manner where it is accessible for future use, it will be recognised as writing.

However, section 4 of the ECT Act makes provision for certain exclusions in the schedules to the Act. The provisions of the Act are not applicable to the following acts and types of documents:

- Alienation of Land Act 68 of 1981
- Wills Act 7 of 1953
- Bills of Exchange Act 34 of 1964
- Stamp Duties Act 77 of 1968
- a sales contract for the alienation of immovable property
- a long term lease (longer than 10 years) of immovable property
- a will
- a cheque or bill of exchange

3.5.4 Signature

''Signature'' is a wide concept. The Guide to the Model Law provides in par 53 that the following functions of a signature may be noted:

- to identify a person,
- to provide certainty as to the personal involvement of that person in the act of signing,
- to associate that person with the content of a document,
- to attest to a person's intent to be bound by the contents of a signed contract,
- to endorse authorship of a text, or
- to confirm physical presence, namely that at a certain time that party was physically present at a certain place.

Several international initiatives have been taken to secure electronic commerce with some form of electronic-authentication law. Technology has been employed to address and fulfil the authentication and identification functions that are impractical and sometimes impossible when Internet contracts and other digital or electronic agreements are concluded.

Legal initiatives include either electronic-signature laws, or digital signatures, or other public key-styled (''PKI'') technologies. Some states in the United States have introduced legislation that addresses both digital and electronic signatures (see < *http://www.mbc.com* >). *These initiatives may be divided into three categories, namely:*

- prescriptive (see, eg, legislation in Utah, Minnesota, Washington and Missouri)
- criteria-based (see, eg, legislation in California and Kentucky)
- signature-enabling (see, eg, initiatives in Iowa, Kentucky and West Virginia)

3.5.4.1 ECT Act: Electronic Signatures

The Act makes provision for ''electronic signatures'' and ''advanced electronic signatures''. A technology-neutral approach has been adopted. The two concepts, namely ''electronic

signatures'' and ''digital signatures'', should not be confused. Remember that although a ''digital signature'' is an ''electronic signature'', the latter concept is much wider.

form of electronic signatures

Electronic signatures include all technologies for replacing handwritten signatures in the electronic environment, namely by use of a digital pen, PIN-codes, scanned signatures and *digital* signatures. Digital signature is the name for a method of signing electronically by using public-key encryption systems. A digital signature is thus one way in which an electronic signature may be created.

As noted above, the Act creates and gives legal recognition to ''electronic signatures'' and ''advanced electronic signatures''. Before explaining the specific provisions where the legal effect of the use of electronic signatures and advanced electronic signatures are addressed in the Act, the basic concepts will be explained.

definition of electronic signatures

The Act defines an electronic signature as **data which is attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature**. So an electronic signature can be any electronic representation of information which is intended to be a signature.

It may be noted that, alongside the traditional handwritten signature, there exist various types of procedures (eg, stamping, perforation), that are sometimes also referred to as ''signatures'', which provide various levels of certainty. The concept of a signature has been adapted so that in certain contexts a stamp, perforation or even a typewritten signature or a printed letterhead might be regarded as sufficient to fulfil the signature requirement. At the other end of the spectrum, there exist requirements that combine the traditional handwritten signature with additional security procedures such as the confirmation of the signature by witnesses or the function of notaries in certifying a signature (see Guide par 54).

The intention of the person applying the electronic signature may thus be to fulfil any of these functions. The Act gives legal recognition to any method of signing an electronic documents or message, namely anything from a password to a scanned ''wet'' signature, as long as the person applying it intends the data to fulfil the function of a signature and she applies it in the form of data in or attached to, or logically associated with other data.

3.5.4.2 Legal recognition of electronic signatures

Electronic signatures are given legal effect in section 13 of the Act. An electronic signature can now serve as the functional equivalent of a wet signature. Section 13(2) provides that an electronic signature is not without legal force and effect merely

on the ground that it is in electronic form. Electronic signatures can take a variety of forms and, depending on the nature of the transaction, could range between simply writing your name at the end of an email to the use of complex biometric-identification technologies.

However, where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used (see s 13(1)). For example, where a law (such as the Copyright Act) requires a signature, only an advanced electronic signature will be valid. Advanced electronic signatures are presumed to be a valid electronic signature and to have been applied properly, unless the contrary is proved (see s 13(4)). An advanced electronic signature has a higher evidential value than electronic signatures. Should the signatory dispute the validity of his or her advanced electronic signature, he or she bears the onus of proving that in court. In the case of an electronic signature, the normal rules of attribution apply, and a party relying thereon must prove that the signatory validly applied the signature.

Section 13(3) provides that parties may sign a contract electronically. Where the parties to an electronic transaction have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if

- a method is used to identify the person and to indicate the person's approval of the information communicated; and
- having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

Parties to an electronic transaction are free to use other methods as an expression of intent. Furthermore, any other statement is not without legal force and effect merely on the grounds that —

- it is in the form of a data message; or
- it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred (see s 13(5)).

In terms of section 13(5) parties to a contract may agree to use a method other than an electronic signature, to express intent or consent. Electronic agreements may thus be validly concluded through ''click wrap agreements'' by clicking on the ''I agree'' icon, or by expressing intent to be bound through passwords or any other method from which such intent can be inferred.

3.5.4.3 Advanced electronic signatures

What is an advanced electronic signature?

The Act also gives recognition and legal effect to a more ''heavyweight'' form of electronic signature, namely an advanced electronic signature. **An advanced electronic signature is** *defined* as an electronic signature which results from a process which has been accredited by the Accreditation Authority. The compliance of various technical means with an ''advanced electronic signature'' is important as in an electronic environment, the original of a message is indistinguishable from a copy, there is no hand-written signature, and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection.

Where a signature is required by law, that is any statute or the common law, then an a advanced electronic signature must be used. An advanced electronic signature is a signature that was generated by a process which has been approved in terms of section 37. Section 37 makes provisions for authentication service providers to register certain processes as advanced electronic signatures. Where such a signature has been approved, the mere use of it creates a presumption of validity in terms of section 13(4).

3.5.4.4 Accreditation

The next question arises: what is ''accreditation''? Accreditation is defined in section 33 to mean **recognition of an authentication product or service by the Accreditation Authority**. The term ''authentication products or services'' is defined in section 1 to mean **products or services designed to identify the holder of an electronic signature to other persons**. The concept of ''identity'' is broader than mere identification of the signatory by name. The concept of identity or identification includes distinguishing him or her, by name or otherwise, from any other person, and may refer to other significant characteristics, such as position or authority, either in combination with a name or without reference to the name.

More definitions are introduced in section 1, namely ''authentication service providers'' and ''certification service providers''. ''Authentication service provider'' means a person whose authentication products or services have been accredited by the Accreditation Authority. In other words, a service provider that provides advanced electronic signatures. A ''**certification service provider**'' means a person providing an **authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message.**

In other words an **authentication product or service** is a

product or service which also **identifies** a person using an electronic signature. Once accredited, these authentication products or services are recognised as ''advanced electronic signatures''. ''Advanced'' electronic signatures will allow a party to place reliance on its authenticity by shifting the burden of proof onto the signatory to disprove its authenticity.

authentication

Authentication by signature is a bigger problem. In most jurisdictions, it seems that the requirement of signature is met only if a physical signature is affixed to a paper document. ''Electronic signatures'' do not suffice, unless specific provision for electronic authentication has been made.

encryption

Public-key systems may be used to provide assurance to the recipient that the person who sent the message or data is actually its author. Public-key systems may also be used to ensure the integrity of the data transmission. Public-key cryptography can thus be used to generate digital signatures. Public-key encryption assures two things for commercial actors: first, that their messages are secure, and secondly, that other transacting parties are authenticated.

two keys

In this technology, the sender and the receiver of an electronic message each posseses two keys — a public key and a private key — one of which is never shared with anybody, whereas the other is shared with everybody. The two keys correspond, so that whatever is encoded with the one key, can be decoded with the other key.

decryption

Reversal of the public-key cryptography described above creates digital signatures. A digital signature is an attachment to a set of data which is composed by taking the output of a hash function, or digest, of the original data that are encrypted with the sender's private key. The hash function puts the original data through an algorithm, resulting in a data sequence unique to the particular message, but much shorter than the message itself. The digital signature can be decrypted only if the recipient has the correct public key. This allows the recipient to verify the identity of the sender.

trusted third parties

The use of public-key cryptography for digital signatures requires the assistance of a trusted third party — also known as a ''certifier'' who establishes that the holders of public keys are who they purport to be. Certifiers thus identify public-key holders and publish and update public keys — a process known as ''certificate issuance''.

neutrality of technology

It has been noted that attempts to develop rules on standards and procedures to be used as substitutes for specific instances of ''signatures'' are undesirable, as it would create a risk of tying the legal frameworks to a given state of technical development. In general, technology-''neutral'' solutions are thus sought.

3.5.4.5 The definitions may be summarised as follows:

(a) An electronic signature is:

- a method of signing
- by use of data associated with other data
- intended by the user to serve as a signature

(b) An advanced electronic signature is:

- an accredited method of signing
- by use of data attached to, incorporated in or logically associated with other data
- intended by the user to serve as a signature, which also
- identifies that user.

(c) A digital certificate is

- an accredited method of signing
- by use of data attached to, incorporated in or logically associated with other data
- intended by the user to serve as a signature and designed to
- identify the holder of an electronic signature
- attached to, incorporated in or logically associated with a data message

3.5.4.6 Establishment of Accreditation Authority

The Act provides for the establishment of an Accreditation Authority within the Department, allowing voluntary accreditation of authentication products or services in accordance with minimum standards. Of course, if authentication products or services are not ''recognised'' by the authority to meet certain standards, they are not accredited. Such ''unrecognised'' accreditation products or services will not be given legal recognition as advanced electronic signatures even though they may meet all the requirements of being electronic signatures that identify the holder of such signature to other persons. In terms of section 1 of the Act, such products or services will be accreditation products or services, albeit, unrecognised accreditation products or services.

3.5.4.7 Criteria for accreditation

The criteria for accreditation of an authentication product or service as an advanced electronic signature is set out in section 38. Section 38(1) provides that the Accreditation Authority will only accredit authentication products or services which

- is uniquely linked to the user;
- is capable of identifying that user;
- is created using means that can be maintained under the sole control of that user; and

- will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;
- is based on the face-to-face identification of the user.

ACTIVITY 3.4

TVS asks your opinion on the following two questions:

- Does their Internet contract constitute ''writing'', and if not, how can this be rectified?
- How can they be sure of the identity of the party that they are dealing with when concluding on-line contracts?

FEEDBACK

- Section 12 provides that a document or information (a) in the form of a data message; and (b) accessible in a manner usable for subsequent reference is regarded as being in ''writing''. The Internet contract is in writing, and need not be followed up with a fax or a letter.
- The identity of the other party can be assured by requiring that the other party uses an advanced electronic signature.

3.6 AMENDMENT

3.6.1 General

new agreement

Once a final and binding agreement has been concluded between the parties, both parties are bound to the terms as agreed. However, it may happen that circumstances change between the time of conclusion of the contract and performance by the parties, or that the parties may have overlooked aspects which they wish to include in their agreement. Because the initial agreement binds both parties through their consensus, the agreement cannot be amended unilaterally by one of the parties. In general, the agreement can be amended by way of a new agreement or contract between the parties in terms of which they agree to amend the original agreement, and agree on the way in which it needs to be amended.

3.6.2 The EU Directive on Electronic Commerce

information to be provided

Article 10 of the EU Directive on Electronic Commerce (see *< http://europa.eu.int/ISPO/ecommerce/legal/legal.htm >*) provides that service providers must provide information on the technical means that can be used for identifying and correcting input errors prior to the placing of orders.

technological means

Article 11 further provides that service providers must make available to the recipients of their service appropriate, effective and accessible technological means that will allow them (the recipients) to identify and correct input errors prior to the placing of orders.

3.6.3 Restrictions

formalities

The freedom of the parties to amend their contract may be restricted if the contract is one for which formalities have been prescribed by legislation, in which case the parties need to comply with those formalities in respect of the amendment as well, or if the contract contains a non-variation clause. Usually, a non-variation clause will stipulate that the agreement may not be changed or amended unless such amendment is in writing, and signed by both parties.

non-variation clause

confirmed in writing

As amending the agreement will involve actual communication between the parties, this will usually take place by way of e-mail or other conventional forms of communication such as fax or telephone. If the agreement contains a non-variation clause (which would be wise, from the point of view of the Internet trader), and any variation is agreed on orally (ie, by telephone), the amendment must be confirmed in writing, either by fax or e-mail, to make it valid and binding.

ACTIVITY 3.5

After ordering the Petrosavers from TVS on the Internet site as described above, Johnson sent an e-mail to TVS saying that he would like to order Petrosavers on a regular basis, but that he would like to have a one-year replacement guarantee on all products, including the current order. After considering this request, Vuzi phoned Johnson to inform him that he was prepared to amend the agreement as requested. However, he took no further steps in this regard. Johnson wishes you to advise him on whether the amendment is valid and binding, and, if not, what would be sufficient to effect a valid and binding amendment.

FEEDBACK

Have you considered the following:

- whether the non-variation clause in the standard terms applies in this particular situation, and that a telephonic (oral) agreement to vary the contract was insufficient to effect a valid amendment

- that the requirement of an amendment in writing will be met by a data message. For example, an e-mail message would have been sufficient to effect a valid amendment. Consider why the telephonic conversation will not be regarded as a data message (read the definition of ''data message'' in the ECT Act).

3.6.4 Contracting Across Borders

Where a dispute arises between parties concerning a trans-border electronic contract, it must first be determined which courts have jurisdiction to hear the case. Once an action has been lodged, the rules of private international law must be applied to determine the applicable legal system. Trans-border legal issues are discussed by Eiselen in the prescribed extract ''Electronic contracts'' in *Information and Communications Technology Law* (ed. Dana van der Merwe) (2009) at 168-179. Study Eiselen's discussion of jurisdiction and choice of law in paragraph 6.3 ''Transborder legal issues'' from page 168 to page 179.

3.7 PERFORMANCE OF MONETARY DEBTS

3.7.1 Online banking law and payment systems

The primary function of money is to serve as a medium of generally accepted exchange to facilitate business transactions. In order to achieve this purpose money or payment instruments need to be generally acceptable within the context in which they will be used. In most countries money is backed by official recognition, giving it the necessary acceptance and security. In the modern economy old fashioned hard currency has been largely replaced by other forms and methods of payment. Although the client of a bank may notionally have 'money' in the bank, this 'money' is simply an obligation on the bank entitling the customer to draw actual money or make payment to someone else, mostly also by notional money like cheques or electronic transfers.

The fact that money value (notional money) has replaced actual money, has opened up the way for the use of many different payment systems such as cheques, credit cards and electronic payment systems. The growth of the Internet and Internet business has led to the development of electronic payment systems which enables electronic transactions to support this growing commercial activity.

3.7.2 Online payment infrastructure

In most cases the online payment systems are simply applications of existing payment systems like credit card payments. The use of the Internet in applying these payment instruments is simply a way of communicating the instructions for payment between the customer and the paying institution, whether it be a bank or a credit card company. There is nothing new in this situation.

Payment in any transaction is simply the transfer of value by one person to another in compliance with an obligation between the parties. If a person has bought a book online, the seller is obliged to deliver the book to the client and the client is obliged to make payment to the seller. Payment takes place when the monetary value agreed upon between the parties is transferred to the seller by the buyer, or someone on its behalf, in an acceptable manner. No seller is obliged to accept a cheque or any other payment method than legal tender (cash), except if the parties have agreed to that payment medium. If an online seller is prepared to accept a credit card payment or payment by electronic cash then payment by the customer in that medium will be proper performance or payment. Our courts will readily accept that there is a tacit agreement that payment will be accepted in a format other than cash, where the circumstances so indicate.

3.7.3 Law of payment

note

Note the following:

- Payment is a bilateral act.
- Payment must be in legal tender (money), unless the parties have agreed (expressly or impliedly) to another form of payment.
- The type of contract determines when performance has to take place if the parties fail to regulate the matter in their contract. For example, most Internet contracts are contracts of sale, and it is a *naturale* of sale that payment of the price and delivery of the thing sold has to take place simultaneously. In cyber malls, the price usually has first to be paid before the goods are despatched, and the parties have thus changed this *naturale* of a sale.

3.7.4 Electronic payment systems

3.7.4.1 Electronic payment, Internet banking and new payment systems

Electronic payments systems have not adapted to electronic

commerce with ease. Eiselen discusses Internet banking, credit card payments and the development of new payment systems.

Study the prescribed extract Eiselen ''Electronic contracts'' in *Information and Communications Technology Law* (ed. Dana van der Merwe) (2009) at 191-199 on electronic payments.

3.7.4.2 Dangers of electronic payments

The exchange of payment information over the Internet constitutes grave dangers. This information is sensitive and is usually confidential. Most companies authorising payment therefore use strict online security systems to try and prevent this information being accessed by unauthorised parties. If someone has the banking details of a customer as well as the customer's PIN number or access code, that information can be used to fraudulently make transfers or payments from that customer's account.

Security of payment has been one of the biggest factors limiting the growth of Internet trading. Today there are a number of payment systems which are fairly safe by making use of advanced online security features. However, contractually the customer is usually at a disadvantage to prove that payments or transfers were not made by her where the correct access codes or PIN have been used.

The abuse of credit card information is even easier because the card number is readily accessible to anyone to whom the information has been disclosed in the normal run of business. Usually as a matter of policy rather than law, credit card companies will reverse charges which are contested by the card holder. The risk therefore seems to be on the trader who accepts such payments. In order to minimise the risk, Internet traders will usually insist on additional personal information which are not apparent from the credit card itself, such as identity number, address, birth date etc., which can be verified with the credit card company before the sale is finalised.

None of these measures, however, are failsafe or tamper proof. In the event of the fraudulent use of payment information it is important to establish who will bear the risk of such fraud. Is it the customer whose information has been abused or is it the trader who has accepted this type of payment and the risks inherent in it? There are no clear answers to these issues and much will depend on the various agreements between the parties and the conduct of the respective parties. If the client

negligently disclosed its payment information such as access codes or PIN numbers to third parties, it would be unfair to expect the Internet trader to bear the risk of abuse and fraud. Conversely, if the customer carefully guards its information and follows the instructions of the trader, it would be equally unfair to burden the customer with that risk.

note

Take note of the following:

- the legal relationship on which electronic fund transfers (EFT) are based
- the three categories of payment cards
- the fact that, at present, payment by credit card is the most prevalent and important form of electronic payment, and will be such for many years to come
- the tripartite legal relationship governing credit cards
- the advantages and disadvantages of credit-card payments
- the three methods that are used to address the risk involved in paying by credit card, and the disadvantages of each method

The disadvantages involved in paying by credit card have caused new electronic payment systems to develop. You need not study these new payment systems in detail, as they are not used extensively at present.

ACTIVITY 3.6

The order form of TVS provides for payment by the customer with a credit card. The customer has to fill in his credit-card number before sending the order. TVS has received a number of complaints from customers who are afraid of revealing their credit-card numbers over the Internet. The three friends come to you for advice.

- Sina wishes to know how they can assure their customers that it is safe to reveal their credit-card numbers on the order forms.
- Vuzi does not understand why he has received only a few requests for mechanical advice, whereas his Petrosavers are selling like hot cakes.

FEEDBACK

- At present, there is a risk involved in sending sensitive credit-card details to an unknown merchant over the Internet. To combat this risk, TVS should consider using the methods of encryption and central registries in conjunction with each other. Although encryption does protect information in transit over the Internet, it does not protect the customer against misuse of information by the

merchant. The additional use of the central registries eliminates this risk, but causes time lags in the completion of transfers. Although a promising new technology, SET (Secure Electronic Transactions protocol) does exist, it is not used very widely at present.
- A possible reason for Vusi's problem is the fact that only 10 percent of the population qualify for credit cards. These people are the most affluent in society, and are not interested in working on their own cars.

FURTHER COMMENTS

The advantages and disadvantages of credit cards can be summarised as follows:

ADVANTAGES

- The institutional framework of this method of payment is well-established by now.
- Many of the larger card issuers are internationally recognised, which facilitates international payments.
- Payment by credit card has become an internationally accepted method in e-commerce.
- Secure Electronic Transactions protocol, a new technological development, hopes to eliminate most of the risks involved in using credit cards for payment on the Internet.

DISADVANTAGES

- The merchant may misuse the customer's information.
- The use of encryption and central registries may lead to delays in transfers.
- Credit-card payments require central processing of the payment instruction. This makes credit cards unsuitable for low-value transactions, owing to fixed transaction costs.
- Each transaction creates an audit trial, so that each payment can be traced.
- Only 10 percent of the population qualify for credit cards.

3.8 CONSUMER PROTECTION

Prescribed article: Jacobs ''Consumer Protection and the Internet'' *SAMLJ* (2004) 16 n4 529-555.

3.8.1 Introduction

South Africa

Consumer protection is very much in its infancy in South African law, and would hardly warrant separate attention.

European Union

However, since Internet trade is so international in nature, Internet traders dealing with, for instance, European consumers, need to take cognisance of the consumer protection measures which have been legislated in Europe, as they may have an effect on their legal position.

At this stage, there is a great deal of awareness regarding the harm that may be inflicted upon unwary consumers participating in e-commerce on the Internet. The Green Paper (75–76) says the following in this regard:

> The electronic market place offers consumers unprecedented choice and twenty-four hours accessibility and convenience. It gives established marketers and new entrepreneurs low-cost access to a virtually unlimited customer base. With these benefits also comes the challenge of ensuring that the virtual marketplace is a safe and secure one to purchase goods, services and access electronic information. Consumers must be confident that the goods and services offered online are fairly represented and that the merchants with whom they are dealing (many of whom may be located in another part of the world), will deliver their goods in a timely manner and are not engaged in illegal business practices such as fraud or deception. Consumers must be protected against the following dangers:
>
> 1 Unsolicited goods and communication;
> 2 Illegal or harmful goods, services and content (eg pornographic material);
> 3 Dangers resulting from the ease and convenience of buying on-line;
> 4 Insufficient information about goods or about their supplier; since, the buyer is not in a position to physically examine the goods offered;
> 5 The abundantly accessible nature of a website;
> 6 The dangers of invasion of privacy, as discussed in the section below;
> 7 The risk of being deprived of protection through the unfamiliar;
> 8 inadequate or conflicting law of a foreign country being applicable to the contract; and
> 9 Cyber fraud.
>
> On the other hand, suppliers are in some danger themselves, through exposing themselves to unknown liabilities, especially in view of the fact that the law on Internet commerce is as yet poorly defined, and differs from country to country. Consumer confidence also requires that consumers have access to fair and effective redresses if they are not satisfied with some aspects of the transac-

tion. To ensure strong and effective consumer protection in an online environment and obviate the need for a long and arduous litigation process, alternative and easy-to-use mechanisms for consumer dispute resolution, redress and enforcement mechanisms are required. Again beyond enforcing current law and developing strong consumer protection policies, consumers must be made aware of the availability of instruments to help them use Internet safely.

A few important developments in this area of law took place recently. For instance, in the past two years documents have surfaced that have an impact in the consumer protection principles' as we know them now. The first document is Privacy and Data Protection Dicussion Paper 109 (Project 124), which came out last year (October 2005). This document highlights information protection principles that can help in shaping the drafting of new information laws. The other document is the Draft Consumer Protection Bill of 2006. This document provides a broad framework for consumer protection in South Africa.

3.8.2 Directive on the Protection of Consumers in Respect of Distance Contracts

Directive

The Directive on the Protection of Consumers in Respect of Distance Contracts (see <*http://europa.eu-int/information_society/topics/ebusiness/ecommerce/index_en/htm*>) was adopted in 1997. The Directive is an important step towards homogeneous consumer protection in the European Union. It is predicted that the Directive will have a great impact on contracting on the Internet.

cyber trade

The Directive affects the practices of those who sell goods and services to European customers on the Internet. Communication over a distance includes contracts made by using e-mail or websites. The Directive also covers the sale of goods or services over the Internet or through a mixture of means of distance communication. Where an advertisement on a website makes mention of a telephone number to be contacted with a view to concluding a contract, the Directive concerned could become applicable.

information

Article 4 prescribes certain information (concerning matters such as the main characteristics of the goods, and the prices) which must be provided to the consumer before a distance agreement is concluded. The information may be provided on any medium that is appropriate to the means of distance communication that is used (such as on e-mail or multimedia). In addition, written confirmation must be furnished to the consumer on another durable medium (see art 5(1)). Gringras et al., are of the opinion that the term ''durable medium'' will not include e-mail.

''cooling off''

Article 6 provides the consumer with a right of withdrawal. The effect of this provision is to provide consumer parties to distance contracts the right to withdraw from the contract at will within seven working days. This exception ensures a ''cooling off'' period, but it does not apply to unsealed video cassettes, records or computer software. The consumer's right of withdrawal does not extend to digitally supplied goods.

3.8.3 The EU Directive on Electronic Commerce

3.8.3.1 Information to be made available

Article 5 of the Directive on Electronic Commerce also provides for the following information to be made available to the consumer:

information

- the name of the service provider;
- the geographical address of the service provider;
- details regarding the service provider, such as the e-mail address;
- the trade register in which the service provider is registered; and the registration number (if applicable);
- particulars of any authorisation scheme that may be applicable;
- whether the service provider is registered with a professional body, and where the professional rules may be accessed (as applicable to regulated professions);
- if the service provider undertakes any activity which is subject to VAT, the applicable VAT identification numbers;
- if applicable, the prices must be stated clearly, and the service provider must indicate whether the price is inclusive of VAT and delivery costs.

3.8.3.2 Commercial communications

clearly identified as commercial communications

Article 6 provides that commercial communications must be clearly identified as such, and that they must contain the following information:

information contained in commercial communications

- the natural or legal person on whose behalf the communication is made
- promotional offers must be clearly identifiable as such, and the conditions to be met in order to qualify must be easily accessible and must be presented clearly and unambiguously
- promotional competitions and games must be clearly identifiable as such, and the conditions for participation must be easily accessible and must be presented clearly and unambiguously

3.8.3.3 Unsolicited commercial communications

Article 7 of the Directive provides that unsolicited commercial communications must be clearly identified as such. The Directive also provides that consumers who do not wish to obtain such communications may register themselves in opt-out registers. Service providers undertaking unsolicited commercial communications must regularly consult the opt-out registers to ensure that they do not send such communications to private persons registered in those registers.

opt-out registers

3.8.4 UNSOLICITED COMMUNICATIONS (SPAM)

3.8.4.1 USA

CAN-SPAM Act

In the USA spam is regulated under the *Controlling the Assault of Non-Solicited Pornography and Marketing Act* of 2003 (CAN-SPAM Act). The Act came into operation on the 1st of January 2004. Prior to this Act, different states in the US had either anti-spam legislations or provisions in their existing Acts that regulated spam. The majority of the states in the US followed the opt-out mechanism, with a few favouring the opt-in. It is not surprising, therefore, that the federal law (CAN-SPAM Act) favours the opt-out mechanism. Opt-out means that one can send spam provided the recipient is given an opportunity to indicate that he or she does not want to receive further spam. The congressional findings with regard to spam included:

opt-out

congression findings

- the convenience and the efficiency of electronic mail are threatened by extremely rapid growth in the volume of unsolicited commercial electronic mail;
- the receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail;
- the receipt of large unwanted messages also reduces the convenience of electronic mail; and that
- many senders of unsolicited commercial electronic mail purposely disguise the source of such mail (see s 2(a) of the CAN-SPAM Act).

Definition: commercial mail message

The term ''commercial electronic mail message'' is defined in general as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose) (see s 3(2)(A) of the CAN-SPAM Act). The commercial electronic mail message does not include a ''transactional or relational messages'' (s 3(2)(B)). A ''transactional or relational message'' means an electronic mail message whose primary purpose is to facilitate, complete

Definition: transactional or relational messages

or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; or to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient (s 3(17)(A)(i-iii)). The above shows that there must have been a relationship that existed between the receiver of such messages and the sender, and therefore, this cannot be regarded as spam.

requirements

There are requirements for the transmission of commercial electronic messages that have to be met before the sender can send spam. These requirements include:

- *Prohibition of false or misleading transmission information*. This Act makes it unlawful for anyone to initiate the transmission to a protected computer of a commercial electronic mail message that contains or is accompanied by header information that is materially false or materially misleading. A header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin (s 5(a)(1)(C)). The term ''header information'' means a source, destination and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message (s 3(8)).

header information

- *Prohibition of deceptive subject headings*. It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, fairly implied on the basis of objective circumstances, that the subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (s 5(a)(2)).
- *Inclusion of return address or comparable mechanism in commercial electronic mail*. The electronic message sent to the recipient must contain a functioning return electronic mail address or other Internet-based mechanism that is clearly and conspicuously displayed so that the recipient may use it to submit or reply to that e-mail in order to inform the sender that they do not want to receive future mailings from the sender (s 5(a)(3)).
- *Prohibition of transmission of commercial electronic mail after objection*. This deals with the opt-out mechanism, which requires that senders must honour the recipients' request to

be removed from the senders' list. The sender is given 10 business days in which to respond to that request (s 5(a)(4)(i-ii)).

- *Inclusion of identifier, opt-out and physical address in commercial electronic mail.* The messages sent to recipients should be clear and conspicuous identification that the message is an advertisement or solicitation. A valid physical and postal address of the sender should be given, as well as a clear and conspicuous notice of the opportunity to decline to receive commercial mail messages (s 5(a)(5)(i-iii)).
- *Aggravated violations relating to commercial electronic mail*. The Act also prohibits the harvesting of addresses and dictionary attacks from public sites such as usenets, chat forums etc (s 5(b)(1)(A)). A dictionary attack is the obtaining of email addresses by using a computer program that generates possible electronic email addresses by combining names, letters or numbers.

dictionary attacks

- *Placing warning labels on commercial electronic mail containing sexually oriented material.* In cases where an email of sexually oriented material is sent, the subject heading must specifically state that the email contains material of that nature. If it does not, the sender will be liable (s 5(d)(1)).
- *Knowingly promoting business with false or misleading transmission information.* The Act also prohibits promotions made by the business in the knowledge that the header information was misleading or false, or in the event that it should have known this and should have taken reasonable steps or action to prevent its transmission (s 6(a)).

There are also penalties attached to the act of spamming. State officials may institute civil actions against the perpetrator(s) on behalf of the recipients, and claim damages from them of up to $2 million for any violation of section 5 (s 7(f)(1-3)).

3.8.4.2 Australia

In Australia, spam is regulated under the Spam Act 129 of 2003, which came into operation on 11 April 2004. This Act makes it illegal to send spam. Australia favours the opt-in mechanism. Opt-in means that the sender must first obtain the user's permission before sending a commercial mail message (spam). The Act sets up a scheme for regulating commercial email and other types of commercial electronic messages. Commercial electronic messages are defined as an electronic message, having regard to the content of the message, the way in which a message is presented and the content that can be located using the links, telephone numbers or contact information. One of the

Spam Act opt-in

Commercial electronic messages

prohibition under Spam Act

purposes of such a message is to offer to supply goods or services or advertise or promote goods or services (s 6(1)(a-f)). The Act prohibits the following:

commercial message with Australian link

- *The sending of unsolicited commercial electronic messages*. A person must not send, or cause to be sent, a commercial electronic message that has an Australian link and is not a designated electronic message (s 16(1)). Commercial messages that have an Australian link are those messages that originate from Australia; or the individual or organisation who sent the messages is an individual that is physically present in Australia when the message is sent; or the computer server that is used to access the message is located in Australia (s 7(a-e)).
- *Commercial electronic messages must include information about the individual or organisations that authorised the sending of the message* (s 17). The message sent must clearly and accurately identify the individual or organisations that authorised the sending of the message; or the message must include accurate information about how the recipient can readily contact that individual or organisation (s 17(1)(a-d)).
- *Commercial electronic messages must contain a functional unsubscribe facility.* The messages sent must have a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual (s 18(1)).
- *Address harvesting software must not be supplied, acquired or used* (s 20).
- *An electronic address list produced by means of address-harvesting software must not be supplied, acquired or used* (s 21 and 22).

The main remedies for breaches of this Act are civil penalties and injunctions against the perpetrators. The court may order the perpetrators to pay a penalty to the Australian Government (s 24 read with s 26(1)). The court also limits the maximum amount that a court may order the defendant to pay the Government (s 25(3)-(4)).

3.8.5 ECT Act: Consumer protection

3.8.5.1 Scope

Chapter VII contains the consumer protection provisions of the Act. Section 42 determines which type of transactions are subject to the provisions of the Act and which are excluded. The following list contains some of the exclusions:

- financial services, investment services, insurance and re-insurance operations, banking services;

- auctions;
- the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;
- where the goods are made to the consumer's specifications; are clearly personalised; by reason of their nature cannot be returned; or are likely to deteriorate or expire rapidly;
- where audio or video recordings or computer software were unsealed by the consumer;
- for the sale of newspapers, periodicals, magazines and books;
- for the provision of gaming and lottery services; or
- for the provision of accommodation
- transport; and
- catering or leisure services

3.8.5.2 Information to be provided

The consumer protection provided is based on providing the prospective buyer or client with sufficient information on the products or services to be provided in order for the client to make an informed decision on the products, the company it is dealing with and any regulatory bodies to which the company subscribe. Therefore the website must contain:

- full information on the physical whereabouts of the company, its identity, registration number and office bearers;
- full information on the goods or services to be provided and their quality and characteristics;
- the full price including any additional costs such as insurance, postage and transport;
- all terms of the agreement;
- estimated time of delivery;
- payment method and security provided by the seller;
- the return and exchange policy of the seller.

The seller or service provider must also provide the consumer with an opportunity to review the entire transaction, including any standard terms, to correct any mistakes and to withdraw from the transaction after review but before final acceptance. Failure by the seller or service provider to provide all of this information or the opportunity to review and correct, makes the contract liable to cancellation within 14 days of receipt of the goods.

The seller is obliged to make use of a payment system that is sufficiently secure to protect the payment information of the consumer. Failure to do so makes the seller liable to any damages the consumer may have suffered as a result of the abuse of its payment information due to such insufficient security measures.

3.8.5.3 Cooling-off period

The most contentious consumer protection provision of the Act is the seven day cooling off period provided for in section 44. The consumer is entitled to cancel any agreement without reason within 7 days of the receipt of goods or within seven days of the contract where services are involved. The consumer is only liable for the cost of returning the goods. Where payment has already been made prior to cancellation the consumer is entitled to a full refund.

3.8.5.4 Unsolicited goods or messages

Section 45 deals with so called 'spam', that is data messages which has not been solicited by the consumer. This type of advertising is very common on the Internet. In terms of this provision any sender of spam must provide the receiver with an opportunity to unsubscribe from the mailing list whereupon the spammer must stop sending the unwanted mail or messages. It further provides that no consumer will be bound to an agreement where the consumer has failed to respond to an unsolicited message or where unsolicited goods or services have been sent to the consumer. The inaction of the consumer may not be regarded as an acceptance. Contravention of these provisions is an offence in terms of the Act and punishable in criminal proceedings.

3.8.5.5 Performance

The seller or service provider must perform within 30 days of the order otherwise the consumer is entitled to cancel the agreement. The seller must therefore dispatch the goods within the thirty days allowed for performance. The seller is also obliged to inform the consumer if it is unable to fulfil its obligations within this period and must return any payments already made.

3.8.5.6 Exclusion of rights

These provisions are applicable to all consumer transactions despite the applicable legal system in terms of section 47. Thus, where a South African consumer has ordered goods from an Australian provider, these provisions will apply even if Australian law is the applicable legal system. Furthermore, a seller or service provider is not entitled to exclude the provisions of this chapter. Such exclusion is null and void.

3.8.5.7 Draft Consumer Protection Bill

See the Draft Consumer Protection Bill of South Africa (Notice 418 of 2006) GG no. 28629. Especially, three of the fundamental rights eg the Right to confidentiality and Privacy (Part B

sections 12-15); the Right to disclosure and Information (Part D, sections 25-34) and Right to fair and responsible marketing and promotion (Part E, sections 35-44). This document is accessible at <*http://www.polity.org.za/pol/notices/2006*>

3.8.6 Privacy Directive

personal data

The Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data (see <*http://europa.eu.int/information_society/topics/ebusiness/ecommerce/index_en.htm*>) requires that the consent of an individual be obtained before the collection and use of personal data (art 7). Article 10 of the Privacy Directive also requires that the purpose for which the data are being collected be disclosed to the individual.

''click data''

The transmittal of personal data to other countries that lack ''adequate laws'' for the protection of personal data is prohibited (art 25). Information on e-consumers — also called ''click data'' — is fast becoming a commercial commodity. The Privacy Directive will have a profound influence on the debate emerging on the rights pertaining to ''click data''.

3.8.7 ECT Act: Privacy Protection

The Act contains a number of provisions on the protection of privacy or personal information in Chapter VIII. However, the importance of this section is diminished by the fact that these provisions are not compulsory but may be voluntarily subscribed to (section 50(2)).

Section 51 sets out the different data principles that must be adhered to by a party subscribing to these principles. These principles are somewhat loosely based on the data protection principles contained in the European Directive on the protection of personal data and is considered to be the minimum standard required from someone dealing with personal data. These principles are also only applicable to data which has been collected electronically, further restricting the scope of this protection. There is also no sanction in the Act where a party does not adhere to these principles.

The following are the principles contained in section 51:

- A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

- A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
- The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
- The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
- The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
- A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.
- The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
- The data controller must delete or destroy all personal information which has become obsolete.
- A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

See the 8 information protection principles as laid out in the Privacy and Data Discussion Paper (Project 124 October 2005).

ACTIVITY 3.7

Vuzi has been getting quite a few orders for his Petrosaver from individual buyers in Europe. He has heard that certain European directives may be applicable to these transactions. TVS asks your opinion on the following:

- Which Directives may be applicable to the Petrosaver orders?
- Should it make the site compliant with the Directive/s?
- What steps should it take to make the site compliant with the Directive/s?

FEEDBACK

- In answering this question, you should have noted that the following directives are applicable: the Directive on the Protection of Consumers in Respect of Distance Contract; the Directive on Electronic Commerce and the Privacy Directive. You should have briefly stated why these directives are deemed to be applicable.
- TVS should make the site compliant with the Directives, which may be good practice; or TVS can stipulate that South African law will be applicable to the contract. This option may, however, not be effective if TVS has to enforce its contract in a European court, because of jurisdictional requirements.
- In order to make the site compliant, TVS first of all needs to protect the personal information of consumers. Secondly, customers should be provided with the necessary information — regarding both with reference to TVS and the Petrosaver product. The Distance Selling Directive must also be complied with, — by *inter alia* confirming the details on a ''durable medium'', and by providing the consumers with a ''cooling-off'' period.

3.9 CHECK LIST FOR A STANDARD AGREEMENT

The cyber trader can determine the terms and conditions upon which he or she is prepared to do business by drafting and including standard terms and conditions on the website. The following check list should be kept in mind to ensure that all the issues that were canvassed above are adequately provided for:

- The time that and the place where the agreement will become final and binding and all actions that are necessary to achieve this, such as confirmation and receipt of the confirmation. If there are any limitations regarding the duration of the offer, they should also be stated.
- Any formalities such as writing, electronic authentication (''electronic signature'') or confirmation that need to be complied with to bring the contract into being.
- Terms and conditions of payment, including the currency in which payment must be made, as well as liability for any taxes, or surcharges to be paid.
- A jurisdictional clause which determines which court or courts will have jurisdiction in the event of a dispute. For South African traders, this will usually be a Division of the South African High Court.
- A choice-of-law clause stipulating which legal system will be applicable to the contract, and also the relationship between

the parties. In the case of South African traders, this will usually be South African law.

- The consumer protection provisions of Chapter VII and make sure that all the aspects and requirements contained therein are dealt with. More specifically care must be taken to include the reference to the cooling off period as required, that the consumer is given an opportunity to review the transaction and change or withdraw from it and that all the information required in section 44 is provided.
- Clauses relating to common-law guarantees or liability that he or she wishes to vary or exclude, such as liability for latent defects, et cetera. These clauses should also deal with guarantee periods, his or her policy regarding returns and repairs of defective products, et cetera.
- Clauses stipulating when and where the transfer of ownership will take place.
- Clauses regulating the method and timing of delivery and transport of goods and the liability for payment.
- Clauses dealing with the availability of stock.
- Limitations regarding the geographical area where deliveries will be made, or services will be performed.
- A clause dealing with the risk of damage to or loss of the goods and their insurance while being transported, and the liability for the costs involved.

STUDY UNIT 4

Copyright implications of the Internet

Tana Pistorius

OVERVIEW

In this study unit, we shall explore the implications of e-commerce on intellectual-property rights, especially on copyright works in digital format. We shall examine the copyright implications of linking, framing and the creation of mirror sites on the Internet. Service-provider liability for hosting infringing material and the limitations of liability of OSPs for copyright infringement will also be examined.

LEARNING OUTCOMES

After completing this study unit, you should be able to do the following:

- understand the impact of e-commerce on intellectual-property rights
- understand the copyright implications of the digitisation of works
- understand and interpret the international treaties
- apply the law to questions regarding infringement by linking, framing or the creation of mirror sites
- understand and apply the concept ''contributory infringement''
- explain and apply the rules regarding the limitation of service-provider liability
- interpret and evaluate the position obtaining in South Africa as compared with the position obtaining in other jurisdictions

SETTING THE SCENE

TVS's website is called ''TSV-ALL'', and the homepage is divided into the following three parts: ''TSV-Art'', ''TSV-Ewrite'' and ''TSV-auto'':

- ''TSV-Art'' — a catalogue containing photographs of Sina's artworks. Some of her prints may be bought on-line.

- ''E-writing'' — Tim's short stories and two chapters of a novel, which he is in the process of writing
- ''E-mechanic'' — Vuzi's advice on mechanical matters which may be requested at R50 per request responded to

Tim is giving subscribers to his website the opportunity of following the creation of his novel. He adds a few pages to the book every week. He has asked subscribers to post suggestions on how the story line could develop on a bulletin board. Sina has added a new feature to ''TSV-Art'', namely a short course on painting techniques. She uses the tutorial matter she received from the University of Higher Learning as her course material, and photographs of various established artists' works to illustrate the various techniques. Students that have enrolled for the course may send Sina examples of their work for evaluation. Vuzi has asked Thieu to create links from Netlink to the website of two major motor-vehicle manufacturers, namely Wolwa and Dienwoo. He creates the links directly to Wolwa and Dienwoo's motor-vehicle repair manuals. He has also created links to his website from various on-line auction sites.

4.1 INTELLECTUAL PROPERTY AND E-COMMERCE

implications of e-commerce

Intellectual property rights are legal means to protect and balance the interests of an individual against those of the public. This is done in terms of disclosure, dissemination, alteration, use and abuse of ideas, with an exclusive right to control and profit from invention and/or authorship of such intangible goods, services and ideas.

It has become relatively easier to infringe intellectual property through the use of electronic technologies. Therefore, there is an urgent need to formulate a system of laws that define and protect intellectual property as a response to technological change, particularly emerging circumvention technologies that are constantly defying copyright on electronic systems. In this context, it becomes increasingly challenging to ensure intellectual property rights and related neighbouring rights are applied to the electronic environment in a manner that is promoting e-commerce. South African intellectual property law is not fully equipped to deal with the implications of the Internet, convergence, multimedia, digital technology and hence e-commerce. (Green Paper 56, 57).

4.2 COPYRIGHT IMPLICATIONS OF THE DIGITISATION OF WORKS

binary bits of ''0's'' & ''1's''

The digitisation process reduces information into binary bits of ''0's'' and ''1's''. This is an essential function of all computerised technology (see Cornish 13–60).

4.2.1 Traditional notions of copyright

traditional notions of copyright

The advent of the Internet has changed the underlying assumptions of the original copyright laws entailed in the Copyrights Act 98 of 1978. The application of traditional copyright law to open public, global networks such as the Internet is hindered by the fact, that traditional protection of intellectual property rights has always specifically referred to the protection of information contained in tangible media such as books (Green Paper 57, 58).

Traditionally, copyright works have the following characteristics:

traditional works

- The works are classified into different categories, for example literary works, artistic works, computer programs, et cetera.
- each category of works has certain exclusive rights, for example for literary works these include the right to make reproductions; to make adaptations, to publish a work, et cetera.

4.2.2 Copyright law and e-commerce

The 1978 Act provides copyright protection for a wide variety of works, namely literary works, musical works, artistic works, cinematograph films, sound recordings, broadcasts, programme-carrying signals, published editions and computer programs.

We may now ask which of the abovementioned copyright works are being used in e-commerce? The following are normally found on websites:

- information on web pages consisting of text, brochures, product specifications, sounds, songs, melodies, videos, photographs, drawings and other graphic works;
- information and products, such as music, videos, computer programs and text (electronic books);
- computer programs that control the websites' systems; and
- contributions on bulletin boards by newsgroups and other individuals.

The following copyright works are thus at issue:

- literary works (text, brochures, product specifications, electronic books and the lyrics of the songs);
- artistic works (photographs, drawings and other graphic works);
- music works (sounds, songs and melodies);
- sound recordings (recordings of music);
- cinematograph films (videos); and
- computer programs

4.2.3 Digitised works

> The convergence of traditional forms of communication into a single electronic environment presents challenges in the attempt to amend the Act and accommodate this new environment. (Green Paper 57)

multimedia

Dealing with copyright in mixtures of different kinds of work, or ''multimedia'' is a totally new experience. Digitised works will make it easier to combine what up to now have been *separate* categories of work, but, these ''combined works'' are difficult to classify (see *Sameulson Rutgers Comp & Tech LJ* 333).

In summary, we can say that, the digitisation of works has the following consequences:

consequences of digitisation

- previously distinct classes of work have merged into multimedia products
- a homogeneous medium of storing and transmitting works has been created
- it is difficult to classify multimedia products
- it is difficult to determine exclusive rights for each category of works, for example, a previously distinct musical work, a computer program and a literary work may have been fused into a multimedia work
- digitalisation and networking alter the traditional means of using copyright works

4.2.4 Causes of concern: protection of digitally-based works

> Copyrights are referred to as the rights to ensure protection of information from duplication and distribution. Computers are changing the way that copyrighted goods can be illegally copied and distributed. All of this occurs cheaply and easily. This creates new challenges for copyright owners and law enforcement agencies in that the distinction originally drawn between copying and distribution is blurred. (Green Paper 60.)

Works in digitised format all have the same characteristcs, which makes it very difficult to protect the copyright subsisting in such works (see Dreier *Copyright World* 36). This is so because these digitised works, by nature, share the following characteristics:

characteristics of digitised works

- easy to copy or capture data
- easy to distribute or transmit
- easy to manipulate or edit
- easy to store data
- easy to search or link data
- different rights for different types of work are not available any more, because of persisting classification problems

4.2.5 Copyright implications

If digitised works are stored or made available for access, or if they are transmitted without authorisation, it is difficult to establish copyright infringement, for the following reasons:

difficulties

- It is difficult to establish the identity of the person who transmitted an infringing copy of a work — was it the host; the access provider, or a remote user?
- The removal of rights-management information makes it difficult to prove copyright ownership.

ACTIVITY 4.1

Tim approaches you for legal advice. He informs you that a friend of his, Leonie, has made a copy of a poem that he wrote, entitled *''Still love and war''* without his authorisation. Leonie has included Tim's work in her own multimedia work, entitled *''War''*, and has put this work on her website. Explain to Tim the copyright implications of the digitisation of works.

FEEDBACK

Make sure that you have explained the following: what digitisation is; that you have described the characteristics of digitised works, and the consequences of the digitisation of works. Here Tim's work, previously a distinct literary work, has become fused in a multimedia work. This is possible, because it is so easy to copy, manipulate, edit and store digitised works.

You need not concern yourself with copyright infringement yet, we only need you to understand the implications of digitisation of works.

4.3 INTERNATIONAL CONTEXT: SCOPE OF RIGHTS AND EXCEPTIONS

4.3.1 Infringement of copyright

Infringement of copyright in a work may be either direct or indirect. The infringement is direct when the infringer does, or causes any other person to do, any of the acts specifically designated in the Act as the sole prerogative of the copyright owner, without having obtained the permission of the copyright owner (see s 23(1)).

Sections 6–11 of the Act contain provisions for each of the categories of works setting out which acts may be done or authorised exclusively by the copyright owner. Thus, for example, in relation to a literary or musical work section 6 provides that the copyright owner shall have the exclusive right

to do or to authorise the doing of the following acts: the reproduction of the work, its publication, its performance in public, a broadcast of the work, the making of an adaptation of the work, and so on. An adaptation with reference to a literary work means a translation of the work.

4.3.1.1 Reproduction

The protection which the copyright owner enjoys as far as the reproduction of the work is concerned is very extensive, since the work may not be reproduced (without his permission) **in any manner or form**. In relation to a literary or musical work the term ''reproduction'' includes a reproduction in the form of a sound recording or cinematograph film. Also, it is important to remember that the definition of the term ''reproduction'' includes a reproduction made of a reproduction of a particular work (sect 1(1)).

The definition of the term ''reproduction'' in section 1(1) where it is expressly stated that in relation to any work the term includes ''a reproduction made from a reproduction of that work''. This means that the making of a copy of an intervening copy of a work (indirect copying) amounts to an infringement of the copyright in the original work.

The right to make reproductions of a work is applicable to reproducing a work in digital format, whether of a permanent, temporary, or transient nature. Section 2(2) states that a work that subsists of digital data or signals complies with the requirement of material embodiment. The term ''reproduction'' is also interpreted widely. It has been held that the making of temporary or permanent electronic copies of works amount to copyright infringement. In *Pastel Software (Pty) Ltd v Pink Software (Pty) Ltd and another* 399 JOC (T) it was held that the temporary and transient electronic reproduction of a work (in this instance on a computer screen) constitutes copyright infringement.

4.3.1.2 Reproduction right: WCT

reproduction right

The WIPO Copyright Treaty is of particular importance as far as the ''reproduction right'' is concerned. Reproduction is applied to the storage of works in digital systems of permanent, temporary, transient and incidental nature. The Diplomatic Conference adopted the following statement on this issue:

> The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention.

digital environment

There is international agreement that permanent electronic storage of a work is a restricted act. America's White Paper on Intellectual Property and the National Information Infrastructure notes the following:

examples of copying

> It has long been clear under US law that the placement of copyrighted material into a computer's memory is a reproduction of that material … in each of the following instances set out below, one or more copies is made … 'When a printed work is ''scanned''' into a digital file, a copy — the digital file itself — is made … ''When other works — including photographs, … are digitalised, copies are made …. Whenever a digitalized file is ''uploaded'' from a user's computer to a bulletin board system (BBS) or other server, a copy is made. Whenever a digitalised file is ''downloaded'' from a BBS or other server, a copy is made. When a file is transferred from one computer network user to another, multiple copies generally are made.

To summarise: the following will all amount to copyright infringement (reproduction) of a work: to save a work on the hard disk of a computer or on a CD ROM disk, to download a work which has been placed on a website (either by saving it on a disk or by printing it), displaying a work on a computer screen or to upload a work on a website.

ACTIVITY 4.2

Sina approaches you for legal advice. She wishes to scan photographs of John's art works, save them on her computer's memory, and then she wishes to send these images to her friend Yen, who lives in Canada. She wishes to know whether she may do this without John's permission.

Explain to Sina which forms of copyright infringement her actions will entail.

FEEDBACK

Sina's proposed action will entail the following forms of infringement:

- First act of reproduction: by scanning the photographs into a digital file, a copy — the digital file itself — is made.
- Second act of reproduction: the storing of the digital images on her computer memory constitutes a reproduction of the work.
- Third act of reproduction: the uploading of the file from

Sina's computer to her service provider entails the making of a copy.
- Fourth act of reproduction: transferring the file from Sina's service provider to Yen's service provider (from one computer network user to another) entails the making of multiple copies.
- Fifth act of reproduction: the downloading of the photograph from Yen's service provider to her (Yen's) computer memory entails the making of a copy of the work.
- Sixth act of reproduction: a further copy is made when Yen prints the image that she has downloaded.

4.3.1.3 Publication

A literary or musical work is published when copies of the work are issued to the public (sect 1(5)). Thus the work may not be distributed without the permission of the copyright owner. The term ''copy'', in relation to a literary or musical work, is defined as a reproduction of the work or an adaption of it (sect 1(1)).

There are two elements to the term 'publication' —

- copies of the work
- made available to the public

It is controversial whether the term 'copies' include ephemeral reproductions in RAM (Random Access Memory — a computer's temporary memory). Section 2(2) states that a work that subsist of digital data or signals complies with the requirement of material embodiment. We may thus conclude that a digitised literary work will meet the inherent requirements for copyright protection. It also then follows that the making available of reproductions of such a work (in digital format) will constitute ''making available of copies'' of such a work.

But even where the term copies connote more permanent reproductions, then making a work available on a web site may still constitute publication, as public that download that work can make reproduce the work in a permanent format. The work can be stored on a hard disk of a computer, or a printout may be made of the work.

It follows that works that are first made available on the Internet, qualify for copyright protection. Such making available may also constitute the first publication of the work, although it will be difficult to determine in which country it was first published. It is also important to note that presently, many literary works are only published in digital format. The mere fact that a work may be accessed online as opposed to CD ROM

format, should not have any effect on the copyright protection of such works.

4.3.1.4 Other unauthorised actions

As for performing the work in public, the term ''performance'' is defined to include any mode of visual or acoustic presentation of a work (sect 1(1)). A work can be performed by the operation of a loudspeaker, a radio, television or **diffusion receiver**, by the exhibition of a cinematograph film, by the use of a record or by any other means. Also, the delivery of a lecture, speech or sermon will constitute a performance of it. It should be noted that the term ''performance'' does not include the broadcasting or re-broadcasting or transmission of a work in a diffusion service.

There is no definition of the term ''public'' in the Act, but it is submitted that where a work is performed before those persons who normally comprise what may be termed the domestic circle, the performance will not be in public. Conversely, where the audience comprises a cross-section of the public and is not limited to a particular domestic circle, the performance will take place in public (see *Jennings v Stephens* [1936] Ch 469 at 481; *Southern African Music Rights Organisation Ltd v Svenmill Fabrics (Pty) Ltd* 1983 (1) SA 608 (C)).

The term ''**diffusion service**'' is defined as ''a telecommunication service of transmissions consisting of sounds, images, signs or signals, which takes place over wires or other paths provided by material substance and intended for reception by specific members of the public'' (sect 1(1)). Such a service may be offered gratuitously, or as part of the amenities provided by an establishment such as a boarding house or hotel, or to subscribers (see Copeling *Copyright and the Act of 1978* par 25 p 31). The Internet may be seen as a diffusion service (see Buys (ed) *Cyberlaw* at 53) but the performance of a work will only take place where there is a public presentation of the work at the receiving apparatus (the computer screen).

4.3.1.5 Right of communication to the public

The question arose whether transmitting a work in digital form over the Internet constitutes infringement of copyright, and, more specifically, whether it constitutes broadcasting of the work, or publishing the work, or placing it in a diffusion service? None of these restricted rights could easily be applied to the transmission of works on the Internet. A new right of ''communication to the public'' was created which grants copyright owners the right to control the transmission of their copyright works on the Internet.

Article 8 of the WIPO Copyright Treaty (WCT) reads as follows:

Article 8 of the WCT

> Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.

communication to the public

A new right that was extended to authors is that authors have the exclusive right of communication of their works to the public by wire, or by wireless means. The right specifically includes the right to make works available to the public in such a way that the public may access them on demand interactively — that is, from different places at different times as they choose individually.

An ''interactive service'' is one that enables a member of the public to receive a transmission of a program especially created for the recipient, or, on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by, or on behalf of, the recipient. Each individual website needs to be analysed to ascertain if it may be ''interactive'' in this context. For example, can the listener visit the site and select the sound recordings heard during the visit? If so, how much control does the individual listener have over what is heard and when it is heard?

One type of ''interactive service'' enables a member of the public to receive a transmission of a program especially created for the recipient, even though it was created upon the request of a third party.

The Agreed Statement concerning Article 8 of the WCT reads as follows:

> It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11*bis*(2). (The WIPO Copyright Treaty and the Berne Convention may be accessed at: <http://www.wipo.int>).

4.3.2 International case law

In *Playboy Enterprises Inc v Webbworld, Inc D/b/a Neptics.com, Bentley Ives, James Gurkin, and Benjamin Ellis* (Case No. 3-96-CV-3222-DES) (extracts from *http://www.loundy.com/CASES/PEI_v_Webbworld.html*). The court held as follows on 6-8:

> ''Infringement occurs when a defendant violates one of the exclusive rights of the copyright holder. 17 U.S.C. Section 501(a). These rights include the right to reproduce the copyrighted work, the right to prepare derivative works, the right to distribute copies to the public, and the right to publicly display the ... images in issue were stored in defendants' 'web server' computers and available for downloading by subscribers. The images retrieved by Mr. Snyder from the Neptic's website are virtually identical to those images which previously appeared in one of Playboy's copyrighted magazines''.

The court referred to *Religious Technology Centre v Netcom On-Line Communication Services Inc* (907 F Supp 1361 (ND Cal 1995)) (hereafter ''RTC''). RTC sued Netcom, an access provider for direct copyright infringement as it provided Internet access to a private bulletinboard system upon which infringing works were placed (on 1365-68). The court held that Netcom was not liable for copyright infringement, as:

> ''Netcom does not create or control the content of the information available to its subscribers; it merely provides access to the Internet, whose content is controlled by no single entity.'' (on 1372).

The court in *Playboy Enterprises Inc v Webbworld* rejected the defendant's argument, namely that ''Neptics'' is performing the same services as ''Netcom'' (in the *Religious Technology Centre v Netcom* case), namely acting as a mere conduit for information.

The court made the following remarks:

> ''This court finds that defendants' reliance on RTC is misplaced. As plaintiff points out, a Neptics subscriber, unlike a Netcom customer, cannot gain access to the Internet using Neptics. The Neptics subscriber must first get onto the Internet using a separate IAP, such as Netcom. Only after gaining access to the Internet can the subscriber connect with the Neptics website. Where Netcom gets paid for providing Internet access for its customers, Neptics gets paid for selling the images it stores on its computers ... Neptics' function is not to provide Internet access, but

> rather to provide its subscribers with adult images which are contained in the storage devices of its computers. Webbworld also argues that it cannot be held liable for copyright infringement because it has no control over the persons who are posting the infringing images to the adult newsgroups from which Neptics obtains its material. While this may be true, Neptics surely has control over the images it chooses to sell on the Neptics' website. Even the absence of the ability to exercise such control, however, is no defense to liability. If a business cannot be operated within the bounds of the Copyright Act, then perhaps the question of its legitimate existence needs to be addressed'' (on 9-11) see <*http://www.loundy.com/CASES/PEI_v_Webbworld.html*>.

In *Playboy Enterprises, Inc v George FRENA d/b/a Techs Warehouse BBS Systems and Consulting, and Mark Dyess* (839 F Supp 1552 (No 93-489-Civ-J-20)) (refer to *http://www.phillipsnizer.com/Internetlibrary.htm* for the full decision), the defendant, George Frena, operated a bulletinboard system named Techs Warehouse BBS (hereafter ''BBS''). The bulletinboard system distributed unauthorised copies of the photographs. The plaintiff sued the defendant for copyright infringement. The court held as follows:

> ''Public distribution of a copyrighted work is a right reserved to the copyright owner, and usurpation of that right constitutes infringement. See *Cable/Home Communication Corp. v. Network Productions,* Inc., 902 F.2d 829, 843 (11th Cir.1990). PEI's right under 17 U.S.C. Section 106(3) to distribute copies to the public has been implicated by Defendant Frena. Section 106(3) grants the copyright owner ''the exclusive right to sell, give away, rent or lend any material embodiment of his work.' Furthermore, the 'display' rights of PEI have been infringed upon by Defendant Frena. See 17 U.S.C. Section 106(5). The concept of display is broad. See 17 U.S.C. Section 101. It covers 'the projection of an image on a screen or other surface by any method, the transmission of an image by electronic or other means, and the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system.' The display right precludes unauthorized transmission of the display from one place to another, for example, by a computer system. 'Display' covers any showing of a 'copy' of the work, 'either directly or by means of a film, slide, television image or any other device or process.' 17 U.S.C. Section 101. However, in order for there to be copyright infringement, the display must be public. A 'public display' is a display 'at a place open to the public or ... There is irrefutable evidence of direct copyright infringement in this

case. It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement''
(see *http://www.phillipsnizer.com/Internetlibrary.htm*)

ACTIVITY 4.3

Sina approaches you for legal advice. She tells you that one of her friends, John, trades on his own website, called ''Line Art''. The website is hosted by Ben. John made three-dimensional computer-formatted reproductions of some of Sina's sculptures. He has sent these unauthorised copies to Teena, a website owner trading in Chile. The material was sent to Teena, via Ben, to her service provider, Sam. Teena has sold 15 of these copies to on-line customers based in Chile.

Sina wishes to know whether John, Ben, Teena or Sam has committed copyright infringement.

FEEDBACK

Your advice to Sina should take the following into consideration:

- First act of infringement by John: by creating a three-dimensional reproduction of the sculptures — an adaptation of Sina's work is made.
- Second act of infringement by John: the storing of the digital images on his computer memory constitutes a reproduction of the adaptation of the work.
- Third act of infringement by John: the uploading of the file from John's computer to his service provider entails the making of a reproduction of the work and an act of communication of the work to the public (art 8 of the WCT).
- Fourth act of infringement: transferring the file from John's service provider (Ben) to Teena's service provider (from one computer-network user to another) (Sam) entails the making of multiple copies. Does it also constitute communication to the public? No, because the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the particular meaning.
- Fifth act of infringement: the downloading of the photograph from Sam's physical facilities for enabling or making a communication to Teena entails the making of a copy of the work (a reproduction), but not an act of communication to the public.
- Sixth act of infringement: when Teena sells and delivers copies of the work to the 15-online customers, multiple

copies of the work are made. Does it also constitute communication to the public? Yes, the right of communication to the public includes the exclusive right of communication of their works to the public by wire or by wireless means.

4.4 SPECIAL FORMS OF INFRINGEMENT ON THE INTERNET

Prescribed articles: Ebersöhn ''Hyperlinking and Deep-Linking'' (2003) 11 part 2 Juta Business Law 73-77; and Ebersöhn ''Framing and Intellectual Property Law'' (2003) 11 part 1 Juta Business Law 49-52.

4.4.1 Linking

What is ''linking''?

Linking and framing are both methods of using third-party content available on the Internet to enhance a webpage or CD-ROM. ''Linking'' is the practice of creating a link from one webpage to another by including a hypertext ''link''. A hypertext link constitutes highlighted words or symbols that, when pointed to and ''clicked'' upon, instruct the browser to go to a new webaddress. The creation of links is a basic element of the World Wide Web, the multiple transversing links of which create the conceptual ''Web'' that gives the medium its name.

The technical background to linking is provided by Lai appendix 5 (232–233), as follows:

> The World Wide Web (WWW) operates on a text-based language called HTML (Hyper Text Markup Language). The text contained in triangular bracket (''<''and''>'') are the HTML directives that determine (in a manner that is similar to the embedded codes used by word processing programs) how the text is to be formatted, and the points of insertion of graphics into text. The potency of HTML is illustrated by the following statement:
>
> <img src=http://lcweb.loc.gov/copyright/mb100.gif.>
>
> This statement contains a link to another computer system and directs the web-broswer program on the user's computer in the following (or equivalent) terms:
>
> > 'This is a citation to an image source (img src). Use the Hyper Text Transfer Protocol (http) to go to the computer site named ''lcweb'' in the domain loc.gov (the Library of Congress website) and in the subdirectory ''copyright'', retrieve the graphic image file (gif), called ''mb100''.'
>
> As this webpage is being displayed on the computer screen, its constituent components are being retrieved from different computers. There is no limit imposed on the number of remote sites which can be used, nor on the physical locations of those sites.

copyright infringement and links

The mere creation of a link does not, in itself, infringe copyright. The coloured or underlined descriptive words appearing on a webpage that indicate a link are usually too few to constitute a work and the possibly detailed technical address or Uniform Resource Locator (URL) that may reside behind a link is also unlikely to be a ''work''. Nevertheless, if a web surfer clicks on the link, his or her browser will download a full copy of the material at the linked address, creating a copy in the RAM of the surfer's computer, courtesy of the address supplied by the party that published the link.

implied licence

It is widely agreed that the permission to download material over the link must be part of an implied licence granted by the person who made the material available on the web in the first place. (See, eg, Hughes 55). What else could have been intended? The content has been put in a form specifically so that it can be downloaded by anyone on the Internet who uses a browser to request a copy of the material at the relevant address.

limits to scope of implied licence

However, the scope of the implied licence is the subject of debate. It is generally agreed that the principles of common law pertaining to the terms that a court will imply into a contract dictate that the terms of the implied licence are limited in nature. In particular, there is no reason to imply that by putting copyright material on the Internet the copyright owner is by implication permitting surfers to re-use the material for commercial purposes.

''deep'' hyper-linking

In particular, the practice of ''deep'' hyperlinking, that is, providing links that bypass the provider's homepage (which may contain advertising and other commercial information), may not be within permissible use as per the implied licence, particularly, if the deep hyperlink is presented on a commercial site. Note, however, that the ''deep link'' does not actually reproduce the copyright owner's material. Deep linking is more an issue of contract and/or trade-practices law than of copyright.

4.4.2 Framing

What is framing?

''Framing'' is the practice of creating a frame or window within a webpage in which the content of a different webpage can be displayed. Usually, when a surfer clicks on a link the new webpage is presented as its owner intended it to be, but many pages also present the content of third-party webpages listed as links, ''framed'' with reminders of the originating page. Frames are most often used to easily help define, and navigate within, a single content provider's webpages. However, if frames are used to present third party material from commercial sites, this immediately gives rise to issues of passing off and misleading or deceptive conduct, as well as copyright infringement.

Lai (234) sketches the technical background to framing as follows:

> The remote user's web-browser display is subdivided into a set of rectangular windows or frames — each of which can be manipulated independently; or the text can be scrolled up or down. Framing is accomplished by using the provisions of the HTML language — the first step is to define a ''frame set'', which divides the screen into different sections (eg see the CNN interactive homepage <http://www/cnn.com). Typically a ''site index'' appears on the left of the page and remains there, regardless of which page is being displayed.

4.4.3 Case law

Unfortunately, the two famous cases on linking were settled before judgement. In *Shetland Times v Wills and Zeine Ltd and Ticketmaster v Microsoft,* commercial sites presented valuable content of a competing site, using ''deep'' hyperlinks. The *Total News* case also dealt with framing.

Ticketmaster

In *Ticketmaster*, the complaint is that a Microsoft site called ''Seattle Sidewalk'' provided links directly into Ticketmaster's on-line ticket-sales page, bypassing ticket-sales information and advertisements.

In *Ticketmaster v. Tickets.com* (U.S. District Court, Central District of California August 10, 2000) the application by Ticketmaster Corporation and Ticketmaster Online-Search, Inc. (hereinafter collectively referred to as ''Ticketmaster'' or ''TM'') for a temporary interdict against Tikets.Com Inc (hereinafter ''T.Com''), was refused.

The following quotes from the unreported decision is important (refer to http://www.gigalaw.com/library/ticketmaster-tickets-2000-08-10-p1.html) for the full decision.

> As to copyright, there is undeniably copying of the electronic bits which make up the TM event pages when projected on the screen. Except for the URL, the copying is transitory and temporary and is not used directly in competition with TM, but it is copying and it would violate the Copyright Act if not justified.
>
> The copying, as summarized above, takes place as a part of the process of taking the (unprotectable) facts from TM's websites so as to turn those facts into facts published by T.Com in its own format. At oral argument, counsel explained that by the nature of the way computers work, it is necessary to copy the electronic signals temporarily on the copying computer's RAM in order to extract the factual data present thereon … TM makes the point that copying

> the URL (the electronic address to the web pages) which is not destroyed, but retained and used, is copying protected material. The court doubts that the material is protectable because the URL appears to contain functional and factual elements only and not original material. It appears likely to the court that plaintiff's odds on prevailing on the fair use doctrine at trial are sufficiently low that a preliminary injunction should not be granted even with the presumption of irreparable injury which goes with copyright infringement''
> (see http://www.gigalaw.com/library/ticketmaster-tickets-2000-08-10-p1.html).

Shetland Times

It is interesting to note that in the *Shetland Island* case, which was settled in November 1997, the terms of settlement permitted deep hyperlinking of the *Shetland Times* report, by the defendant subject to the following conditions:

conditions for hyperlinking

- a ''*Shetland Times* story'' underneath every headline hyperlink, there must be the words
- adjacent to the headline, there must be a button shadowing the *Shetland Times* masthead and logo
- the words ''*Shetland Times* story'' and the button must go to the homepage

A Danish court has early in July 2002 ruled in *Danish Newspaper Organization v Newsbooster* (http://www.newsbooster.com) (the full name and reference of the case is not available yet) that so-called 'deep linking' is a breach of copyright. The case was brought by the Danish Newspaper Organisation (DNO) against the Newsbooster service, which linked to articles on 28 of the plaintiffs news websites without going through their home pages. The court held that the newspaper articles were copyrightable works.

The court held as follows:

> ''The text collections of headlines and articles, which make up some Internet media, are thus found to constitute databases enjoying copyright protection pursuant to section 71 of the Danish Copyright Act. Under section 71(1) of the Act, the makers of the databases, i.e. the Principals, have the exclusive right protected by the said provision.''

On liability for linking the court held as follows:

> ''By means of its search engine, Newsbooster offers its users regular updating of the search results turning up on the background of the users' predefined search criteria. As a result, the news outlines providing users with relevant headlines with deep links to articles on Newsbooster's website or in Newsbooster's electronic newsletters need to

> be supplemented and updated on a regular basis. Consequently, Newsbooster's search engine — and therefore not the users — needs to crawl the websites of the Internet media frequently for the purpose of registering headlines and establishing deep links in accordance with the search criteria defined by the users.
>
> As a result, Newsbooster repeatedly and systematically reproduces and publishes the Principals' headlines and articles. Newsbooster has a commercial interest in this business. In view of the fact that the basis of Newsbooster's commercial deep-linking activities is that the Internet media produce linkable material; that the material used by Newsbooster constitutes the business base of the media to which Newsbooster is linking; that Newsbooster's news communication service with deep links to the Principals' newspapers is in competition with the said newspapers; and that Newsbooster, in addition to competing with the Principals, may impair the advertising value of the Principals' websites and thus reduce the advertising revenues from banner ads, etc., the Court finds that by reproducing and publishing the Principals' headlines and articles, Newsbooster does unreasonably prejudice the Principals' interests.
>
> The search service offered by Newsbooster, including the electronic distribution of newsletters, with deep links from the websites Newsbooster.com and Newsbooster.dk and from the newsletters to articles displayed in the Principals' Internet media and
>
> Newsbooster's reproduction and publication of headlines from the Principals' media on Newsbooster's websites and in Newsbooster's electronic newsletters, thus conflicts with section 71(2) of the Danish Copyright Act.''

The court ruled that Newsbooster is prohibited from offering a search service with deep links from the websites newsbooster.dk and newsbooster.com directly to the plaintiffs' news articles; reproducing and publishing headlines from the Internet versions of newspaper articles; distributing electronic newsletters with deep links directly to the newspaper articles; and reproducing and distributing headlines from the newspapers. (The quotations from the court's ruling was obtained from ''Translation of pages 29–42 of the ruling made by the Bailiff's Court on 5 July 2002 at *http://www.newsbooster.com/?pg=judge&lan=eng*.)

***Total News* case**

Framing can have an effect similar to that of ''deep'' hyperlinking. In *Washington Post to v Total News*, Total News and its associated companies offered a news service that provided links to other major web-based news services, but which, when

''clicked'' by a surfer, did not load the whole page, but presented the original news service within a Total News frame. Total News was sued by The Washington Post, Cable News Network Inc and Reuters News Media Inc. The news networks pointed out that by adding its own advertising in the frame and reducing the size of their webpages as presented to the surfer, Total News was cluttering and reducing in size their advertising, damaging delivery of the advertising that each had promised to its advertisers.

The *Total News* case was settled in June 1997. The terms of settlement permitted linking in highlighted plain text but not in any manner that might apply an affiliation between the plaintiffs and the defendant, might cause confusion, or might ''dilute'' (there is a law of trade-mark dilution in the US) the plaintiff's trademarks.

ACTIVITY 4.4

Vuzi has asked Thieu to create links from Netlink to the websites of two major motor-vehicle manufacturers, namely Wolwa and Dienwoo. He creates the links directly to Wolwa and Dienwoo's motor-vehicle repair manuals. He has also created links to his website from various on-line auction sites.

Vuzi approaches you for legal advice. He wishes to know whether he may create links from his website to Wolwa's and Dienwoo's websites. He would also like to display some pages of Wolwa's and Dienwoo's repair manuals on his website.

FEEDBACK

It is important to note that if, as seems to be the case, the right to link to copy material put on the Internet is governed by an implied licence, the copyright owner may specify the terms on which linking is permissible. There is no apparent reason why a copyright owner may not include linking conditions on his or her homepage as purported contractual terms applying to the use of his or her material and, if suitably notified to users, thereby dictate precisely the terms on which linking may take place. It will be interesting to see whether any such terms are enforceable as contracts, or fail for lack of consideration of the Web surfer. Elaborate conditions of this kind may be unenforceable for being in restraint of trade.

Vuzi may create links to the websites as described. However, Vuzi must be advised against deep ''hyperlinking'' or fram-

ing, as it may cause liability for dilution, passing off or copyright infringement.

ACTIVITY 4.5

What are the similarities and differences between linking and framing?

FEEDBACK

Note that framing may involve linking, but that linking does not involve framing. Also explain how ''deep linking'' and framing may constitute deceptive trade practices, and how these two practices can have a similar effect.

4.4.4 Caching

''Caching'' is also a form of copyright infringement on the Internet. Lai (235–236) explains the process as follows:

> Caching refers to the storing of copies of material from an original source site (eg a webpage) for later use when the same material is requested again, thereby obviating the need to go back to the original source for the material. To establish the necessary implications for the reproduction right and exceptions thereto, ''caching'' has to be studied to (i) determine its purpose; (ii) ascertain its various forms; (iii) ascertain its attributes, particularly in relation to transience; and (iv) ascertain its ''integral'' nature or otherwise.

(iii) Types of caching

It is impossible to predict how many such caches exist in a particular connection. There are generally four types of caching.

- **Mirror Caching.** Also known as ''caching servers''. These occur when a frequently accessed website is downloaded to another server in anticipation that the information will be required sometime in the future. It relieves net traffic, since a user will avoid the need to read the page from the original source.
- **Web Caching.** Many Internet Service Providers operate ''web caches'', of which there are two kinds; ''pull-caches'' and ''push-caches''. The content of pull-caches is determined by which pages are requested by the users — they respond to actual demand for webpages from remote sites, and store the most frequently

accessed webpages. Push-caches work by receiving pages from remote sites in anticipation of demand. In this way time-consuming reloads are avoided.

- **Proxy Caching.** This occurs when a Local Area Network (LAN) or corporate in-house network stores frequently used material. Alternatively, ISPs also may store on their servers for a certain period of time webpages that have been previously requested by their users. On request, such pages would be downloaded from server rather than original source.
- **User Caching.** A user's web-browser, eg Netscape or Internet Explorer, caches the webpages accessed during a particular browsing session (''Back'' and ''Forward'' functions). Netscape, for example, has a cache file which stores all the webpages browsed by the user over time. If the user does not clean out his cache, the material (copyright infringing or otherwise, and perceptible) remains as a file in a subdirectory in the user's hard disk.

4.5 FAIR USE ON THE INTERNET

> The Copyright Act No. 98 of 1978, recognises the notion of ''fair use'', which provides that copyright shall not be infringed by any fair dealing with certain works, such as copying for purposes of research or private study or personal or private use, etc. The Berne Convention noted that the ''fair use'' provisions in the context of digitised use should be approached just as they are in ''traditional'' environments. Commercial use, which harms actual or potential markets, will, therefore, probably constitute infringement, whereas non-profit educational transformative use will most probably often be deemed fair. (Green Paper 60)

In terms of Article 10 of the WIPO Copyright Treaty, signatories may carry forward and appropriately extend limitations and exceptions to the digital environment. The Agreed Statement concerning Article 10 of the Treaty emphasises the need to maintain a balanced copyright regime:

> It is understood that the provisions of Article 10 permit Contracting Parties to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention. Similarly, these provisions should be understood to permit contracting parties to devise new exceptions and limitations that are appropriate in the digital network environment.

It has been noted that the fair-use provisions in the context of

approach in digital environment

digitised use should be approached just as they are in ''traditional'' environments. Thus, commercial use which harms actual or potential markets will probably always be infringing, whereas nonprofit educational transformative uses will probably often be deemed to be fair. Between these extremes, the courts will have to determine what typifies fair use.

Dworkin (paper delivered at the Conference on International Intellectual Property Law and Policy 11) notes that, according to a WIPO Committee of Experts, in considering the implications of reprographic reproduction and the exceptions of article 9(2), the following must be taken into account:

factors for determining fair use

(a) the nature of the work copied — in certain instances such as data bases and sheet music, the free reprographic reproduction would necessarily conflict with the normal exploitation of the work
(b) the extent of the copying — (eg is it an entire book or only one article from a periodical which is being copied?)
(c) the number of copies made
(d) the nature of the entity which makes or allows the making of the copies (eg whether it is a non-profit-making library, archives or school or a company where copies are made in connection with commercial activities) and
(e) the purpose of the copying (ie whether it is for private use or commercial activity).

4.6 LIABILITY FOR INFRINGEMENT

Prescribed article: Visser ''A new Online Service Provider Liability Regime'' (2003) 11 part 1 Juta Business Law 40-44.

4.6.1 Contributory infringement

In countries such as the United States of America, liability for copyright infringement has been extended by the notion of ''contributory infringement''. In *Sony Corp v Universal Studios Inc*, the US Supreme Court stated the following:

> [T]he absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringement on certain parties who have not themselves engaged in the infringing activity. For ... the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another.

MP3 file-sharing technology and copyright infringement was the subject matter of the well-known case *A&M Records Inc v Napster Inc* 239 F3d 1004 (2001). ''MP3'' is an abbreviation for

''MP(EG) layer 3'', namely a audio and data compressor capable of compressing digital audio files to one twelfth of their original size.

The MP3 technology is fully explained in *A&M Records Inc v Napster Inc:*

> ''Napster facilitates the transmission of MP3 files between and among its users. Through a process commonly called 'peer-to-peer' file sharing, Napster allows its users to: (1) make MP3 music files stored on individual computer hard drives available for copying by other Napster users; (2) search for MP3 music files stored on other users' computers; and (3) transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet. These functions are made possible by Napster's MusicShare software, available free of charge from Napster's Internet site, and Napster's network servers and server-side software. Napster provides technical support for the indexing and searching of MP3 files, as well as for its other functions, including a 'chat room,' where users can meet to discuss music, and a directory where participating artists can provide information about their music (on 1011)
>
> ... Plaintiffs claim Napster users are engaged in the wholesale reproduction and distribution of copyrighted works, all constituting direct infringement. The district court agreed. We note that the district court's conclusion that plaintiffs have presented a prima facie case of direct infringement by Napster users is not presently appealed by Napster. We only need briefly address the threshold requirements (on 1013)

The court concluded that Napster's activities amount to copyright infringement. The court held that the uploading of the music works constitute an infringement of the plaintiff's right to distribute her works and that the downloading of the music works constituted the unauthorised reproduction of her work (at 1014). These infringing actions were committed by users of the Napster service. The question then arose whether Napster could be held liable at all for infringement. In referring to contributory infringement the court held as follows:

> ''Traditionally, 'one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer.' (on 1019).

The court then discussed the elements of knowledge and material contribution as follows:

''A. Knowledge

Contributory liability requires that the secondary infringer ''know or have reason to know'' of direct infringement ... The district court found that Napster had both actual and constructive knowledge that its users exchanged copyrighted music.

It is apparent from the record that Napster has knowledge, both actual and constructive, of direct infringement. Napster claims that it is nevertheless protected from contributory liability by the teaching of *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). We disagree. We observe that Napster's actual, specific knowledge of direct infringement renders *Sony's* holding of limited assistance to Napster. We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system. The *Sony* Court refused to hold the manufacturer and retailers of video tape recorders liable for contributory infringement despite evidence that such machines could be and were used to infringe plaintiffs' copyrighted television shows. *Sony* stated that if liability 'is to be imposed on petitioners in this case, it must rest on the fact that *they have sold equipment with constructive knowledge of the fact that their customers may use that equipment to make unauthorized copies* of copyrighted material.' Id. at 439, 104 S.Ct. 774 (emphasis added) ... The *Sony* Court declined to impute the requisite level of knowledge where the defendants made and sold equipment capable of both infringing and 'substantial non-infringing uses.' Id. at 442 (on 1020) ...

...

We are bound to follow *Sony*, and will not impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights. *See* 464 U.S. 104 S. Ct. 774 at 436 (rejecting argument that merely supplying the 'means' to accomplish an infringing activity' leads to imposition of liability) (on 1020-1021).

Regardless of the number of Napster's infringing versus non-infringing uses, the evidentiary record here supported the district court's finding that plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users' infringement of plaintiffs' copyrights (on 1021).

...

We agree that if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement. *See*

> *Netcom*, 907 F. Supp. at 1374. Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material, (see *Sony* 464 U.S. at 436, 442-43). To enjoin simply because a computer network allows for infringing use would, in our opinion, violate *Sony* and potentially restrict activity unrelated to infringing use (on 1021).
>
> We nevertheless conclude that sufficient knowledge exists to impose contributory liability when linked to demonstrated infringing use of the Napster system (on 1021).
>
> ...
>
> B. Material Contribution
>
> Under the facts as found by the district court, Napster materially contributes to the infringing activity. The district court correctly applied the reasoning in *Fonovisa*, and properly found that Napster materially contributes to direct infringement. We affirm the district court's conclusion that plaintiffs have demonstrated a likelihood of success on the merits of the contributory copyright infringement claim. We will address the scope of the injunction in part VIII of this opinion (on 1022).

As a result of this decision Napster ceased its free service. Copyright owners are now paid royalties for the distribution of their music works.

Although the principle of ''contributory infringement'' has not been established in any reported decision on South African copyright law, there are indications that our courts may be prepared to accept such principle (see *Atari Inc v JB Radio Parts (Pty) Ltd;* see the discussion by Dean, par 8.25, 1–50; *Bosal Africa (Pty) Ltd v Grapnel (Pty) Ltd* 893 (claim dismissed for lack of proof of knowledge of infringement)).

delict

Were one to assume that copyright infringement is merely a form of delictual liability, the liability of someone who assists, aids, or abets the commission of copyright infringement can be based on the broad principles of the Aquilian action. In *McKenzie v Van der Merwe* (51), the following was stated:

> [U]nder the lex Aquilia not only the persons who actually took part in the commission of a delict were held liable for the damage caused, but also those who assisted them in any way.

(This principle has been applied in a trade-mark context, namely in *Omega, Louis Brandt et Frere SA v African Textile Distributors* 954 and 957).

The remedies available, then, to a successful plaintiff in an action for ''contributory infringement'' are damages and injunctive relief (an interdict). These remedies are also available to a successful plaintiff in an action for direct infringement of copyright (see s 24(1) of the Copyright Act).

fault

Fault (knowledge in some form or other) is required in respect of an award of damages only at common law, (see *Hawker v Life Offices Association of South Africa; R & I Laboratories (Pty) Ltd v Beauty Without Cruelty International (South African Branch)* 754–755; *Long John International Ltd v Stellenbosch Wine Trust (Pty) Ltd* 143; for statutory copyright infringement, see s 24(2)). In passing, note that this principle is in line with article 45(1) of the TRIPS Agreement, which requires that

> [J]udicial authorities shall have the authority to order the infringer to pay the right holder damages adequate to compensate for the injury the right holder has suffered because of an infringement of that person's intellectual property right by an infringer who knowingly, or with reasonable grounds to know, engaged in infringing activity.

4.6.2 Service-provider liability

4.6.2.1 Introduction

When the liability of a particular on-line service provider (OSP) is to be determined, one should remember that the law of delict and copyright law impose liability for acts or omissions in a specific instance. So, an OSP's liability will depend on the role it plays in a particular transaction. If, on the one hand, an OSP makes unauthorised reproductions of a protected work (eg, for technical reasons, such as caching), it may be liable for direct infringement of copyright. But if, on the other hand, it merely transmits or facilitates access to copyright-infringing material, it may be liable for ''contributory infringement'' at common law.

Role of the OSP

The technical role played by OSPs (also referred to as Internet service providers (ISPs)), in the digital environment establishes potential liability of OSPs: the question is, in which instances is such potential infringement principal in nature, and in which instances is it accessory in nature? Here we shall consider the liability of OSPs for copyright infringement only. (Liability may, of course, also be imposed on them by the law regarding trade secrets, unfair competition, product liability, defamation, and the like).

Currently, this is one of the most controversial issues in copyright law. Koelman & Hugenholtz (paper delivered at a workshop) say the following:

> Should providers be treated as electronic publishers, and thus made directly liable for all the infringing gigabytes flowing through their servers? Or are they mere the postmen of the Internet, common carriers exempt from all liability? As always in the realm of law, the answer lies somewhere in the middle.

Article 8 of the WCT:

Article 8 of WCT

> Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.

The Agreed Statement concerning Article 8 of the WCT reads as follows:

> It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11*bis*(2).

(see *Playboy Enterprises Inc v Frena; Sega Enterprises Limited v MAPHIA; Religious Technology Centre v Netcom On-Line Communication Services, Inc and of Church of Religious Technology v Dataweb BV;* **study** the discussion of these, and other cases, in *Cyberlaw* 62–66).

There are two models for limiting the liability of OSPs for copyright infringement in this context. At the outset, note the following striking difference between the two models: whereas the European model has opted for an all-embracing horizontal approach, the American model deals with copyright liability strictly within the framework of copyright law.

4.6.2.2 American model

a Introduction

The United States Congress passed the Digital Millennium Copyright Act ('DMCA') which was signed into law on 28 October 1998. The DMCA incorporates the Online Copyright Infringement Liability Limitation Act as Title II. The Act adds a new section 512 to chapter 5 of the United States Copyright Act,

which deals with the enforcement of copyright. This statute limits the availability of remedies which an author may seek for copyright infringement against an OSP. The limitation of liability depends upon the OSP's meeting certain threshold requirements and performing certain functions or acts.

effect of the DMCA

To begin with, here are three general observations about the effect of the statute:

(1) Although the DMCA limits the liability of OSPs in certain circumstances, it does not impose new liabilities on them, or curtail or affect any existing defences available to an OSP against a claim for copyright infringement.
(2) The DMCA does not limit the rights of authors to hold an OSP's users, subscribers, or account holders liable for their acts of copyright infringement.
(3) The statute does not exempt OSPs for acts of copyright infringement that fall outside the ambit of the statute, or prevent authors from holding OSPs liable to compensate for damage caused by such acts (see Oktay & Wrenn — paper delivered at a workshop 1).

definition of a service provider

What is a service provider? To qualify as a ''service provider'', an entity should offer the transmission, routing, or provision of connections ''for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material sent or received''; provide ''online services or network access'', or operate facilities for such services or access. The definition encompasses the basic functions and services needed by users to access the Internet and enjoy its benefits. At the same time, it does not encompass all people using the Internet — only those who perform the functions that make the Internet available to users.

To avail itself of the liability limitations, a service provider must meet the following three threshold requirements:

three threshold requirements

- It must have adopted and ''reasonably implemented'' a policy providing that it will terminate, in appropriate circumstances, the accounts or subscriptions of repeat infringers;.
- It must inform its subscribers and account holders of its policy.
- It must accommodate, and not interfere with, ''standard technical measures''.

The availability of remedies for copyright infringement against a service provider is limited if the service provider satisfies the three threshold requirements mentioned above and performs certain stated functions or acts, namely:

- transmitting, routing, and providing connections to infringing material (the ''mere conduit'' limitation)
- system caching storing infringing material at the direction of a user (the ''hosting'' limitation), or
- linking or referring users to infringing material (the ''linking'' limitation)

notice & take-down

In exchange for the four limitations mentioned above, service providers agreed to a procedure in the DMCA commonly known as ''notice and takedown''.

universities' limitation

In addition to the four limitations created for all service providers, Nonprofit Education Institutions (NEIs) may benefit from special rules that may immunise **universities** for the infringing acts of academic staff or graduate students which otherwise may be imputed to an NEI as employer, and prevent it from relying on these four limitations.

Section 512(e) provides that the acts or knowledge of a member of the academic staff or a graduate student will not be imputed to the ''public or other non-profit institution of higher education'' (''NEI'') that employs him or her if

- the academic or graduate student is ''an employee of such institution ... performing a teaching or research function''
- the academic's or graduate student's infringement does not involve the provision of on-line access to instructional materials that are or were required or recommended by that academic or *graduate* student within the proceding three-year period for a course taught at such NEI
- the NEI has not received more than two notifications which claim copyright infringement by such academic or graduate student within the three-year period
- the NEI provides all users of its system or network with informational materials that accurately describe and promote compliance with American copyright law

deny access

The DMCA authorises limited injunctive relief against service providers who comply with the Act's requirements to deny access to infringers and block infringing content. Section 512(j) provides that a court may grant only three specific forms of equitable relief against a service provider (other than a service provider that is also an NEI) which qualifies for the system-caching, hosting, or linking limitations, namely:

- an order restraining the service provider ''from providing access to infringing material or activity residing at a particular site on the provider's system or network'';
- an order requiring a particular infringer's account or subscription to be terminated by the service provider in order to deny it access to the system or network

remedies

- such other injunctive relief as the court may consider necessary to prevent or restrain infringement of specific material at a particular on-line location, ''if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose''.

no access

In the case of a service provider (that is not also an NEI) entitled to the ''mere-conduit'' limitation, a court may enjoin such service provider from providing access to a subscriber or account holder who is using the service provider's services to engage in infringing activity only by terminating its account or restraining it from providing access to infringing material at a particular online location outside the United States.

Injunctive relief may be granted only if a service provider is given notice and the opportunity to appear, except in the case of orders ''ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network''.

4.6.2.3 European model

a EU Directive on Copyright in the Information Society

The European Commission has addressed the reproduction right in the Proposal for a European Parliament and Council Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society.

Article 2 states the following:

> Members States shall provide for the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part.

transient & accidental copying

This provision covers the transient copying which occurs during transmission of a work over the Internet. The proposed article 5(1) states that the following reproductions will be exempted: temporary acts of reproduction, such as **transient and incidental** acts of reproduction which are an **integral and essential part** of a technological process, including those which facilitate effective functioning of transmission systems, whose sole purpose is to enable the use to be made of a work or other subject matter, and which have no independent economic significance.

prohibited hosting

While system caching does seem to fall within the ambit of article 5(1) (see recital 23), OSPs which store protected works more or less **permanently** on their servers (such as hosting service providers) may still incur liability for direct copyright infringement.

b Directive on Electronic Commerce

Of more importance in the present context is the fact that, in November 1998, the European Commission published its Directive on Electronic Commerce.

The Directive applies to ''information society services'' (as defined in the Directive [98/34 EC] dealing with technical standards and rules on the information-society services), which are defined as follows:

> ... normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of services.

The liability rules are modelled upon the 1997 *Informations- und Kommunikationsdienste-Gesetz* (Multimedia Act) in Germany. Unlike the DMCA, the proposed directive applies to both civil and criminal liability for copyright infringement.

Like the DCMA, the proposed E-commerce Directive limits the liability of OSPs acting as the following:

limitations

- mere conduits (see art 12)
- engaging in system (proxy) caching (see art 13)
- acting as hosts (see art 14)

Note the following two observations:

knowledge of removal

- In respect of the system-caching limitation under the Directive: it is not the knowledge of the unlawful nature of the cached material as such, but rather the knowledge of removal at the initial source, or the fact that a competent authority has ordered such removal, that may prompt an OSP to block access to the cached copy.

uniform hosting limitations

- Although the Directive intends to limit civil and criminal liability in horizontal fashion, the exemption from liability is entirely uniform with regard to hosting service providers.

Article 14(1)(a) sets a double standard — the absence of ''actual knowledge'' and ''awareness''. The latter threshold applies only ''as regards claims for damages''. So, a hosting OSP will incur criminal liability only if he or she has actual knowledge that the activity is illegal.

The Directive does not deal with information location tools or educational institutions providing on-line services. The proposal also does not contain any specific ''notice and takedown'' procedures. Article 21 provides that the need for proposals concerning the liability of OSPs for hyperlinks and location-tool services, as well as ''takedown notices'' and attribution of

liability following the taking down of content will be analysed by the Commission before 17 July 2003.

4.6.2.4 ECT ACT: Service Provider Liability

Chapter XI deals with the limitation of liability of service providers or so-called intermediaries and creates a safe harbour for service providers who are currently exposed to a wide variety of potential liability by virtue only of fulfilling their basic technical functions. The service providers may seek to limit their liability where they have acted as mere conduits for the transmission of data messages. The Act provides for specific requirements that the service provider's actions must meet before the clause may be invoked to limit his or her liability.

a Definition

Section 70 provides that a ''service provider'' means any person providing information system services. Section 71 makes provision for the recognition of representative body by the Minister. The Minister must be satisfied that

- its members are subject to a code of conduct;
- membership is subject to adequate criteria;
- the code of conduct requires continued adherence to adequate standards of
- conduct; and

the representative body is capable of monitoring and enforcing its code of conduct adequately.

Section 72 then provides that the limitations on liability established by the ECT Act is available to a service provider only if —

- the service provider is a member of the representative body referred to in
- section 71; and
- the service provider has adopted and implemented the official code of conduct of that representative body.

A limitation of liability is provided for mere conduits, caching, hosting, and information location tools. The approach adopted in the ECT Act is a hybrid of both the European approach in the E-commerce Directive and the approach adopted in the DMCA of the US.

b Mere conduit

Section 73(1) provides that a service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider —

- does not initiate the transmission;
- does not select the addressee;
- performs the functions in an automatic, technical manner without selection of
- the data; and
- does not modify the data contained in the transmission.

Section 73(2) provides that the acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place —

- for the sole purpose of carrying out the transmission in the information system;
- in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and
- for a period no longer than is reasonably necessary for the transmission.

c Caching

Section 74 provides that a service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider —

- does not modify the data;
- complies with conditions on access to the data;
- complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;
- does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the data; and
- removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 77.

d Hosting

Section 75(1) provides that a service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from

data stored at the request of the recipient of the service, as long as the service provider does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.

The limitations on liability established by section 75 do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its websites in locations accessible to the public, the name, address, phone number and e-mail address of the agent and does not apply when the recipient of the service is acting under the authority or the control of the service provider.

e Information location tools

Section 76 provides that a service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person

- is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
- does not receive a financial benefit directly attributable to the infringing activity; and
- removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

f Take-down notification

Section 77 provides that a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include

- the full names and address of the complainant;
- the written or electronic signature of the complainant;
- identification of the right that has allegedly been infringed;
- identification of the material or activity that is claimed to be the subject of unlawful activity;
- the remedial action required to be taken by the service provider in respect of the complaint;

- telephonic and electronic contact details, if any, of the complainant;
- a statement that the complainant is acting in good faith;
- a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct.

Section 77(2) provides that any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down. A service provider is not liable for wrongful take-down in response to a notification (section 77(3)).

Section 78 makes it clear that the ECT Act does not place an obligation on service providers to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

4.6.2.5 Conclusions

The basic principles which can be distilled from the above two models are, broadly, the following:

- access providers (''mere conduits'') are exempt from liability
- in the absence of knowledge or ''awareness'', hosting OSPs are not liable for damages
- once hosting OSPs acquire the necessary knowledge or ''awareness'', they are not liable for damages if they immediately disable access to the infringing content
- injunctive relief against OSPs is available.

4.7 ELECTRONIC-RIGHTS MANAGEMENT

Article 12 of the WCT makes the following specific reference to electronic-rights management:

> (1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:
>
> (i) to remove or alter any electronic rights management information without authority;
>
> (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, ''rights management information'' means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

definition of ''electronic-rights management''

The agreed Statement concerning Article 12 of the WCT reads as follows:

> It is understood that the reference to ''infringement of any right covered by this Treaty or the Berne Convention'' includes both exclusive rights and rights of remuneration.
>
> It is further understood that Contracting Parties will not rely on this Article to devise or implement rights management systems that would have the effect of imposing formalities which are not permitted under the Berne Convention or this Treaty, prohibiting the free movement of goods or impeding the enjoyment of rights under this Treaty.

4.8 DEVICES TO CIRCUMVENT COPYRIGHT-PROTECTION SYSTEMS

4.8.1 Introduction

Over the last few years, software developers have been testing prototype copy-protection systems for computer software and digital works. Equally substantial efforts have also gone into the circumvention of these protection systems, to the ultimate detriment of the copyright owner. As a result, various legislative measures have been put forward to prohibit acts and devices that circumvent these technological protection systems, the latest offerings of which are to be found in the Proposed Directive, the US Digital Millennium Copyright Act of 1998 and the WCT.

4.8.2 The WCT

The WCT makes provision for the violation of technological protection measures of copyright works. Article 11 provides the following:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in

respect of their works, which are not authorized by the authors concerned or permitted by law.

4.8.3 The position obtaining in the US

Chapter 12 of the DMCA provides as follows:

> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.
>
> (3) As used in this subsection —
>
> (A) to ''circumvent a technological measure'' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and
>
> (B) a technological measure ''effectively controls access to a work'' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

Study the prescribed extract from Pistorius ''Copyright Law and IT'' in *Information and Communications Technology Law* (ed. Dana van der Merwe) (2009) at 269-274 on anti-circumvention and the enforcement of rights management in developing countries.

4.8.4 Concluding remarks

The use of technological protection measures to safeguard copyright works in digital format is necessary in light of the ease with which these works may be exploited. The various legislative measures that have been put forward to prohibit acts and devices that circumvent these technological protection

systems are indicative of the growing importance of this subject matter.

4.9 DIGITAL LICENSING OF INFORMATION PRODUCTS

4.9.1 Licensing of computer programs: shrink-wrap agreements

role played by the law of contracts

At first, in the computer software industry, software either was provided to customers as an inducement to buy hardware, or was individually licenced to customers who often had especially commissioned it (see Samuelson 284–285). Contract law may in certain instances bolster or complement the copyright protection of works, but it should be noted that contract law applies only between parties bound by the contract: a contract cannot bind third parties. Also, contract law has not been harmonised, although international legal rules for e-commerce, including aspects of contracting on the Internet, are being negotiated (see, eg, EU Directive on Electronic Commerce). When a mass-market in software began to emerge in the 1980's, a number of software developers began commercially distributing their mass-market software in packages containing ''shrink-wrap licences''.

regulation of use

Shrink-wrap licence agreements were introduced in order to protect the copyright enjoyed by computer-program developers. These agreements regulate the use of computer programs on a uniform basis on an international scale, and are designed to deter the pirating of software.

This practice gained wide application in the software industry, despite substantial doubts about the enforceability of these licences — both as a matter of contract law and as a matter of intellectual-property policy (see Samuelson paper delivered at the Conference on International Intellectual Property Law and Policy).

4.9.2 What is a ''shrink-wrap agreement''?

What is a ''shrink-wrap agreement''?

A shrink-wrap agreement is simply a printed standard-form agreement put or printed on top of the package containing the computer program to be marketed. It is encased in a cellophane wrapper — hence the term ''shrink-wrapped''. These agreements have also been called **''box-top''**, **''tear-me-open''** or **''blister-pack''** agreements (see *Smith Computer Law & Practice* 129). Shrink-wrap agreements are used for mass-marketed software (Stern *Rutgers Computer & Technology LJ* 51). Such agreements come into effect when consumers break open the plastic shrink-wrap or install the software on their computers, thereby assenting to the terms of the licence.

It is interesting to note that none of the acts — now permitted to be performed by the user would in any event have constituted copyright infringement had there been no express authorisation by the copyright owner. The following question now arises: Why a shrink-wrap agreement, if the citation of general copyright restrictions would have a similar effect. Such citation would not be sufficient, for the following reasons:

(1) This approach would be impractical, since the copyright laws of the different countries of distribution differ, which would necessitate the drafting of several different copyright notices.
(2) Some countries provide inadequate, or even no copyright protection to computer programs.

three reasons

(3) Software proprietors are trying to avoid applying the ''first-sale doctrine''. It will no longer be difficult to define the true nature of the agreement if the sale transaction and the licence agreement are regarded as two separate transactions. Only in cases of the retailer acting as the software developer's agent or in cases of mail-order sales it may be difficult to distinguish between the two.

4.9.3 Nature of the shrink-wrap agreement

nature of shrink-wrap

The shrink-wrap agreement purports to create a licence agreement between the purchaser of the computer program and the computer program-producer. As such, it is distinct from the contract of sale between the purchaser and the retailer.

A shrink-wrap agreement grants the user a non-exclusive licence to use the program and accompanying documentation, subject to certain restrictions. Also, the software agreement sometimes explicitly states *that the* licence does not constitute a sale. Title to and copyright in the program, accompanying documentation and any copy made by the user remain with the software-development or publishing corporation.

Typically, the relationship entered into for the acquisition of software is either a licence, or a single payment for use in perpetuity: in both cases, ownership of copyright is not transferred to the user (see Symon 121).

definition of ''licence''

In general terms, a copyright licence may be defined as the authorisation by the copyright owner to perform certain acts which, in the absence of the express authorisation, would have constituted copyright infringement. The primary difference between a licence and a sale is that in the case of a licence, the licensor may place restrictions of use and other limitations on the licensee, whereas in the case of a sale of an article, the only restrictions that apply to the buyer are those prescribed by

copyright law. An analogy may be drawn with manufacturers' guarantees of consumer goods, which also seek to create a separate contract between the manufacturer and the consumer.

ACTIVITY 4.6

Sina and Thieu approach you for legal advice. They wish to market the following works:

- ''TSV-Art'' — a catalogue containing photographs of Sina's artworks: some of her prints may be bought on-line
- ''E-writing'' — Tim's short story

They wish to know whether they should licence the use of their copyright works, or whether they should sell their works on-line.

FEEDBACK

You should explain the difference between a licence and a sale to Sina and Thieu. Remember, although you may buy a work protected by copyright, such as a book, you only become the owner of the physical copy of the work, and you do not also become the copyright owner of the work. Would your answer be any different if they whished to sell the original copy of their work to Sam, a publisher?

4.9.4 Conclusion of a shrink-wrap agreement

conclusion of a shrink-wrap agreement

A warning on the outside of the cellophane wrapper informs the customer that by breaking the seal, he or she accepts the terms of the agreement, which are visible through the cellophane. The typical notice also states that if the user is unwilling to agree to the terms and conditions of the licence agreement, he or she may return the unopened package to the vendor for a full refund.

click-wrap agreement

A concept similar to a shrink-wrap agreement, namely ''click-wrap'' agreement, has been developed for the sale of computer programs via **electronic commerce**. Basically, a click-wrap agreement will entail a screen on a commercial website with the terms and conditions of a contract of sale. If the user then wishes to purchase products offered through this ''electronic shop'', he or she will be instructed to ''click'' on certain icons, indicating his or her acceptance of the terms of the contract (see this study guide, study unit 3, for the discussion of ''Acceptance of standard terms'' ''contracts of adhesion'', ''ticket cases'' and ''click-wrap contracts''.)

ACTIVITY 4.7

List the similarities and differences between a shrink-wrap agreement and a click-wrap agreement.

SIMILARITES	
Shrink-wrap Agreements	**Click-wrap Agreements**

DIFFERENCES	
Shrink-wrap Agreements	**Click-wrap Agreements**

FEEDBACK

You should have noted that the similarities between shrink-wrap agreements and click-wrap agreements are as follows:

- Both indicate a manner of acceptance — by breaking the seal or by ''clicking''.
- Both require an action by the user.
- Both incorporate standard terms.
- Both have become entrenched in standard trade practices.

You should have noted that the differences between shrink-wrap agreements and click-wrap agreements are as follows:

- Shrink-wrap agreements are used in conventional trade, whereas click-wrap agreements are used in the electronic environment.

- Shrink-wrap agreements are generally used for computer programs only, whereas click-wrap agreements are used in the electronic environment for all types of product or service.
- Shrink-wrap agreements purport to establish licensing agreements between the user and the copyright owner after the contracts of sale have been concluded, whereas click-wrap agreements are used for concluding sales of products or services, or for the licensing of software.

4.9.5 International initiatives in the regulation of click-wrap agreements

4.9.5.1 The position obtaining in the United States of America

a Uniform Computer Information Transactions Act

UCITA

A very important development in the United States was the enactment of the Uniform Computer Information Transactions Act 2000 (referred to as ''UCITA'' and previously known as ''Art 2B'') which creates an enforceable set of rules for electronic licensing agreements.

reasonable medium

The Act provides that the offer and acceptance may be made in any manner, and by any medium reasonable in the circumstances (ss 202 and 203). Electronic interactions between human and electronic agents (that is, automated systems) are sufficient to create a valid contract (s 206).

manifest assent

A person adopts the terms of a contract by manifesting assent. He or she can do so by signing the record embodying the terms, or by some other affirmative conduct, such as clicking on an icon. The adopting party must have had the opportunity to review the terms before reacting. All that is required is that the terms or record be brought to his or her attention before manifesting assent. It is not necessary for him or her to have actually read, understood or negotiated the terms in order to be bound (s 203).

mass-marketed software

Section 208 deals specifically with mass-market licences such as shrink-wrap and click-wrap licences. It mentions a series of rules which will render mass-market licences enforceable, even though they are not signed by both parties, and even if the licence terms are not available prior to the purchase. The section endorses the use of click-on licences by providing that assent to the terms of the licence may be manifested before or during the initial use of, or access to, the software. If the licence terms are presented to the licensee after an initial contract, the licensee must have had reason to know that the terms would be proposed later for assent.

affirmative conducts

A licensee manifests assent by signing the record or term, or by some other affirmative conduct (see *Evans Fordham Intellectual Property, Media and Entertainment LJ* 277–278). This assent may be shown by using the product after having an opportunity to know about the licence terms. A party must be afforded an opportunity to decline to take such action after having the opportunity to review the licence.

opportunity to decline

A licensee manifests assent by signing the record or term, or by some other affirmative conduct that, under the licence, constitutes acceptance of the record or term, as long as the party was afforded an opportunity to decline to take such action after the licence. If the terms of the licence are available for review only after the licensee has paid its fee, the licence is not binding, and a refund is available if the licensee stops using the software and returns all copies. If a specific term is one that the licensor should know would cause an ordinary and reasonable licensee to refuse the licence, that term does not become part of the licence unless the licensee ''manifests assent'' to that specific term.

b The ProcCD case

The first decision to accept article 2B's approach to mass-market licences was *ProCD v Zeiderberg.*

The protected work was a CD-ROM version of a national telephone directory, containing millions of entries and packaged in a shrink-wrap licence. Pro-CD charged a low price to consumers, and a much higher one to commercial users of the product. The defendant ''bought'' a consumer package and then, in violation of the licence, sold the information contained over the Internet. Inside the box was a form indicating that the information on the disk was licenced for home use only. Because Zeidenberg could have obtained a refund if he had not liked the terms, and because of the potential for market failure if the licence was not enforced, the court of first instance, decided to enforce the shrink-wrap licence and found that Zeidenberg's loading of the software onto a website constituted a breach of the home-use licence term.

A second issue in *Pro-CD* was whether federal copyright policy forbade enforcement of this contract clause. Zeidenberg also argued that federal copyright law should ''pre-empt'' enforcement of a state contract, since the state law cannot alter the delicate balance of federal copyright law.

The Appellate Court, however, disagreed. Easterbrook J, writing for the majority, found no pre-emption problem once he differentiated between rights that were good against the person in agreement alone, and rights that were good against the world. Since there was an ''extra element'' of agreement, the state-contract claim was not ''equivalent'' to a copyright claim.

Hence, federal policy did not pre-empt enforcement of this state-contract provision.

The *Pro-CD* decision has generated controversy, regarding both its assessment of state-contract law and its pre-emption analysis. Some commentators continue to question whether it is appropriate to enforce shrink-wrap and other mass-market licences for copyrighted works. Although other commentators have endorsed the results of *ProCD*, these commentators would like the courts to distinguish between socially beneficial shrink-wrap licence terms and licence terms that reduce competition and retard innovation (Reichman & Franklin, paper delivered at the Berkeley Conference). It has been noted that it is unclear to what extent European courts would follow *ProCD*'s validation of shrink-wrap licences (see Samuelson paper delivered at the Conference on Intellectual Property Law & Policy 16).

4.9.5.2 The position obtaining in the European Union (EU)

a The Directive on Electronic Commerce

Article 10 of the Directive on Electronic Commerce refers expressly to electronic contracts concluded by electronic means and refers to ''the different technical steps to follow to conclude the contract'' (see article 10(1)(a)). The Directive thus also refers indirectly to click-wrap agreements.

b Case law

Beta v Abode

A Scottish court gave effect to shrink-wrap terms allowing a right to return software *(Beta v Adobe)* and has thus confirmed the enforceability of click-wrap agreements.

However, a Dutch court held that a licence agreement could not be formed by opening the package of software, even as between commercial entities *(Coss Holland BV v TM Data Nederland BV)*. It has been noted that it is highly doubtful whether a European court would have come to the same conclusion in circumstances similar to those of the *ProCD* case.

Coss Holland

ACTIVITY 4.8

Thieu approaches you for legal advice. He has written a computer program which teaches users how to compose a short story. Thieu wishes to market the program on-line in the EU and in the US. However, he wishes users to use the program only for noncommercial and private use. Thieu wishes you to advise him on the following aspects:

- whether such an agreement will be valid and enforceable in the US and in the EU
- what the content and construction of the click-wrap agreement should be

FEEDBACK

In your advice you should address the enforceability of click-wrap agreements as decided by the court cases above. You should also have included those requirements to determine what the content and construction of the click-wrap agreement should entail.

4.10 COPYRIGHT LAW AND THE INTERNET: THE POSITION OBTAINING IN SOUTH AFRICA

4.10.1 Copyright law and digitisation of works

reproduction

South Africa has acceded to the WIPO Copyright Treaty, but has not yet implemented its provisions in national legislation. However, as a member state of the Berne Convention, we agree with the interpretation of article 9 and the exceptions permitted under it as expounded in the WIPO Copyright Treaty. The reproduction right of the copyright holder of a literary or art-

reproduction

artistic work fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention (it is also a reproduction in terms of s 6 of the Copyright Act of 1978).

South African copyright law has not yet been amended to accommodate the e-commerce implications within the realm of traditional copyright principles. The ECT Act, however, makes provision for the limitation of liabilitiy of service providers.

shrink-wrap agreements

Although an analysis of the general principles of South African law of contract indicates that a shrink-wrap agreement is in compliance with the basic requirements of an enforceable contract, the enforceability of such agreement has not yet been tested by a South African court of law. The superior bargaining power of the software developer puts the consumer in a ''take-it-or-leave-it'' position, and several of the user's statutory entrenched rights may be curtailed by this agreement forced upon him or her.

South African software developers who wish to market their products internationally, as well as domestic users of software products, should take note of international developments, as the law of a foreign nation may be regarded as the proper law of such contract. Recent developments in the United States, in particular, should be heeded. It is clear that standard shrink-wrap licences accepted by a user in South Africa may be subject to interpretation according to the law of a foreign jurisdiction.

ACTIVITY 4.9

How do I know where and against whom I can institute a claim for copyright infringement if John, resident in the United Kingdom, makes use of a service provider located in the United States to send unauthorised copies of paintings of a South African artist, Thandi, to a commercial dealer, ''Cyberart'', which is located in Australia?

FEEDBACK

When determining the liability of a particular OSP, one should remember that the law of delict, the law regarding unfair competition and copyright law impose liability for acts or omissions in a specific instance. So, an OSP's liability will depend on the role it plays in a particular transaction.

To answer your question: if an OSP makes unauthorised reproductions of a protected work (eg, for technical reasons such as caching), it may be liable for direct infringement of copyright. Especially if ''in-links'' and framing are used, it will form a ground for copyright infringement. Hypertext linking may, in certain instances, constitute infringement. ''In-linking'' to create meta sites may also constitute infringement. Case law exists where this has been established.

But if, on the other hand, an OSP merely transmits or facilitates access to copyright-infringing material, it may, at common law, be liable for ''contributory infringement''. With the potential liability of OSPs established in this way, attention has now shifted to mechanisms for limiting such liability. For example, if a service provider was acting as a ''mere conduit'' or if no knowledge of infringing content is proved, acts such as the US's Digital Millennium Copyright Act provide for the limitation of liability of such service providers.

Remember that copyright is protected internationally, and that no formalities are necessary for protection to exist. For example, if countries are member states of the Berne Convention, works created in member states are afforded the same protection as works of foreign origin.

In general, if content of author Thandi is created and protected in country A (South Africa), and its content is violated by a server hosted by Y in country B (the United States), the action may be instituted in the United States. The copyright law of South Africa will be applied to determine whether copyright protection exists, and the copy-

right principles of the United States will be used to determine whether copyright was infringed by John, and whether any limitations of liability are applicable in terms of the laws of South Africa. If Thandi wishes to act against Cyberart, she must institute action in Australia.

4.11 CONCLUSION

By now, you should be able to identify the different international instruments relevant to copyright protection, and to determine their relationship with one another. You should also appreciate that copyright, like other intellectual-property rights, is territorial by nature — the rights of an author in a country are determined by the law of that particular country, and are completely independent of equivalent rights governing the same subject matter in other countries.

4.12 CHECK LIST FOR INTERNET CONSIDERATIONS

Most materials on the Internet, such as computer software, codes, et cetera, are protected by copyright.

Check list for copyright considerations:

- downloading material from the Internet may involve breach of copyright
- browsing is permissible, provided that a temporary and incidental copy is made in the process of viewing the material
- hypertext links with other websites are normally permissible
- deep-linking is not permissible
- framing must not be done so as to obscure third parties' advertisements and other information
- hosting is permissible: however, if hosting is done with the knowledge of infringement, liability will follow
- requirements for limitation of liability for linking, framing, and hosting must be complied with
- if applicable, obtain permission for links
- include a copyright notice on the website
- obtain permission for loading/displaying third parties' copyright works
- implement electronic-rights-management systems
- use technological protection measures
- provide contact details of the webmaster

If you are still unsure about any aspects of copyright law and the Internet, try to answer the self-evaluation questions listed below.

4.13 SELF-EVALUATION QUESTIONS

(1) Can a service provider be held liable if a subscriber posts infringing copyright material on his or her site?
(2) Are e-mails and contributions to mailing lists or discussion forums copyrightable? May these messages be distributed; posted?
(3) When will framing constitute copyright infringement?
(4) When will linking constitute copyright infringement?
(5) What is ''electronic-rights management''?
(6) What are the latest developments in copyright infringement on the Internet?

STUDY UNIT 5

The protection of electronic databases

Tana Pistorius

OVERVIEW

In this study unit, we shall explore the protection of electronic databases. We shall examine the process of database creation, and explore the role of electronic databases in the information society. The copyright protection of original electronic databases and the *sui generis* protection of nonoriginal databases will also be examined.

LEARNING OUTCOMES

After completing this study unit, you should be able to do the following:

- understand the role of e-databases on the Internet
- understand the process of creating a database
- understand and interpret the provisions of the international treaties
- understand and apply the concept ''originality''
- explain and apply the rules regarding the protection of nonoriginal databases in the EU
- interpret and evaluate the position obtaining in South Africa as compared with the position obtaining in other jurisdictions

SETTING THE SCENE

TVS's website is called ''TSV-ALL'', and its homepage is divided into the following three parts: ''TSV-Art'', ''TSV-Ewrite'' and ''TSV-auto''. Vuzi becomes involved in the creation of an electronic database of spare parts and accessories.

PRESCRIBED MATERIAL

None.

5.1 INTRODUCTION

Why databases?

Why do we cover this subject matter in a course on commercial-law aspects of electronic commerce? The answer lies in the fact that databases form the core of the Internet. The Internet's most powerful feature is its ability to connect individuals with a myriad of sources containing thousands of pages of information (see Caffarelli *Boston Univ J of Science and Technology* para 28). The Internet has been described as offering ''access to information and resources beyond measure, limited only by your ability to find them'' (Caffareli *Boston Univ J of Science & Technology* par 29). Much of this information is organised in the form of databases. It is obvious that in the information age there is a need for a secure means of protecting databases in cyberspace.

ACTIVITY 5.1

Find three kinds of search engines on the Internet.

FEEDBACK

You will learn more about the different kinds of databases. Evaluate your answer to the above activity after reading 5.3 below.

5.2 THE ROLE OF ELECTRONIC DATABASES

the role of data-bases

The Internet has changed from a quiet means of communication in academic and scientific-research circles to a major global data pipeline through which large amounts of intellectual property move (see Hayes *Texas Intellectual Property LJ* 2–3). Initially, on-line information-retrieval services were expensive, and so were used by a relatively small community of corporate or academic subscribers only. The development of the Internet has changed this situation forever, and has made the term ''on-line'' a household word (Forhan *Capital University LR* 869).

5.3 WHAT DO ELECTRONIC DATABASES CONSIST OF?

What are ''electronic databases''?

Electronic databases are simply organised collections of recorded data or information in an electronic or digital form, from where such data or information may be accessed, reproduced, or retracted. It has been said that few people have information. Instead, what they actually have is data, in such quantities that it causes **information overload or blackout** (Bastian *Boston College Environmental Affairs LR* 426; see also Reichman & Samuelson *Vanderbilt LR* 64–65).

tools of information

Databases are the tools that provide information about information. They have become the new building blocks of knowledge (Bastian *Boston College Environmental Affair LR* 426), and they are indispensable to e-commerce. The importance of electronic databases should not be underestimated — they form the core of information technology and all information systems (see Lavenue *Santa Clara LR* 1).

search engines

Over the past several years, the market has exploded with new tools for searching, matching, collating, updating, replicating, and distributing data. A now familiar example is that category of tools often lumped as ''Internet search engines''. A ''search engine'' is simply a computer program designed to accept inquiries from the user and search large electronic databases for relevant information (Forhan *Capital University LR* 877). In response to simple user requests, search engines can root out digital property irrespective of geographic location (see Brown, Bryan & Conley *Richmond J of Law & Technology* text at note 24).

5 sets of tools

The popular term ''search engine'' actually embraces five categories of tools: **directories** (such as Yahoo), **Magellan search engines** (such as Lycos, Infoseek, and Webcrawler), **super search engines, meta search engines, and special search engines.**

super search engines

Super search engines expand on the search-engine concept by searching for key words within the text of webpages, instead of just in page titles, descriptions, and meta tags. A meta search engine (such as like Metacrawler and Savvy Search) allows users to employ multiple search engines, or even super search engines, simultaneously (Brown, Bryan & Conley *Richmond J of Law & Technology* text at note 24).

meta search engines

Meta search engines typically do not contain a site database of their own: they merely route requests to a variety of different engines, and then compile and return the results to the requesting party.

special search engine

A special search engine targets specific types of information such as Usenet newsgroups (DejaNews), telephone listings (Infospace), and FTP (File Transfer Protocol) archive sites (FTP Search). These engines all search by keyword, although the actual search logic depends upon the individual engine. The search engine's algorithm breaks down the question to determine the search criteria and locate relevant responses (see Forhan *Capital University LR* 877).

5.4 LEGAL PROTECTION OF DATABASES

5.4.1 Introduction

The variety of entities grouped together under the heading ''database'' comprises a complex array of potential intellectual

variety of entities

property. The principal categories include the data itself, the effort used to locate it, the effort and any originality involved in selecting and arranging the available data, and the tools for search and organisation, together with all aspects of their creation (Brown, Bryan & Conley *Richmond J of Law & Technology* text at note 32).

raw effort vs new software

The process of collecting and organising information in its most basic form is a matter of raw human effort. They maintain that the effort involved in the production of an old-fashioned database such as a telephone directory falls into this category. The cliché often used to describe scientific research is quite apt: this type of process is indeed made up of 99 percent sweat and one percent originality. At the other end of the spectrum we find the development of new software tools to mine existing data resources.

ease of exploitation

Tremendous resources are often invested to assemble large quantities of information into a database. Still, the resulting product is vulnerable to being quickly and inexpensively copied with current digital technology. The ease with which digital property can be located, accessed, copied, modified, and distributed is without precedent. Also, advances in copying and editing capabilities can lead to recompilations and new derivatives beyond the imagination, let alone the knowledge, of the original owner (Brown, Byran & Conley *Richmond Journal of Law & Technology* 2). It has been noted that, from an economic point of view, all electronic databases have two characteristics in common — ''they are costly to produce, but they are easy to reproduce or copy'' (Nelson *J of Intellectual Property Law* 455).

ease of access

Moreover, because of widespread access to global information networks, pirated copies of a database can be disseminated in a matter of moments to millions of people across the globe at a fraction of the development costs. Consequently, compilers of uncopyrightable databases face diminishing prospects of commercial success unless they obtain international standards of protection to thwart pirating of their products (Bastian *Boston College Environmental Affair LR* 428–429).

ACTIVITY 5.2

Apply the knowledge you gained in study unit 4 on the effect of digitisation of intellectual-property law. Apply this to the problems facing electronic databases.

FEEDBACK

All the features that make digitised copyright works easy to exploit and difficult to protect are also features of electronic databases.

legal problems

Like new technologies of the past, databases have caught the world's intellectual-property system napping. Computers can, of course, archive, compare, manipulate, and distribute data with astonishing facility. But, in addition, neither the data, nor the labour involved in collecting, recording, and arranging it, has a secure place in the current structure of intellectual-property law (Brown, Bryan & Conley *Richmond J of Law & Technology* 2). As the database market grows and cross-border information flow increases, the demand for a stable and harmonised legal environment for databases increases (see Barrett & Coulter *Computer Law & Practice* 34).

5.4.2 Copyright protection

5.4.2.1 Introduction

the role of copyright

Copyright law, electronic databases, and the Internet are inextricably linked. There are two main reasons for the close relationship between copyright law and the flow of information on the Internet. First, much of the material that is communicated on the Internet constitutes works of authorship, such as literary and musical works, audiovisual works, computer programs, and database information, which fall within the usual subject matter of copyright. Secondly, since the very nature of an electronic on-line medium requires that data be copied or reproduced as it is transmitted through the various nodes of the network, copyright rights are obviously at issue (Hayes *Texas Intellectual Property LJ* 3).

5.4.2.2 Criteria for the subsistence of protection

a Selection and arrangement

selection & arrangement

Article 2(5) of the Berne Convention reads as follows:

> Collections of literary or artistic works … which, by reason of the selection or arrangement of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections.

Article 10(2) of the TRIPS Agreement provides the following:

> Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself

Article 5 of the WCT reads as follows:

> Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation.

The Agreed Statement concerning Article 5 of the WCT reads as follows:

> The scope of protection for compilations of data (databases) under Article 5 of this Treaty, read with Article 2, is consistent with Article 2 of the Berne Convention and on a par with the relevant provisions of the TRIPS Agreement.

Article 3 of the EC Directive on the Legal Protection of Databases reads as follows:

(1) In accordance with this Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected by such copyright. No other criteria shall be applied to determine their eligibility for that protection.
(2) The copyright protection of databases provided for by this Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves.

ACTIVITY 5.3

Complete the following spreadsheet by inserting the ''selection and arrangement'' requirements for the subsistence of protection for databases in terms of the Berne Convention, the TRIPS Agreement and the WCT.

Requirements for protection		
Berne Convention	**TRIPS Agreement**	**WCT**

FEEDBACK

In your answer, you should have indicated as many similarities and differences as possible, by referring to the type of materials protected, the form that it must be in, the manner in which it must be selected and the copyright protection which vests in the underlying material itself.

b Originality

originality

Traditional copyright principles require a measure of originality or creativity in the selection or arrangement of data in a compilation, or other indications of creative authorship, for the compilation to attract copyright. The requirement of originality for copyright protection of compilations is interpreted differently in various legal systems.

Berne Convention

Article 2(5) of the Berne Convention for the Protection of Literary and Artistic Works states that collections of literary or artistic works (such as encyclopaedias and anthologies) which, by reason of the selection and arrangement of their contents, constitute intellectual creations are protected as such, without prejudice to the copyright in each of the works forming part of such collections. Bare facts cannot be protected by copyright, but compilations of facts are within the subject matter of copyright protection if these compilations constitute original works of authorship.

sweat of the brow

United Kingdom and Commonwealth courts have, famously or infamously, favoured the ''sweat -of-the-brow'' approach to database protection (see *Waterlow Publishers Ltd v Rose*; *Waterlow Publishers Ltd v Reed Information Services Ltd*). If an author has expended labour and skill in creating the work, it will enjoy copyright protection, notwithstanding the bland nature of the work.

high level of skill

Under traditional German copyright principles, most factual databases do not qualify for copyright protection unless their ''selection, accumulation and organization'' has been the subject of know-how beyond that of the average programmer (see *Incassoprogramm*; see also Pattison *European Intellectual Property Review (EIPR)* 113–114). In terms of French copyright law, which requires original works to reveal something of the author's own personality, and Dutch Copyright law, most compilations will not enjoy copyright protection (see *Van Dale v Romme*, quoted by Cornish 3 n9; see also Pattison *EIPR* 114 n12–13).

US before Feist

Before the Supreme Court's decision in *Feist Publications Inc v Rural Telephone Services Co* 344–348), American courts occasionally granted copyright protection for the effort involved in finding and assembling a body of collected data under the ''sweat-of-the-brow'' doctrine (see, for example, *Jeweler's Circular Publication Co v Keystone Publication Co*; *Leon v Pacific Telephone & Telegraph Co*).

Feist

However, in *Feist*, the court held that the expenditure of labour and capital (the ''sweat of the brow'') on the creation of a compilation, no matter how extensive in nature, in and of itself, does not make a compilation copyrightable (364). (This case involved the most primitive of all forms of database — a telephone directory).

3 requirements

The court noted that the following three elements form the basis of the copyright protection of a factual compilation of pre-existing facts: the compilation

(1) consists of pre-existing facts or data,
(2) is selected, co-ordinated, or arranged by the author, and
(3) is an original work of authorship ''by virtue of the particular selection, co-ordination, or arrangement'' of the data (357).

originality requirement

''Originality'' requires only a ''minimal level of creativity'' evidenced by the fact that the author worked independently of any pre-existing materials in selecting and arranging the new compilation (358). It has been said that the second element is the most important one, as it requires a court to evaluate a compilation's originality by examining the author's selection and arrangement of the data (see Caffarelli *Boston University J of Science & Technology* para 30).

new rule: a standard

It is an open question whether *Feist* sounded the death knell for copyright protection of noncreative databases. However, it is clear that *Feist* has raised the originality bar. The standard may be minimal, but it is still a standard. Also, courts are no longer free to ignore the originality requirement, or to substitute ''sweat of the brow'' (see Brown, Bryan & Conley *Richmond Journal of Law & Technology* text at note 93).

Warren

In *Warren Publishing Inc v Microdos Data Corp*, the plaintiff published a directory of information about American cable-television systems, called the *Television & Cable Factbook*. The defendant marketed a software package that contained the same information. Warren asserted that the software package infringed the copyright in its ''factbook''. The court, however, ruled that the compilation was not entitled to copyright protection, for it lacked sufficient creativity (1520). Proponents of database-protection legislation often point to *Warren Publishing* to justify their calls for stronger protection (see Nelson *Intellectual Property LJ* 464).

catalogue protection

A special form of copyright protection, akin to neighbouring rights, may be found in Scandinavia and the Netherlands. In Scandinavia, ''catalogue protection'' may be afforded to factual compilations; the Dutch extend such protection to ''nonpersonal'' writings.

ACTIVITY 5.4

Vuzi becomes involved in the creation of an electronic database of spare parts and accessories. He wishes to know what a ''database'' is, and whether his database will be protected by copyright law. Explain the legal requirements for the copyright protection of databases to him.

FEEDBACK

The situation should be evaluated in terms of South African copyright law. Refer to study unit 4 and the prescribed material and refresh your knowledge on the requirements for the subsistence of copyright protection. Remember that databases (whether they are in electronic or paper form), fall under literary works in terms of the Copyright Act 98 of 1978.

5.4.3 Competition law

In the United States, the Supreme Court expressly stated that protection for the investment of labour and capital in non-creative databases ''may in certain circumstances be available under a theory of unfair competition'' (*Feist* 354).

A few courts have also recognised noncopyright protection for facts amounting to ''hot news'' under state laws of misappropriation.

In *National Basketball Association v Motorola Inc*, it was held that New York common law protects time-sensitive data from ''free-riding'' under limited circumstances (845). In this case, the National Basketball Association brought a copyright-infringement action against Motorola, the manufacturer and promoter of hand-held pagers that provided real-time information updates about professional basketball games. The operation of the pagers relied on a ''data feed'' from reporters who watch the games on television or listen to them on the radio. Information concerning the score and time remaining was then relayed by modem to a satellite, which emitted a signal updating each of the pagers. The court held that the information transmitted by Motorola to its pager customers did not constitute ''hot news'', and so the National Basketball Association was denied copyright protection (845).

hot news

The Second Circuit explained that a 'hot news' claim is limited to cases in which

limits

(1) a plaintiff generates or gathers information at a cost;
(2) the information is time-sensitive;
(3) a defendant's use of the information constitutes 'free riding' on the plaintiff's efforts;
(4) the defendant is in direct competition with a product or service offered by the plaintiffs;
(5) the ability of other parties to ''free ride'' on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened.

Unfair-competition principles are limited to regulating the behaviour of competitors. Database protection should address not only the ''free rider'', but also the ''information Samaritans'' (Bastian *Boston College Environmental Affairs LR* 443). Also, private unauthorised use of databases may not be addressed through principles of unfair competition.

only competitors

5.4.4 Contract law: ''click-on'' contracts

The proprietor's options include the offering of on-line contracts whereby users may assent to a ''click-on'' licence, with or without user identification, as a condition to access or downloading capability, or both. The proprietor may thus seek to regulate use of his or her database by means of contract law.

click-on contracts

The most recent, and perhaps the most authoritative, case which addressed click — on contracts (*ProCD Inc v Zeidenberg*)

was a ''high-tech version'' of *Feist* — the protected work was a CD-ROM version of a national telephone directory, containing millions of entries and packaged in a shrink-wrap licence (see the discussion of shrink-wrap and click-wrap agreements in study unit 4).

Pro-CD charged a low price to consumers and a much higher one to commercial users of the product. The defendant ''bought'' a consumer package and then, in violation of the licence, sold the information over the Internet. The Seventh Circuit held that a shrink-wrap licence is an ordinary contract that is enforceable under the Uniform Commercial Code (UCC).

limits of law of contract

Contract law may in certain instances bolster or complement the copyright protection of databases. However, it should be noted that contract law applies only between parties bound by the contract: a contract cannot bind third parties. Also, contract law has not been harmonised, although international legal rules for e-commerce, including aspects of contracting on the Internet, are being negotiated.

5.4.5 Conclusion

important databases excluded

Copyright law seems to be the most apt system for the protection of databases. However, the requirement of ''originality and a modicum of creativity'' is too stringent for electronic information tools, which process and store information automatically. In practice, it is becoming increasingly difficult in practice to determine whether, and which aspects of, a database meet this requirement, as new technologies which permit more ''intelligent'' computer-based analysis of text blur the line between information and expression. The most important commercial and scientific databases are effectively excluded from copyright protection, as they do not meet the requirements of originality.

ACTIVITY 5.5

Vuzi has created his own electronic database of spare parts and accessories. He has scanned the information pertaining to all the parts and accessories of the 20 most popular makes of car. Vuzi has spent two months collecting all the information and he has also spent some time in arranging all the information under specific headings. Vuzi wishes to know what form of protection will be the best for his database: copyright law, law of competition, or contract law. Explain the advantages and disadvantages of protection under each of the areas of law.

FEEDBACK

Your advice to Vuzi should include all relevant information. Have you considered the following:

- To qualify for copyright protection, the database must meet certain requirements.
- The copyright can be enforced against third parties.
- It is very difficult to detect infringement of an electronic database.
- The copyright systems of most countries contain similar elements, as most are members of the Berne Convention.
- Contract-law principles differ from country to country.
- Contracts may not be enforced against third parties.
- The law of competition will not be a deterrent as far as ''information Samaritans'' or ''free riders'' are concerned.
- Not all infringers are competitors.
- In certain instances, a monopoly over information may be seen as ''anticompetitive'' in nature.

5.5 INTERNATIONAL INITIATIVES

5.5.1 The EU Database Directive

5.5.1.1 Introduction

Database Directive

The European Community adopted the Council Directive on the Legal Protection of Databases (''the Database Directive'') on 11 March 1996, after nearly eight years of deliberation. The primary purpose of the Database Directive is to stimulate investment in databases, and so increase the European share of a market which is a ''cornerstone'' to the economic-development plans of the Union (Bastian *Boston College Environmental Affairs LR* 440).

definition

Article 1(2) of the Database Directive gives a very broad definition of the concept ''databases'': the term connotes ''a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means''. It is not required that the data contained within the database ''be physically stored in an organized manner''.

all-inclusive

This very broad definition is specifically intended to include nonelectronic databases and the materials necessary for the operation or consultation of certain databases, such as thesaurus or indexation systems Thus, a CD-ROM-based multimedia package, a World Wide Web site, an electronic or paper library-card catalogue would fall within the scope of the Database Directive

Article 1(3) excludes from protection under the Database Direc-

tive any computer programs used in the manufacture or operation of databases. Article 2 of the Database Directive provides that it does not pre-empt other community statements on copyright, including the 1992 Council Directive on the Legal Protection of Computer Programs (''the Software Directive''). Article 2 appears to be at odds with Recital 20, which states that protections may extend to ''the materials necessary for the operation or consultation of certain databases'', such as the ''thesaurus and indexation systems''.

exclusions

Some also argue that a computer program could be seen as a thesaurus or index for operating or consulting a database (see Baker & McKenzie and Hart 105 par 6.15). We prefer the view that ''thesaurus'' and ''index'' refer to other collections of data stored with the database to facilitate access to it. An index may be maintained to increase the speed of access, whereas a thesaurus may be used to define parallel or equivalent meanings of certain items of data.

computer program

Some databases may contain executable instructions (Bainbridge 171). It is unclear whether the Database Directive or the Software Directive will apply to the mechanisms involved in manipulating the contents of a database (see Baker & McKenzie and Hart 105; Bastian *Boston College of Environmental Affairs LR* 441). Pattison's argument (*EIPR* 115) that the command procedures for accessing databases are included under the ''system for obtaining or presenting information'' applies with equal force to ''materials necessary for the operation or consultation of certain databases''. Such command procedures will attract copyright protection only if the database with which it is used is copyrightable.

command procedures

However, the Software Directive will continue to specify the appropriate level of copyright protection for search engines and related software tools (see Brown, Bryan & Conley *Richmond Journal of Law & Technology*, text at note 131; also see recital 23 and art 1). Recital 23 applies to database-management systems, such as search engines, used in the **making and operation** of a database which fall outside the scope of the Database Directive.

Software Directive

Note that recital 20 to the Database Directive is restricted to **materials necessary for the operation or consultation of a database.** It may be argued that these works, such as command procedures, form part of the structure of the database and that they form an integral part of the arrangement of the material.

material included/ excluded

Recital 17 to the Database Directive includes materials such as **text, sound, images, numbers, facts, and data.** The Directive does not apply to all data. Restrictions are, for example, imposed on the use of **personal data.**

5.5.1.2 Copyright protection

The Database Directive extends copyright protection only to databases that by reason of selection or arrangement of the database's contents constitute ''the author's own intellectual creation'' — databases which evidence some measure of ''originality'' or ''creativity'' on the part of the author (see recital 15 and art 3(1)). Article 5 states that compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself, and is without prejudice to any copyright subsisting in the data or material contained in the compilation.

intellectual creation

Article 5 adopts the approach of the American Supreme Court's decision in *Feist Publications Inc v Rural Telephone Services Co* 344–348, in which it was held that only the selection or arrangement of a compilation of facts, and not the facts themselves, can be protected under copyright. The Database Directive rejected the traditional approach of the United Kingdom and Ireland and raised the threshold for copyright protection. As noted, this standard is very similar to that applied in the United States after *Feist*, with one further limitation — under the Database Directive, there must be intellectual creation by a human author for copyright protection to exist (art 4(1)). It may be questioned whether it is conceptually correct to restrict the originality requirement to the selection or arrangement of the data, rather than to have it relate to the work as a whole. Barrett & Coulter (*Computer Law & Practice* 35) argue that a database is characterised as much by the totality and comprehensiveness of its contents as by their selection and arrangement.

human author

machine only

The requirement of a human author raises questions about the extent to which a database can be protected under copyright law if the selection and arrangement of data is accomplished by a computer program with minimal human contribution. A case in point is, computer-generated databases.

Article 4(1) provides that the author of a database is a natural person who has created the database, and, if legislation of member states permits, the legal person designated as right-holder. Pattison (*EIPR* 119) notes that this begs the question regarding who is the ''creator''? Is it the person who entered the materials into the database, the person who chose the selection and arrangement criteria, or the person who made the arrangements for the making of the work?

definiton of ''author''

The Database Directive provides that moral rights of the author fall beyond its scope (see Recital 28). It would thus appear that an author may enter into a separate agreement regarding moral

moral right

rights of a work (see Barrett & Coulter *Computer Law & Practice* 35). Also, the Database Directive does not provide clear guidance on where the line should be drawn between an original and a nonoriginal database.

exclusive rights

The Database Directive extends the exclusive right to the author to carry out or to authorise certain acts regarding the database. These acts include the following:

- the temporary or permanent reproduction of the database
- the translation, adaptation, arrangement, and any other alteration of the database
- any form of distribution to the public
- any communication
- any display or performance of the database to the public (art 5)

interactive service?

The Database Directive did not concern itself with digital servicing or temporary distribution. Also, the nature of rights in transmission on demand is not addressed, as it is uncertain whether public communication must be for general reception at a given time (see Cornish 6).

5.5.1.3 Sui generis protection

a Introduction

Article 7 of the EC Directive on the Legal Protection of Databases reads as follows:

> (1) Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.
>
> ...
>
> (4) The right provided for in paragraph 1 shall apply irrespective of the eligibility of that database for protection by copyright or by other rights. Moreover, it shall apply irrespective of eligibility of the contents of that database by copyright or by other rights. Protection of databases under the right provided for in paragraph 1 shall be without prejudice to rights existing in respect of their contents.

b Substantial investment

The *sui generis* provisions of the Database Directive protect the contents of any noncopyrightable database that is the product of substantial investment in obtaining, verifying, or presenting the database's contents (see Recital 39 and art 7(1)). There are no

substantial investment

specific standards for determining the substantiality of an investment. The test is quantitative as well as qualitative in nature. The investment may concern the obtaining, verification, or presentation of the content (see Cornish 8). Not every compilation of information will be considered a ''database'' for the purpose of the sui generis right. To qualify for protection, a database must be ''a collection of independent works, data or other materials arranged in a systematic or methodical way, and individually accessible by electronic or other means''.

c Scope of protection

scope of protection

The *sui generis* right enables the maker of a database ''to prevent extraction and/or re-utilization of the whole or of a substantial part'' of the database contents, and the repeated and systematic extraction or reutilisation which unreasonably prejudices the maker's ''legitimate interests'' (arts 7(1) and (5)).

extraction

''Extraction'' is defined as

- the permanent or temporary transfer
- of all, or a substantial part of the contents of the database
- to another medium
- by any means or
- in any form.

''Reutilization'' means

- any form of making
- the contents, or a substantial part of the contents, of the database
- available to the public, whether by

reutilisation

  — distributing copies
  — renting
  — on-line, or
  — some other form of transmission

RAM downloads

Extraction occurs when contents are transferred from paper to disk; RAM downloads also fall within the restricted acts, as the Directive refers to temporary or permanent transfers (see Lui *International J of Law and Information Technology* 85). To download a substantial portion of an electronic database onto the memory of a computer thus constitutes infringement.

no resale control

The right to control resale is exhausted by the first sale of a copy of a database with the consent of the rightholder (art 7(2)(a)–(b) and Recital 44).

The scope of protection of uncopyrightable databases is comprehensive in nature. Article 6 expressly states that the repeated and systematic extraction or reutilisation of insub-

repeated & systematic extraction/utilisation prohibited

stantial parts of a database may also amount to the extraction or reutilisation of a substantial part. This is an important provision, for the typical use of a database involves this very type of access (see Brown, Bryan & Conley *Richmond Journal of Law & Technology* text at note 159).

d Exclusions

Several exceptions are allowed, such as the extraction and/or utilisation of insubstantial parts, or the use of the database for any purpose which does not conflict with normal exploitation of the database or unreasonably prejudices the legitimate interest of the maker (arts 7(2) and 8(1)–(2)). These exceptions are narrower in nature than the similar fair-use exceptions under copyright law. For example, the *sui generis* right has no exceptions regarding to criticism or review, news reporting, or library use.

fair-use exceptions

In addition to these mandatory exceptions, member states may limit the *sui generis* right in certain ways. They may allow the extraction or reutilisation of a substantial part of the contents of a database without its maker's authorisation, provided that such extraction or re-utilisation is for noncommercial purposes, when

other exceptions

(1) the extraction is from a nonelectronic database, for private purposes (art 9(a))
(2) the extraction is reasonable and for the purpose of illustration for teaching or scientific research, as long as the source is indicated (art 9(b)), or
(3) the extraction and/or reutilisation is for the purpose of public security or an administrative or judicial procedure (art 9(c))

e Duration of right

15 years

Article 10(1) provides that the *sui generis* right protects the qualifying database from the moment it is completed; the protection expires 15 years from the first day of January following the date of completion. Perhaps more importantly: if any ''substantial change'' is made to the database, or if a series of successive changes, which constitute a ''substantial new investment'' in the database, accumulates, a further term of protection of 15 years can be obtained see (art 10(3)). The renewal of protection by way of substantial new investment may **perpetuate** protection of dynamic databases.

f Reciprocity

The principle of reciprocity has been incorporated. The *sui generis* right does not apply to databases made by persons

comparable protection

outside the European Union unless they reside in a jurisdiction which provides comparable protection to European Union citizens (recital 56).

g Court cases

The provisions of the Database Directive has been interpreted in case law. A short discussion of some of the cases is given in the prescribed extract from Pistorius ''Copyright Law and IT'' in *Information and Communications Technology Law* (ed. Dana van der Merwe) (2009) at 303-305. Study these prescribed pages.

h Concluding remarks

The *sui generis* right provided by the Database Directive creates an intellectual-property right which goes much further than the copyright law of most countries. This right is not subject to compulsory licensing arrangements, even if the database compiler is the sole source of the database contents.

easy to protect/ easy to infringe

In effect, the Database Directive has created an ''easy-to-protect/easy-to-infringe'' system to protect noncreative databases (see Bastian *Boston College Environmental Affairs LR* 445). Bastian notes that it is ''easy to protect'' because the Database Directive broadly defines a database and provides a *sui generis* intellectual-property right with only a showing of a qualitative or quantitative substantial investment. It is ''easy to infringe'' because of the broad protection afforded by the *sui-generis* right.

The Database Directive has been implemented in many member states, notably also in the United Kingdom (see Copyright and Rights in Databases Regulations). The United Kingdom and Ireland had to raise the originality level for the copyright protection of databases beyond the ''sweat of the brow''. The requirement for database protection has been placed on par with that of the Database Directive (see reg 6).

ACTIVITY 5.6

Vuzi has created his own electronic database of spare parts and accessories. He has scanned the information pertaining to all the parts and accessories of the 20 most popular makes of cars. Vuzi has spent two months collecting all the information, and he has also spent some time in arranging all the information under specific headings.

Vuzi wishes to know what level of protection his database will enjoy in the United Kingdom.

Vuzi has also noted a website on the Internet that advertises a catalogue of motor-car accessories such as car waxes, et cetera. Vuzi has noted that the webmaster of the website is a German national. The website is also hosted in Germany. The database is marked with the words ''database right'', Vuzi wishes to know whether he may download insubstantial parts of this database on a daily basis. He wishes to know whether such extraction will be excused if it is done for educational or for nonprofit purposes.

FEEDBACK

Your advice to Vuzi should include all relevant information. Have you considered the following:

- To qualify for copyright protection, the database must meet certain requirements.
- The copyright systems of most countries contain similar elements, as most are members of the Berne Convention.
- The United Kingdom is a member of the EU; note, therefore, that the provisions on reciprocity apply as far as nonoriginal databases are concerned.
- It should be assumed that the electronic database hosted on the German website is protected in terms of the Database Directive.
- You should advise Vuzi on what the right of extraction and reutilisation means.
- You should explain the exceptions to these rights to Vuzi.

5.5.2 The position obtaining in the United States

The first failed attempt to address the strengthening of database protection in the United States was HR 2281, which formed part of the Digital Millennium Copyright Bill. This proposal followed the approach of the Database Directive.

The Collections of Information Antipiracy Bill (HR 354) has been described as a response to a need to complement copyright law with a federal misappropriation law which imposes a liability on any person who extracts, or uses in commerce, all, or a substantial part, of a collection of information gathered, organised, or maintained by another person through the investment of substantial monetary or other resources, in order to cause harm to the actual or potential market of that other person.

Another approach is to codify at federal level the various state misappropriation laws and to limit the cause of action created to competitive misappropriation of time-sensitive (or ''hot-news'')

information. The preference for a misappropriation approach to protection is consistent with *National Basketball Association v Motorola*. Nelson (*Intellectual Property LJ* 479) notes that adopting legislation which incorporates the ''hot news'' test expounded in *Motorola* would be likely to allow significant reuse of information by subsequent compilers.

5.6 POSITION OBTAINING IN SOUTH AFRICA

When it is said that to be original a work must emanate from the author himself and not be copied from another work, this is, in reality, something of a generalisation. For it is not necessary that every aspect of the work must emanate from the author himself — the author is perfectly at liberty to use existing subject-matter. But where he does so, his work must be more than simply a slavish imitation of some earlier work. To some extent at least it should be the result of the author's own independent labour.

Exactly what degree of labour is required is difficult to say. In the circumstances it may perhaps be best to resort to past decisions of the courts, though it has been said that there is a ''rough practical test that what is worth copying is worth protecting'' (per Petersen J in *University of London Press Ltd v University Tutorial Press Ltd* (supra), approved in *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 All ER 465 (HL)).

Copyright protection has frequently been extended to compilations of non-copyright material because of the labour and skill involved in selecting and arranging the material. For example, protection has been given to compilations such as:

- a street directory (*Kelly v Morris* (1866) LR 1 Eq 697);
- a list of stock-exchange prices (*Exchange Telegraph Co Ltd v Gregory & Co* [1896] 1 QB 147);
- an alphabetical list of railway stations in a railway guide (*H Blacklock & Co Ltd v C Arthur Pearson Ltd* [1915] 2 Ch 376);
- a trade catalogue (*Purefoy Engineering Coy Ltd & another v Sykes Boxall & Coy Ltd & others* (1955) 72 RPC 89 (CA));
- a racing information service (*Portway Press Ld v Hague* [1957] RPC 426);
- chronological fixture lists of football clubs (*Football League Ltd v Littlewoods* Pools Ltd [1959] Ch 637);
- a directory of telefax users (*Fax Directories (Pty) Ltd v SA Fax Listings CC* 1990 (2) SA 164 (D)); and
- a catalogue and price list (*Payen Components SA Ltd v Bovic CC & others* 1995 (4) SA 441 (A)).

When one reads these decisions as a whole, one comes to the conclusion that for a compilation to receive recognition as an

original copyright work, the labour and skill which go into the compilation must be such that the compilation cannot simply be regarded as a copy of existing subject-matter, but rather as a work that contains features and qualities absent in the material form from which it was initially composed.

South African intellectual-property law is clearly lagging behind. The requirement of originality is satisfied solely by the fact that the contents of a particular compilation must have been **independently** collected, and not copied from another. Similarly, under South African copyright, law databases are afforded copyright protection as compilations if they were created by the author's own skills or labour (see *Waylite Diary CC v First National Bank Ltd*). It is clear that the protection of original and nonoriginal databases is of the utmost importance if South Africa wishes to compete and trade effectively on the Internet. Also, as a result of the reciprocity provisions of the Database Directive and other international instruments which are likely to follow, amendments to the Copyright Act 98 of 1978 to raise the level of protection of databases and to address issues such as the scope of protection are necessary.

5.7 CONCLUSION

The keys to copyright protection of databases are selection and arrangement. However, the more comprehensive the database, the less copyright protection may be available.

If everything is included, there is no selection. Stone and Pernick (*The Computer Lawyer* 17) note that a comprehensive database which contains the entire universe of relevant data may be commercially useful, but is not copyrightable, as ''selection'' requires the exercise of creative judgment in culling facts, and not using the relevant universe. This principle may be especially problematic for digital databases such as those accessed through the Internet, since their very appeal is their all-inclusiveness (see Brown, Bryan & Conley & others 1995 (4) SA 441 (A). Also see *Richmond Journal of Law & Technology*, text at note 93).

However, if we conclude that we do wish to protect all types of database, what form should the protection take? The form of protection has the following two components: the nature of what is protected, and the conduct that is prohibited.

Regarding the first component, there seems to be no realistic alternative to the European model of predicating protection on the investment of substantial time or money in the compilation effort (ie, ''sweat of the brow'' or ''bulge of the purse''). It has never been seriously proposed that information itself should be protected (except by the law regarding trade secrets). The

compilations seeking protection are by definition unoriginal in nature. As Brown, Bryan and Conley (*Richmond Journal of Law & Technnology*, text at note 205) so eloquently put it: ''Sweat equity is all that is left''.

It has been noted that there are primarily two reasons why the European Union adopted a norm based on a *sui generis* property interest, instead of one based on principles of unfair competition.

First, a *sui generis* form of protection overcomes the logistical difficulty of harmonisation of legal regimes which vary between member states, both in form and degree of development. Secondly, there was a desire to protect databases from ''information Samaritans'' and ''free riders'' (see Bastian *Boston College environmental Affaris LR* 443; Reichman & Samuelson *Vanderbilt LR* 81). Over and above the difficulties inherent in the harmonisation of the unfair competition laws of member states, the *sui generis* form of protection also addresses the prevention of both commercial and noncommercial appropriation of database content.

Also, as unfair-competition principles are limited to regulation of behaviour between competitors, a norm based on a *sui generis* property interest catches not just the ''free rider'', but also the ''information Samaritan'' (Bastian *Boston College Environmental Affairs LR* 443).

We still know very little about the principles to be applied to computerised databases. So, when we speculate about the legal fate of, for example, Internet databases accessed with powerful search engines, we should remember how little we actually know at this point (see Brown, Bryan & Conley *Richmond Journal of Law & Technology*, text at note 93).

5.8 SELF-EVALUATION QUESTIONS

You may evaluate your knowledge by answering the following questions regarding database protection:

(1) What is a''database right''?
(2) Can a database be protected simultaneously by a database right and copyright?
(3) Is the database right available to a South African creator of an electronic database?
(4) What other forms of protection are available for nonoriginal databases?
(5) How much may I legally download from an electronic database?

STUDY UNIT 6

Domain names and trade marks

Tana Pistorius

OVERVIEW

In this study unit, we will explore the implications of the registration of domain names. The trade mark and domain-name conflicts will also be discussed. We shall explore on-line dispute resolution for solving legal problems that will arise from Internet trading. We shall examine the existing on-line dispute-resolution mechanism, and in particular the rules created by ICANN for on-line dispute resolution of issues relating to domain-name registration.

LEARNING OUTCOMES

After completing this study unit, you should be able to do the following:

- understand what the nature and function of domain names are
- know why and how to register a domain name
- understand what the interrelations between domain names and trade marks are
- know how and where on-line dispute resolutions are conducted

SETTING THE SCENE

TVS's website is called ''TSV-ALL'', and its homepage is divided into the following three parts: ''TSV-Art'', ''TSV-Ewrite'' and ''TSV-auto''. Your clients wish to know what the difference is between trade marks and domain names. Sina and Tim ask you to explain technical terms such as ''top-level domain names''. TSV wishes to register ''TSV-Art.metallinks'', ''TSV-Ewrite'' and ''TSV-auto'' as domain names. Advise your clients on how to obtain their own domain names. Sina becomes embroiled in a dispute with an American website owner who trades under ''METALLINKS.COM''. Sina approaches you for legal advice on how to handle this dispute.

6.1 INTRODUCTION

''.com''

Domain names are also known as ''webaddresses'', ''.com's'', ''dot com's'', ''url addresses'', or ''net names''. In the glossary of terms (Annexure I) a domain name is defined as ''a unique name, which represents each computer on the Internet''. The Domain Name System (DNS) was established to find an orderly manner in which the Internet can be accessed. It is a system that associates a name with each Internet address.

There are two main forms of domain names classified as, first, country top-level domains and denoted by ccTLD's, and second, generic top-level domains denoted by the abbreviation: gTLD's.

6.2 WHAT EXACTLY IS AN IP ADDRESS?

The above-mentioned definitions do not bring us any closer to what a domain name is. Domain names are indeed linked to the identification of computers on the WWW. As we saw in study unit 2, the WWW is a massive network of computers and servers. Each computer is identified by means of a numeric ''Internet Protocol Address'' (''IP address''). An IP address contains the following:

IP address
URL

- Four groups of three digits.
- Each digit can have a value from 0 to 255.
- The protocol which administers this addressing system is the ''TCP/IP'' (Transmission Control Protocol/Internet Protocol).
- The full statement ''http://www . . . '' is the URL (''Universal Resource Locator'') — the string of characters which identifies the communication protocol used (http) and the IP address of the server site.

6.3 HOW IS A DOMAIN NAME ALLOCATED?

6.3.1 Top-level domains and second-level domains

Like a telephone number, a domain name is a unique **identifier** that points to a certain site on the World Wide Web. Each computer on the Internet has a unique numeric Internet Protocol address, such as ''148.317.2.08''. These numbers are not user-friendly and give no indication of what this address contains, or rather of what type of website this is.

unique number

A domain name is a **mnemonic** that is easy to remember, but it also indicates what the website contains. It is easier to remember ''new-cars.co.za'' than ''431.401.773''. Typically, domain names operate like telephone dialling codes in reverse. The first portion of the name points to a specific site, the second points to the broad category the site falls in and the third portion is the code of the country in which the site is registered. A telephone dialling code would work in the reverse. For

instance, (2712) 429 8334: 27 is the country code (South Africa), 12 is the city code (Pretoria) and 429 8334 is the telephone number of one of your lecturers for this course.

To return to domain names: ''**unisa.ac.za**'' refers to the University of South Africa's website. This site is registered in the academic (ac) domain in South Africa (za). The country code is called the ''top-level domain'' (za) (TLD), and the ''ac'' refers to ''academic'', the second-level domain (SLD). The SLDs are unique and identify the owner of the website. The URL would be as follows: *http://www.unisa.ac.za*.

TLD
SLD

ACTIVITY 6.1

Write down the meaning of the following second-level domains in South Africa:

- .gov.za: .....
- .edu.za: .....
- .ac.za: .....
- .co.za: .....
- .ngo.za: .....
- .mil.za: .....
- .law.za: .....
- .web.za: .....
- .tm.za: .....
- .net.za: .....
- .school.za: .....
- .nom.za: .....
- .org.za: .....

FEEDBACK

You will find a description of these second-level domains at <www.whois.co.za>. It is interesting to note that although the second-level domain ''edu.za'' is administered for distance-learning organisations, the University of South Africa uses the second-level domain ''.ac.za'' for academic institutions.

6.3.2 gTLDs

Website owners often use one of several globally available ''generic TLDs'' (or ''gTLDs'').

Akhtar & Cumbow (*Intell Prop & Tech F* 110501) note the following regarding gTLDs:

gTLDs

These extensions are short forms for the field of activity in which the particular TLD was originally intended to be used — ''.com'' (commercial), ''.net'' (Internet services), ''.org'' (nonprofit organisations), ''.edu'' (institutions of higher learning), and ''.gov'' (governmental agencies). In practice, registration of domain names in the ''.com,'' ''.net'' and ''.org'' TLDs has not been restricted to users in the appropriate fields. Thus, numerous commercial entities own ''.org'' domain names, many nonprofit organisations use ''.com'' domain names, and relatively few of the registrants of ''.net'' domain names are actually Internet service providers.

The other portion of the domain name is the second-level domain name (''SLD''), consisting of the string of words that precedes the TLD.

ACTIVITY 6.2

Sina and Tim ask you to explain technical terms such as ''top-level domain names'' and ''second-level domain names''.

FEEDBACK

You should simply explain to them that the top-level domain names refer to the country code — for example, ''.uk'' refers to the United Kingdom, and ''.co.za'' or ''.com.uk'' refers to the second-level domain name — commercial establishments in South Africa and the United Kingdom respectively.

6.4 WHY REGISTER A DOMAIN NAME?

Whydomain.com at <*http://www.domainregister.com/*> mentions the following advantages of registering a domain name:

advantages of domain names

- Increases your name recognition
- Makes it easy for your customers to remember your address
- Indicates you are a serious Internet player
- Helps brand your image
- Adds a level of trust and integrity to your site
- Many search engines refuse to list pages from free sites
- Some search engines will only index the first page of a domain site
- Domain names containing ''keywords'' aid in higher search engine ranking
- Allows you to use your domain address (www.yourname.com) and virtual email addresses (yourname@yourname.com) on your business cards and letterhead

- Once a domain name has been registered, it is no longer available. The most popular and easily-remembered domain names are being reserved daily, at the rate of one domain name every 5 seconds!

  At that rate, in the near future, only obscure domain names will be available to the general public!

- Avoids somebody else from registering the name you want.
- Lets you change your current e-mail provider and still keep the same e-mail address
- Protects your Internet advertising investment from failure of your Internet Service Provider (see Whydomain.com at <http://www.domainregister.com/>)

6.5 HOW TO SELECT A DOMAIN NAME

selection of domain name

- Make it as short as possible.
- Make it memorable.
- Make it easy to spell.
- Make it pronounceable.
- Make it directly related to your business's name, or
  - — make it directly related to key words from your industry, or
  - — make it descriptive of your site's content. (See Whydomain.com at <http://www.domainregister.com/>.)

domain names v trade marks

Conflicting domain names and trade marks may be in use. We shall deal with this issue later. However, it is interesting to note that many characteristics of a domain name will render it unregistrable as a trade mark: for example, descriptive terms are generally not registrable as trade marks, as they are not deemed to be capable of distinguishing the proprietor's goods and services from that of others. The ''use of key words from the industry'' may also not be registrable as trade marks, as these marks are reasonably required for use in the trade — for example, ''creamy'' for dairy products.

These bars to registration do not apply to domain names. As long as the domain name meets certain requirements, it is registrable as a domain name on a ''first-come-first-serve'' basis.

ACTIVITY 6.3

TSV wishes to register the following as domain names: ''TSV-Art.metallinks'', ''TSV-Ewrite'' and ''TSV-auto''.

FEEDBACK

You should advise TSV that, provided that these names are still available, the following domain names could be registered:

- ‘‘‘TSV-Art.metallinks.co.za’’
- ‘‘TSV-Ewrite.co.za’’
- ‘‘TSV-auto.co.za’’

However, should TSV wish to use its website as a training institution, it could also consider the following domain name:

- ‘‘TSV-Art.metallinks.edu.za’’

TSV could also use gTLDs as domain names, such as:

- ‘‘TSV-Art.metallinks.edu’’
- ‘‘TSV-auto.com’’

ACTIVITY 6.4

TSV wishes to follow your advice and register the following as domain names: ‘‘TSV-Art.metallinks.co.za’’, ‘‘TSV-Ewrite.com’’ and ‘‘TSV-auto.co.za’’. Advise your clients on how to obtain their own domain names.

FEEDBACK

SLDs are assigned on a first-come-first-served basis, and, more importantly, only one person or company can have a particular SLD combined with a particular TLD. TSV must thus conduct domain-registration searches in the ‘‘whois’’ databases of the registries it wishes to register the domain names in. TSV must then instruct the relevant registrars to register the domain names. The registrars will ensure that the technical requirements for the domain name registrations are met, such as the delegation of name servers for the domain names.

6.6 THE IMPACT OF DOMAIN NAMES ON TRADE-MARK RIGHTS

The registration and/or the use of a domain name may infringe on trade-mark rights. Study the prescribed extract from Pistorius ‘‘Domain Names and Infringement of Trade Marks on the Internet’’ in *Information and Communications Technology Law* (ed. Dana van der Merwe) (2009) at 205-222.

6.7 MANAGEMENT OF THE .za DOMAIN NAME SYSTEM AND ALTERNATIVE DISPUTE RESOLUTION IN SOUTH AFRICA

South Africa recently implemented the management of the .za domain name system as provided for in the ECT Act. This aspect is explained in Pistorius ''.za Alternative Dispute Resolution Regulations: The First Few SAIIPL Decisions', 2008(2) *Journal of Information, Law & Technology (JILT)*, <*http://go.warwick.ac.uk/jilt/2008_2/pistorius1*> 2-20. Study the following excerpt from the article:

1 South African Domain Name Administration & Zadna

South Africa's domain name system has grown very informally since the Internet made its first appearance in the country in 1980s when the .za domain-name space was administered by UNINET (Vecciatto, 2007). The idea that an independent Domain Name Authority be established for South Africa was first raised in a discussion paper in 1999. The next year this was formally raised as a governmental policy in the Green Paper (2000) of the Department of Communications <*http://www.ecomm-debate.co.za*>. The proposal was met with disbelief and it was vehemently opposed by the Namespace ZA (2002), the industry stakeholder. The South African government remained convinced that its involvement in the .za DNS was crucial for the emerging information economy. The government believed that the policy-formulation process in the ICT arena should be inclusive of all stakeholders. The view was also expressed that the new economy, like all other free-market economies, is not perfect and therefore requires the government's intervention, particularly in the formulation of policy, to extend services to both public institutions and citizens who wish to access such services (Green Paper, 2000).

The South African Government enacted its policy with the establishment of the .za Domain Name Authority (Zadna) as a section-21 company in the Electronic Communications and Transactions Act, 2002 (s. 59). The objects, powers, and matters incidental to the incorporation of the company are provided for in sections 59-67 of the ECT Act. The Minister is empowered to establish a national policy concerning the .za DNS (s. 68). The Authority is responsible for administering and managing the .za domain name space in compliance with international best practices and to licence and regulate registries and registrars. The Authority must also publish guidelines on the general administration and management of the .za domain name space and facilitate and maintain public access to a repository (s. 65; Marx, 2004, pp 125-127).

On 18 May 2007 Zadna assumed responsibility for the administration and management of the .za domain-name space

<http://www.zadna.org.za>. Since its inception the Zadna has focused its efforts on developing suitable policies and procedures for improved management of the .za domain space (Vecchiatto, 2007). On 30 July 2007 the Zadna's policies and procedures were published *www.zadna.org.za/policy/za.policy.and.procedures.20070802-GM.pdf>*. In terms of these policies a single registry model must be adopted and role-players will be invited to apply for licences as registry operators and registrars.

At present, several organisations administer the various .za second level domains. For instance, .co.za is administered by UniForum and .org.za by Internet Solutions. The .mil.za, and .gov.za SLDs are respectively administered by the South African National Defence Force, the State IT Agency. Other SLDs are administered by private individuals. A major concern is the SLD administrators' infrastructure to support public domain names. When the licensing regime is introduced the DNA will administer these domains. However, the Zadna has yet to promulgate licensing regulations with clear technical requirements (Du Toit, 2007).

2. .za Domain Name ADR Procedure

South Africa's Alternative Dispute Resolution (ADR) Regulations *<http://www.domaindisputes.co.za/downloads/AlternativeDisputeResolutionRegulations.pdf>* were promulgated in November 2006 in terms of section 69 read with section 94 of the ECT Act. Domain name ADR procedures are necessary due to the fact that a lack of harmonisation between the Domain Name System and trade mark law has allowed a number of illegal practices to emerge, including the deliberate, bad-faith registration of well-known trade marks as domain names, a practice known as ''cyber squatting'' (*British Telecommunications Plc v One in a Million Ltd* (1998) FSR 265; see generally Singleton, 2003, pp14-30; Ramappa, 2003, pp7-33). As will be seen below, the South African Alternative Dispute Resolution (ADR) Regulations enable the accredited providers to effectively deal with cyber squatting *<http://www.domaindisputes.co.za/downloads/AlternativeDisputeResolutionRegulations.pdf>*. One of the very first adjudications dealt with the bad-faith registration of the well-known name of the South African telecommunications provider (*ZA2007-0003 Telkom SA Ltd v Cool Ideas CC <http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0003.pdf>*). A dispute may also arise where the registrant registers a domain name incorporating a well-known mark without the proprietor's permission for purposes of expressing criticism or appreciation (''gripe'' or ''fan'' sites) (refer to the ''Citroën decision for the legitimacy of a ''fan site'' below).

Apart from blatant cyber squatting or cyber griping, genuine disputes may also arise (Smith, 2002, p76). The first of such genuine disputes is where the same mark is used by different persons in respect of different goods and services. For example, where two companies have independent, legitimate rights to a name, such as an American company that sold tennis racquets under the name ''Prince'', and an English company that sold software under the name ''Prince'' (*Prince v Prince Sports Group* 1998 FSR 2; Halberstam et al., 2002, p103; *World Wide Fund for Nature v World Wrestling Federation Entertainment Inc*, Court of Appeal 27 February 2002, *Times Law Report* 12 March 2002; Murray, 1998, p 285). The second type of ''genuine dispute'' is where the use of a ''split mark'' is in dispute. Here the same mark is owned and used by different persons for different territories in relation to the same goods or services (Smith, 2002, p 176). As will be seen below, and ''genuine disputes'' have been dealt with by the .za ADR provider.

The South African ADR Regulations were largely based on ICANN's Uniform Dispute Resolution Policy (UDRP) <*http://www.icann.org/udrp/udrp-policy-24oct99.htm*> and the United Kingdom's domain name procedures <*http://www.nominet.org.uk/disputes/drs/decisions*>. The Regulations are intended to resolve disputes over .za domain names registered under the .co.za sub-domain. This sub-domain primarily registers domain names of commercial (profit-making) entities. Previously, the only possible action which could be taken against the unauthorised registration of a co.za domain name was to institute court proceedings for trade mark infringement in South Africa (Greenberg, 2004, p 45). The .za ADR, like the UDRP, is an efficient alternative to court litigation (see generally, Motion, 2005, p 148; Christie, 2000; Donahey, 1999; Wilbers, 1999, p 273; Ryan, 2001, pp 27-30; Hurter, 2000, pp 199-208; Pistorius, 2008, p 237).

The Regulations stipulate the administrative process which should be followed in lodging a co.za dispute. First, an ADR provider accredited by the Authority to resolve co.za domain name disputes must be selected. A party wishing to declare a co.za domain name dispute can do so by using one of the accredited ADR providers. Currently, South Africa has two accredited ADR providers, AFSA <*http://www.domaindisputes.co.za*> and SAIIPL *http://www.domaindisputes.co.za*>.

A registrant must submit to proceedings under the rules if a complainant asserts, in accordance with the procedure, that the complainant has rights in respect of a name or mark which is identical or similar to the domain name and, in the hands of the registrant the domain name is an abusive registration (reg. 3(1)).

An ''abusive registration'' is defined as a domain name which

either took unfair advantage of or was unfairly detrimental to the complainant's rights at the time when the domain name was registered; or a domain name which has been used in a manner that takes unfair advantage of, or is unfairly detrimental to the complainant's rights (reg. 1). Under paragraph 4(a) (iii) of the UDRP Policy <*http://www.icann.org/en/udrp/udrp-policy-24oct99.htm*> a domain name holder must both register and use a domain name in bad faith in order for the conduct to amount to an abusive registration. The .za ADR Regulations, like the Australian .auDRP <*http://www.auda.org.au/policies/auda-2008-01/*> requires either bad faith registration or subsequent bad faith use of the domain name. Bradfield (2001, p 234) argues that this proscribes ''passive warehousing'' of domain names simply to prevent companies or third parties from registering such domain names. The practical effect of the difference is minimal as panels have nevertheless interpreted the ''*and*'' to mean ''*or*'' (Bradfield, 2002, p 234).

Regulation 1 provides that an ''offensive registration'' means a domain name in which the complainant cannot necessarily establish rights but the registration of which is contrary to law, *contra bones mores* or is likely to give offence to any class of persons. This means that the applicant can base its dispute on the grounds that the registered domain name is offensive on the grounds of religion, ethnicity, race, gender or incitement to cause harm. The introduction of the concept of an offensive registration is unprecedented.

''Rights'' and ''registered rights'' are not a closed list of rights but include intellectual property rights, commercial, cultural, linguistic, religious and personal rights protected under South African law (reg. 1). This broad approach is advantageous and it follows that business names will also fall within the list of ''rights'' (Bradfield, 2001, p 234).

Factors, which may indicate that the domain name is an abusive registration is listed in regulation 4(1) (a) and includes circumstances indicating that the registrant has registered or otherwise acquired the domain name primarily to -

(i) sell, rent or otherwise transfer the domain name for valuable consideration in excess of the registrant's reasonable out-of-pocket expenses directly associated with acquiring or using the domain name;
(ii) block intentionally the registration of a name or mark in which the complainant has rights;
(iii) disrupt unfairly the business of the complainant; or
(iv) prevent the complainant from exercising his, her or its rights.

A registration may also be deemed to be abusive where circumstances indicate that the registrant is using, or has registered, the domain name in a way that leads people or businesses to believe that the domain name is registered to, operated or authorised by, or otherwise connected with the complainant (reg. 4(1) (b)). The corresponding UDRP Policy paragraph 4(b) (iv) is much narrower as it is restricted to intentional attempts to attract, for commercial gain, Internet users to the registrant's web site or other on-line location.

Evidence, in combination with other circumstances indicating that the domain name in dispute is an abusive registration, that the registrant is engaged in a pattern of making abusive registrations will also point to an abusive registration (reg. 4(1)(c)), whereas the corresponding paragraph in the UDRP Policy provides that the complainant must show that the registrant has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that he has engaged in a pattern of such conduct. Other factors include the provision of false or incomplete contact details provided in the ''whois'' database, or a relationship between the complainant and the registrant, where the complainant has (i) been using the domain name registration exclusively; and (ii) paid for the registration or renewal of the domain name registration (reg. 4(1)(d)-(e)). Note that this is not a ''closed list'' of factors, similarly to the approach adopted in the UDRP and the .auDRP (Bradfield, 2001, p 234).

As noted above, an offensive registration may be indicated if the domain name advocates hatred that is based on race, ethnicity, gender or religion and/or that constitutes incitement to cause harm (reg. 4(2)). This ground for the cancellation of a domain name is of South African origin. A rebuttable presumption of abusive registration arises if the complainant proves that the registrant has been found to have made an abusive registration in three or more disputes in the 12 months before the dispute was filed (reg. 4(4)).

Regulation 5 sets out factors, which may indicate that the domain name is not an abusive registration. Where the domain name is identical to the mark in which the complainant asserts rights, the burden of proof shifts to the registrant to show that the domain name is not an abusive registration (reg. 5(d)). The relevant circumstances or factors must have existed before the registrant was aware of the complainant's cause for complaint. For example, the registrant must be able to show that she has used or made demonstrable preparations to use the domain name in connection with a good faith offering of goods or services. The domain name will also not be an abusive registration if the registrant can show she was commonly

known by the name or legitimately connected with a mark which is identical or similar to the domain name. Lastly, the domain name will not be an abusive registration if the registrant can show that she has made legitimate non-commercial or fair use of the domain name (reg. 5(a)). Fair use of a domain name that is being used generically or in a descriptive manner will also defeat a claim of abusive registration (reg. 5(b)).

Regulation 27 provides that the adjudicator must decide the Dispute on the documents placed before her. Adjudicators' decisions are guided by national, foreign and international laws (reg. 13(2)). Regulation 13(1) provides that an adjudicator must consider and must be guided by previous decisions of other adjudicators (national decisions) and decisions by foreign dispute resolution providers (foreign decisions). An adjudicator must provide in his or her decision the full reference to national and foreign decisions as well as national, foreign and international law that he or she considered (reg. 13(3)).

Foreign decisions are routinely followed in the .za ADR proceedings. The WIPO Arbitration and Mediation Centre is internationally recognised as the leading dispute-resolution service provider in these areas (Greenberg, 2004, p.43). The WIPO decisions are based on the UDRP <*http://www.wipo.int/amc/en/domains/search/index.html*> and they are followed closely in most .za ADR adjudications. Other foreign decisions that are followed emanates from the National Arbitration Forum (NAF) decisions based on the UDRP <*http://domains.adrforum.com/decision.aspx*>, the Nominet UK (.uk) decisions based on the .UK DRS <*http://www.nominet.org.uk/disputes/drs/decisions*>, and the decisions form New Zealand <*http://dnc.org.nz/drs/index.php?clsid=1013*>.

Regulation 9 sets out the possible decisions pursuant to a dispute before an adjudicator. In the case of a complaint regarding an abusive registration the adjudicator can refuse the dispute or the transfer of the disputed domain name to the complainant. In the case of a complaint relating to an offensive registration the adjudicator can refuse the Dispute or order the deletion of the domain name and prohibit future registration of such a domain name. The last possible decision is the adjudicator's refusal of the dispute as the dispute constitutes reverse domain name hijacking.

3. Brief overview of the first SAIIPL decisions

Although two providers have been accredited, only the SAIIPL has to date rendered decisions on domain name disputes under the ADR Regulations. The SAIIPL ADR decisions are published on-line at <*http://www.domaindisputes.co.za/content.php?tag=6*>. To date twenty three decisions have been published

and one decision is currently pending. The 80% success rate of .za complainants mirrors the success rate of the WIPO panels. Accusations of impartiality and pro-trade-mark tendencies have been raised against the WIPO panels (Bradfield, 2001, p 237). Sharrock (2001, p 838) notes that accusations that UDRP panellists are biased have been, at a minimum, significantly exaggerated. The fact remains that the SAIIPL panels' high success rate may give raise to similar unfounded perceptions.

Several factors complicate the matter for panellists who have a limited time within which to come to a decision. These factors include the lack of national precedents and limited experience on the part of adjudicators. A few inconsistent decisions have been rendered by the SAIIPL panel of adjudicators, notwithstanding their high level of competency and adequate training. These inconsistencies resulted mostly due to interpretational differences. A higher level of consistency will develop as more disputes are adjudicated. The level of consistency of adjudications will also be enhanced once a searchable database of national decisions becomes available.

3.1 Rights of the complainant

Regulation 3(1)(a) requires the complainant to prove, on a balance of probabilities, that she has rights in respect of a name or mark which is identical or similar to the domain name and that the domain name is an abusive registration. In *ZA2008-00016 Aqua Divers International (Pty) Ltd v Divetek (Pty) Ltd* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00016.pdf*> the adjudicator held that the phraseology ''rights in respect of'' is conceptually broader than ''rights to a mark (ZA2008-00016, p 11). In this case the adjudicator held that the complainant can claim commercial rights in respect of MARES and DACOR, pursuant to a distribution agreement (ZA2008-00016, p 12).

The .za adjudications have refined the principles applicable to complainants' rights to unregistered trade marks and the scope of trade-mark rights in the disclaimed features of a device mark. The most contentious issue is the time when a complainant's rights must be established.

3.1.1 Common-law marks

The complainants' rights to unregistered trade marks arose in the first complaint under adjudication, ZA2007-0001 (*Mr. Plastic Mining and Promotional Goods v Mr Plastic CC*) <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0001.pdf*>. In this case the complainant averred that the registration and use of the disputed domain name infringed the common-law rights he held in the unregistered trade mark

''MR PLASTIC''. The adjudicator held that a claim of passing-off by the complainant, if sustained, would render the domain name in dispute and its use by the registrant an abusive registration (ZA2007-0001, p 11). The complaint was dismissed as both the complainant and the registrant used the disputed name and they both had acquired concurrent rights to the name (Viljoen, 2007).

In ZA2007-0009 (*Holistic Remedies (Pty) Ltd & Amka Pharmaceuticals (Pty) Ltd v Oxygen for Life (Pty) Ltd*) <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0009.pdf*> the adjudicator qualified this principle. In this case it was held that the case of ZA2007-0001 should not be interpreted that it established a burden of proof that a complainant would be successful in a passing-off case. The complainant is required to illustrate, on a balance of probabilities, that it has a goodwill and reputation protectable by way of passing off action (ZA2007-0009, pp 13-14). It is submitted that the approach in ZA2007-0009 is correct, as it is only necessary to establish a "right" in a name for the purposes of the domain name ADR. It would thus suffice if the first requirement for a passing off action, namely goodwill and reputation in the name, is established.

The adjudicator in ZA2007-0001 noted that it is trite that the more descriptive a name or mark is the less it is inherently adapted to distinguish the goods or services of a particular trader from those of another (ZA2007-0001, p 14; see also *Reddaway v Banham* (1886) RPC 218, 224). A name or mark, which is inherently lacking in distinctiveness, can acquire distinctiveness through extensive use. Mere use and a reputation does not equate with distinctiveness (*Bergkelder Bpk v Shoprite Checkers (Pty) Ltd* 2006 (4) SA 275 (SCA)). It must be shown that the consequence of the use and reputation has brought about a situation where the name or mark has acquired a ''secondary meaning'' which in fact denotes one trader, and no other. Relevant evidence of such ''secondary meaning'' may include evidence related to length and amount of sales under the mark. The nature and extent of advertising, consumer surveys and media recognition is also relevant (D2000-0575 *Uitgeverij Crux V W Frederic Isler Skattedirektoratet v Eivind Nag*; D2000-1314 *Amsec Enterprises, LC v Sharon McCall*; D2001-0083 *Australian Trade Commission v Matthew Reader*; D2004-0322 *Transfer Imperial College v Christophe Dessimoz*).

In ZA2007-0008 (*Homefront Trading 272 CC v Ward*) <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0008.pdf*> the complainant was the registrant of the domain name private-sale.co.za and the disputed domain name was privatesale.co.za. The adjudicator held that the complainant had not established a protectable right in the descriptive words

''private-sale'' and the dispute was refused (ZA2007-0008, p 18). In reaching this conclusion, the adjudicator considered various Nominet and WIPO decisions. He noted that caution should be exercised in doing so because, in the United Kingdom, ''rights'' are more narrowly defined and specifically exclude a name or term which is wholly descriptive of the complainant's business, whereas the UDRP requires the complainant to establish a ''legitimate interest'' in a domain name (ZA2007-0008, p 15). The adjudicator noted that despite these differences, the general approach adopted by WIPO and the Nominet panels has been that, where domain names are wholly descriptive, rights or a legitimate interest can only be established where sufficient use has been made of the name to have given rise to the acquisition of a ''secondary meaning'' (ZA2007-0008, p 16).

The adjudicator noted that the complainant's ownership of the domain name private-sale.co.za is part of his commercial or personal rights, which obviously include the right to trade freely without unlawful interference or competition from anyone. The adjudicator noted again that whilst the conduct of the registrant in seeking to divert custom from the complainant to himself certainly raises a critical eyebrow, his conduct is neither *contra bonos mores* in a passing off sense, nor is it of such an unfair or dishonest nature that it is *contra bonos mores* in any other way (ZA2007-0008, p 17). The adjudicator stated that granting monopolies in simple descriptive terms adopted as domain names and in the absence of compelling evidence of ''secondary meaning'' would play havoc with the reasonable requirements and rights of traders and others to use such names themselves (ZA2007-0008, p 18).

3.1.2 Scope of registered rights

In ZA2007-0005 (*Telkom SA Ltd & TDS Directory Operations (Pty) Ltd v The Internet Corporation*) First complainant's registered rights in respect of the device mark THE PHONE BOOK was at issue.

The complainant's registered trade mark numbers 1996\06591 1996\06592 and 1996\06593 for THE PHONE BOOK logo in classes 16, 35 and 38 respectively.

The adjudicator noted two features of the complainant's trade mark registrations that were deemed important in deciding whether the complainant had rights in a mark, which is identical or confusingly similar to the disputed domain name. First, the fact that the trade mark

consists of a logo or a device, and secondly, the fact that it contains a disclaimer (ZA2007-0005, p 14).

The adjudicator held that the legal significance of the fact that the trade mark registrations consist of a device mark was highlighted in a Nominet decision, DRS NO. 01399 (*Loans.Co.Uk Ltd v Abbeyway Contracts Limited* par. 7.8) as follows:

> ''A registered trade mark for a word and device mark rather than the word alone may only be of limited value in a domain name dispute, which necessarily relates only to words in which Rights might have been acquired.''

In ZA2007-0005 the adjudicator held that the position is complicated further where the trade mark in question consists of descriptive words combined with a logo (ZA2007-0005, p 15). The complainant's trade mark rights not only comprises of descriptive words ''phone'' ''book'' and ''foonboek'' written in a stylised form and combined with a logo, but the registration has also been endorsed with a disclaimer. The following disclaimer is entered against the registration:

> ''Registration of this mark shall give no right to the exclusive use of the word PHONE, or of the word FOONBOEK, or of the word BOOK, each separately and apart from the mark...''.

The legal effect of this disclaimer was at issue. The adjudicator rejected the complainants' argument in their Reply that the effect of the disclaimer is merely to limit the complainants' rights in respect of the word PHONE on its own and the word BOOK on its own but not in respect of the combination of the two words ''PHONEBOOK'' or ''PHONE BOOK'' (ZA2007-0005, p 15). The adjudicator disagreed and held that the crux of the matter is that the complainants enjoy no registered protection for the words separate and apart from the mark. Furthermore, the use of a disclaimed feature or disclaimed features of a trade mark cannot amount to trade mark infringement (ZA2007-0005, p 15-16; Webster & Page par 9.19; par 12.8.9). The adjudicator held that the registered trade mark is neither identical nor similar to the domain name phonebook.co.za.

The decision of ZA2007-0005 was the first (and the only decision) to be appealed. Several aspects of the ZA2007-0005 decision were appealed, inter alia also the initial adjudicator's ruling that the registered trade mark is neither identical nor similar to the name phonebook.co.za. The Appeals Panel in ZAAP2007-0005 (*Telkom SA Ltd & TDS Directory Operations (Pty) Ltd v The Internet Corporation*) <*http://www.domaindisputes.co.za/downloads/decisions/ZAAP2007-0005.pdf*> held that the effect of the disclaimer in the registered trade mark is to deprive the First complainant of rights in the word

FOONBOEK, or the version which has the "equivalent meaning", the English expression ''PHONE BOOK''. The Appeals Panel held that as use of a disclaimed feature cannot amount to infringement of registered rights it follows that the complainants do not have rights that can be infringed in the registrant's use of the domain name (ZAAP2007-0005, p.10).

In summing up its reasoning on this point the Appeals Panel noted that trade marks do not give monopolies in ideas, but serve to distinguish products of a similar nature. The Appeals Panel concluded that the complainants do not have the necessary rights to proceed with a complaint as required by the Regulations (ZAAP2007-0005, p 13).

3.1.3 The Relevant Time of Establishment of Rights

In ZA2008-00020 *Mxit Lifestyle (Pty) Ltd v Andre Steyn* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00020.pdf*> the adjudicator noted that she agrees with findings of the panels under the Nominet and UDRP policies, namely that the date on which rights must exist is the date of the Complaint and not the registration date of the disputed domain name (p 14). She held that the issue of the registrant's registration of the disputed domain name prior to the establishment of the complainant's rights is only relevant to questions concerning the registrant's legitimate interest and bad faith (ZA2008-00020, p 14; DRS/03078, D2000-0270 and D2002-0669). Similarly, in ZA2007-0008 *Homefront Trading 272 CC v Ian Ward* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0008.pdf*> the adjudicator held that the fact that the registrant's registration of the disputed domain name pre-dated the complainant's registration was irrelevant (ZA2007-0008, p 17).

This issue was discussed in the WIPO Arbitration and Mediation Centre's *Overview of WIPO Panel Views* under the third UDRP element. The question is whether bad faith can be found where the disputed domain name was registered before the trade mark or other rights of the complainant were acquired. The panels' consensus view is that where a domain name was registered before a trademark right was established, the registration of the domain name was not in bad faith because the registrant could not have contemplated the complainant's non-existent right (WIPO Overview, p 8). It is noted that in exceptional circumstances, for example where the respondent is clearly aware of the complainant, and the aim of the registration was to take advantage of the confusion between the domain name and any potential complainant rights, bad faith can be found.

According to Buys, the legal representative of the complainant, the ZA2008-00020 decision sets important precedents:

> ''...Firstly, it was decided that a complainant only have to show rights in a name that is similar to the disputed domain name on the date of the dispute and not on the date upon which the domain name was registered...'' (Anon, 2008, *http://mybroadband.co.za/news/Internet/5548.html*>).

This sweeping statement should be qualified with reference to the definition of an abusive registration. Regulation 3(1) requires the registrant to assert that she has rights in respect of a name or a mark which is identical to the domain name and, in the hands of the registrant the domain name is an abusive registration. However, the enquiry does not end there as the complainant must also prove that the domain name is an abusive registration. Under paragraph 4(a) (iii) of the UDRP Policy a domain name holder must both register and use a domain name in bad faith in order for the conduct to amount to an abusive registration. Regulation 1 of the .za ADR Regulations requires a complainant to prove that the disputed domain name is an abusive registration, *either* as a result of a bad faith domain name registration *or* as a result of the bad faith use of the domain name.

The definition of an abusive registration in regulation 1 is specific on when the complainant's rights must exist. Part (a) of the definition of an abusive registration provides that it is a domain name which was registered or otherwise acquired in a manner which, *at the time when the registration or acquisition took place,* took unfair advantage of or was unfairly detrimental to the complainant's rights (Emphasis Supplied). The general rule is where the domain name was registered before the trade mark or other rights of the complainant were acquired the disputed domain name can only be an abusive registration if it has been used in a manner that takes unfair advantage of, or is unfairly detrimental to the complainants' rights in accordance with regulation 1(b) (ZA2008-00022 p 11; ZA2007-0009 pp 12 & 14). In ZA2008-00020 the complainant could not prove its rights at the date of registration of the domain name. The adjudicator correctly noted that even if the registrant was innocent in registering the disputed domain name mixit.co.za, his use of the domain name was not innocent (ZA2008-00022 p 16).

It follows that the registration or acquisition of a domain name before the rights of the complainant were acquired or established will not be an abusive registration in terms of regulation 1(a). In exceptional circumstances, a bad faith registration can take unfair advantage or be detrimental to the potential rights of the complainant. Foreign decisions referred to by the WIPO Overview that bad faith can be found where, for example, the respondent is clearly aware of the complainant,

and the aim of the registration was to take advantage of the confusion between the domain name and any potential complainant rights, could be persuasive (p 8).

3.2 Identical or Confusingly Similar

Where a registrant has merely added a descriptive/generic word to a distinctive trade mark the domain name will still be deemed to be confusingly similar to the trade mark (ZA2007-0003 *Telkom SA Ltd v Cool Ideas CC* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0003.pdf*>; the discussion of the similarity of the ''nike'' domain names in ZA2007-0003, p 13: In D2000-1598 the domain names ''niketravel.com'' and ''nikesportstravel.com'' were found to be similar to the trade mark NIKE; DRS04601 in which ''nikestore.com'' was held to be similar to ''NIKE''; and DRS01493 in which ''nokia-ringtones.com'' was found to be similar to ''NOKIA'').

In NAF/FA141825 it was held that:

> ''[It] is also well-established under the Policy that a domain name composed of a trademark coupled with a generic term still is confusingly similar to the trademark''.

In ZA2007-0010 (*Multichoice Subscriber Management Services (Pty) Ltd v JP Botha*) <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0010.pdf*> the well established legal principle that a domain name that comprises a trade mark coupled with a generic term is confusingly similar to the trade mark was confirmed (ZA2007-0010, p 6; also decisions ZA2007-0003 and ZA2007-0004 *Telkom SA Limited and TDS Directory Operations (Pty) Ltd v The Internet Corporation* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0004.pdf*>). In ZA2007-0010 the adjudicator held that ''mwebsearch.co.za'' is indeed confusingly similar to the trade mark MWEB, incorporating as it does, the whole of the distinctive mark MWEB in conjunction with the generic and non-distinctive term ''search'', which is in common use. (See also the adjudicators' decisions that the domain name suncityvacation. co.za is similar to the trade mark SUN CITY in ZA2008-00023 *Sun International South Africa Ltd. v Blue Chip Accommodation CC* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00023.pdf*> and that sunglasshut.co.za is identical to the trade mark SUN GLAS HUT in ZA2008-00015 *Luxottia US Holding Corporation v Preshal Iyar*).

''Typo squatting'' or ''domain mimicry'' takes place where domain names are registered with one letter or number altered (Bradfield, 2001, p 234). For instance, ''microsOft.com'' will be deemed confusingly similar to ''Microsoft Corporation'' (Loundy, 1997, p 465). Regulation 3(1) (a) requires the complainant to show that the domain name is identical or similar to the

complainant's mark. In the case of typo squatting the domain name will be similar to the mark and the right holder will thus have a course of action irrespective of whether the registrant engaged in cyber squatting or typo squatting.

ZA2007-0006 (*Standard Bank of South Africa Ltd v Cox* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0009.pdf*>) was a typical typo squatting case. The adjudicator held that the domain names standerdbank.co.za, standarbank.co.za, wwwstandardbank.co.za, standerdank.co.za, standardank.co.za, stanardbank.co.za, standardban.co.za, standadbank.co.za, standardbak.co.za, stndardbank.co.za, stadardbank.co.za, and sandardbank.co.za, were for all interests and purposes identical to the complainant's trade mark STANDARD BANK and amounts to typo squatting (ZA2007-0006, p 5). The domain names in issue resolved to websites that officered services directly overlapped with that of the complainant. This was regarded as evidence that the domain names were registered and used in bad faith (ZA2007-0006, p 6). The adjudicator held that the domain names were registered in bad faith and that the domain names were used in a manner that takes unfair advantage of, or is unfairly detrimental to the complainant's rights. The domain names were transferred to the complainant ((ZA2007-0006, pp 7-8).

3.3 Evidence of Abusive registration

The adjudicator must examine all the circumstances of the case to determine whether a registrant is acting in bad faith. Examples of circumstances that can indicate bad faith include where the complainant has rights in a well-known trade mark, where the registrant provided no response to the Complaint, where the registrant concealed his identity and where it is impossible to conceiving a good faith use of the domain name (D2000-0003 *Telstra Corporation Limited v. Nuclear Marshmallows*; D2000-0574 *Jupiters Limited v Aaron Hall*; D2002-0131 *Ladbroke Group Plc v Sonoma International LDC*).

One interesting aspect of the first .za decisions is the determination of ''unfair advantage'' or ''unfair detriment''. The other interesting aspect is the extent to which trade-mark law principles played a role in determining whether a registration is abusive or not. Trade mark law was applied to determine whether a domain name has been used in a manner that takes unfair advantage of, or is unfairly detrimental to the complainant's rights.

3.3.1 Unfair advantage or unfair detriment

In ZA2007-0007 *Federation Internationale de Football Association (Fifa) v X Yin* <*http://www.domaindisputes.co.za/*

downloads/decisions/ZA2007-0007.pdf> the domain name fifa.co.za was at issue. The adjudicator noted that regulation 4(1) (b) is not a paragon of drafting clarity (ZA2007-0007, p 16). Regulation 4(1) (b) provides:

A registration may also be deemed to be abusive where circumstances indicate that the registrant is using, or has registered, the domain name in a way that leads people or businesses to believe that the domain name is registered to, operated or authorised by, or otherwise connected with the complainant (reg. 4(1) (b)).

The adjudicator noted that the domain name in question is registered. It is difficult to perceive how the domain name can be registered ''in a way'' that leads to the stated effect (outside of the domain name). The adjudicator assumed that the intention of the regulation is to incorporate within the ambit of the circumstances there postulated the import of the name per se (ZA2007-0007, p 16). In the adjudicator's view, the domain name registration is likely to take advantage of, or be detrimental to the complainant's rights, particularly in light of the fact that FIFA is one of the funders of the 2010 WORLD CUP tournament in South Africa. The issue in this regard is not the extent to which the registration will prejudice such licensing and franchising efforts, but the potential for it to do so (ZA2007-0007, p 17).

On the question of whether the domain name registration has the requisite quality of ''unfairness'', the adjudicator held that the same considerations that the Constitutional Court applied in *Laugh It Off Promotions CC v SAB International (Finance) BV* (2006 (1) SA 144 CC) would not necessarily apply to domain names. The court held the following with reference to the alleged tarnishment of a trade mark:

> ''The section does not limit use that takes fair advantage of the mark or that does not threaten substantial harm to the repute of the mark, or indeed that may lead to harm but in a fair manner. What is fair will have to be assessed case by case with due regard to the factual matrix and other context of the case.'' (par. 49)

The adjudicator noted that given the infinite proportions of access to such a site, and the possibilities of its use (and abuse), a likelihood of substantial economic detriment cannot be the sole standard for assessing unfairness in the context of domain name disputes. In this regard, the adjudicator noted that evidence was put forward of an intention on the part of the registrant to continue to avail himself of the benefit and advantage of the use of the mark FIFA in a domain name. The adjudicator deemed this to be unfair (ZA2007-0007, p 19). The adjudicator concluded that although the website *http://www.*

fifa.co.za > would only have an insubstantial consequence for FIFA, the domain name fifa.co.za was an abusive registration (ZA2007-0007, p 19).

In ZA2008-00016 the adjudicator noted that two factors need to be considered in determining unfair advantage or unfair detriment. The adjudicator held that the advantage or detriment must be to the complainant's rights. In the particular case the promotion of the sale of genuine goods was not unfair or detrimental to the complainant's distribution rights (ZA2008-00016, p 16). Any advantage gained would be as a result of the reputation of the marks and not as a result of taking advantage of the complainant's rights (ibid). The complainant failed to make a case that the domain name constituted an abusive registration (ZA2008-00016, p 22).

3.3.2 Blocking registrations and disruption of business

The adjudicator in ZA2007-0003 (*Telkom SA Limited v Cool Ideas 1290 CC*) held that a blocking registration has two critical features. The first is that it must act against a name or mark in which the complainant has rights. The second feature relates to an intent or motivation in registering the domain name in order to prevent a complainant from doing so. (ZA2008-00021 *Sun International (IP) Ltd v Will Green* < *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00021.pdf* > pp 13-14; ZA2008-00015 *Luxottia U.S. Holding Corporation v Preshal Iyar* < *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00015.pdf* > p 11).

In ZA2008-00022 *Samsung Electronics Co. Ltd v Sean Elsworth* < *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00015.pdf* > the complainant established rights in the mark ''SAMSUNG'' which had been registered by the registrant as samsungcartridges.co.za and samsungcartridge.co.za. The adjudicator agreed with the complainant's contention that the registrant did not conceive the disputed domain names independently of the complainant's trade marks. The adjudicator thus concluded that the registrant was not acting in a bona fide manner when he registered the disputed domain names. The complainant did not make any substantive case that the registrant registered the domain names with the express intent of blocking the registrant from registering the domain names (ZA2008-00022, p 11). The adjudicator referred to various foreign decisions where it was held that the disruption of a business of a complainant may be inferred where the registrant has registered a variant of the complainant's marks (ZA2008-00022, p 12). The complainant thus discharged the onus of proving that the disputed domain names were abusive registrations.

3.4 Factors negating an abusive registration allegation

Regulation 5(a) (i) provides that the registrant may provide evidence of its use of, or demonstrable preparations to use, the disputed domain name in connection with a bona fide offering of goods or services before being aware of the complainant's cause of complaint. First, the phrase ''demonstrable preparations to use'' requires ''real preparations that are calculated to result in deployment of an operational website address addressed by that name'' (D2001-0932, *Sydney Markets Ltd v Shell Information Systems*; NAF 0095856, *Treeforms Inc v Cayne Industrial Sales Corp*). Secondly, the steps in preparation to use the domain name must be taken before becoming aware of the complainants' cause of complaint.

Passive use may amount to use in bad faith. Many foreign decisions have held that the ''use'' requirement includes both positive action and inaction (D2000-0059 *Barney's Inc v BNY Bulletin Board*; D2000-0400 *CBS Broadcasting Inc v Dennis Toeppen*; D2000-0487 *Video Networks Limited v Larry Joe King*; D2000–194 *Recordati SPA v Domain Name Clearing Company*; and D2000-0468 *Revlon Consumer Products Corporation v Yoram Yosef aka Joe Goldman*). It has been held that failure to make bona fide use of a domain name during a two-year period following registration constitutes bad faith (D2005-0472 *Hexagon v Xspect Solutions Inc*; D2000-0004 *Mondich & American Wine Biscuits Inc v Brown*). In ZA2008-00020 the adjudicator held that as the domain name ''mix-it.co.za'' resolved to an empty web site there was not use of demonstrable preparations to use the domain name before being aware of the complainant's cause of complaint (ZA2008-00020, p 17).

Regulation 5 provides that a domain name will also not be an abusive registration if the registrant can show she was commonly known by the name or legitimately connected with a mark which is identical or similar to the domain name. In ZA2008-00023 the registrant claimed that the domain name was not an abusive registration as she (the registrant) is the complainant's booking agent and she was therefore promoting the complainant's business by booking accommodation for its clients (ZA2008-00023, p 15). Furthermore, the website only promoted the complainant's business. The registrant's claim that the domain name suncityvacation.co.za only promotes the complainant's Sun City resort and is therefore not an abusive registration, was rejected by the adjudicator. The adjudicator noted that an abusive registration begins with the registration of the domain name and the content of a website does not have any bearing on the issue (ZA2008-00023, p 16). The adjudicator also noted that the complainant has no control over the contents of

the website and that the registrant could have traded under any other name (ibid).

The domain name will not be an abusive registration if the registrant can show that she has made legitimate non-commercial or fair use of the domain name (reg. 5(a)). Fair use of a domain name that is being used generically or in a descriptive manner will also defeat a claim of abusive registration (reg. 5(b)). Where a domain name is used to denote the services it is offering it cannot amount to generic or descriptive use of the domain name (ZA2008-00023 p 17). Use of a domain name also cannot be fair where such use is misleading or where it takes unfair advantage of the reputation and goodwill of a trade mark (ibid).

Landing pages or domain parking sites can be customised or automated. UDRP and Nominet panels have been faced with much adjudication wherein they had to decide whether such use constitutes fair use. Domain name parking sited or landing page were at issue in ZA2008-00020 *Mxit Lifestyle (Pty) Ltd v Andre Steyn* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00020.pdf*>. The adjudicator noted that a number of factors are relevant in analysing landing pages. These include whether the domain name is an obvious trade mark, whether the website's content is related to the dictionary meaning of the domain name (for example laptops being offered for sale at laptop.com), whether the landing page provides links or advertisements for competing products, whether the landing page appears to be a pretext for cyber squatting and whether the registrant registered and use the relevant domain name or other domain names in bad faith on other grounds (ZA2008-00020, p 18).

Olivier & Jearey (2008) note that it is not clear if and to what extent - the fact that the domain name is an obvious trade mark or whether the landing page provided links or advertisements for competing products were considered in making the finding that

> ''the registrant generates revenue from the sponsored links and advertisements that appear on the landing pages and as a consequence of the confusion with complainant's trade mark.''

They also noted that the initial conduct of the registrant in using the keywords ''chat'', ''messaging'' and ''Mxit'' had ceased. The parked domain name used ordinary terms that are unrelated to the complainant's rights for search engine optimization (such as fashion, clothing, and music). Olivier and Jearey speculate that one may conclude that the similarity of the trade mark and domain was primarily sufficient to convince the adjudicator that the domain name was an abusive registration (ibid). The

adjudicator noted that the circumstances set out in regulation 4(1) (b) continue to exist, notwithstanding the fact that the use of the keywords ceased (ZA2008-00020 p 16). The premise for the decision went beyond the similarity of the mark and the domain name. It was based on the fact that the domain name and the complaint's mark is so similar that people are likely to believe that the disputed domain name is connected with the complainant (ZA2008-00020 p 16).

3.5 Reverse Domain Name Hijacking

Reverse domain name hijacking is the use of the Regulations in bad faith in an attempt to deprive the registrant of her domain name (reg. 1). It is thus the unlawful attempt to obtain a domain name that has previously been registered by a lawful owner (Marx, 2004, p 117; Viljoen, 2007).

ZA2007-0005 was the first .za ADR case where reverse domain name hijacking was considered. In the face of the dearth of national decisions the adjudicator turned to foreign decisions for guidance. It was noted that foreign decisions have held that the registrant must show that complainants knew the registrant's legitimate interests in the disputed domain name or the clear lack of bad faith registration and use, and nevertheless brought the Complaint in bad faith (D2000-1224 *Sydney Opera House Trust v Trilynx Pty Ltd*; D2000-0993 *Smart Design LLC v Hughes*; *eResolution Case* AF-0170a–0170c *Loblaws Inc v Presidentchoice.inc/Presidentchoice.com*; eResolution, June 7, 2000).

Bad faith encompasses both malicious intent and recklessness or knowing disregard of the likelihood that the registrant possessed legitimate interests (D2000-0993, *Smart Design*, supra). In AF-0170a0170c (Loblaws, supra) it was held:

> ''in a case where the trademark, although a well-known supermarket brand, is a common English phrase used as a mark by other businesses, the failure to conduct a cursory investigation seems especially unreasonable''

Legitimate interest in the use of a domain name has two requirements. The first is that the registrant must use a generic word to describe his product or business. The second is that the generic use of the word must be without the intent to take advantage of a complainant's rights in that word.

In ZA2007-0005 the adjudicator concluded, on the balance of probabilities, that the registrant had a legitimate interest in the disputed domain name by virtue of having been the first to register the generic words ''white pages''. The disputed domain name whitepages.co.za is used in connection with a bona fide offering of goods or services. The mere fact that the white-

pages.co.za website was inactive for a relatively short period does not detract from this fact. The adjudicator held that as the complainants failed to prove their rights under regulation 3(1)(a), their allegation that the domain name was used in a manner that takes unfair advantage of, or was detrimental to their rights was also doomed.

The adjudicator held that the complainants had no proper objection to the disputed domain name. Since the complainants were being professionally advised throughout, the adjudicator came to the inescapable conclusion that the complainants were aware of the lack of proper grounds for the objection to the domain name (ZA2007-0005, p 23). The adjudicator stated that the Complaint was brought in bad faith primarily to deprive a registered domain-name holder of its domain name and that the Complaint constituted an abuse of the administrative proceedings (ZA2007-0005, p 24). ZA2007-0005 was the first case to be appealed.

In ZA2007-0008 *Homefront Trading 272 CC v Ian Ward* <*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0008.pdf*> an allegation of reverse domain name hijacking was once again made. The adjudicator decided this case before the Appeals Panel published its decisions. The adjudicator in ZA2007-0008 rejected the registrant's allegation, but based his findings on an unusual interpretation of the meaning of reverse domain name hijacking. The adjudicator held that the complainant's conduct involved the lawful and bona fide acquisition of a domain name (and associated business) and nothing in its conduct had been aimed at undermining the registrant's domain name privatesale.co.za, nor the business of the registrant (ZA2007-0008, p 18). The adjudicator also noted that at the time when the complainant obtained the domain name private-sale.co.za, the registrant was not conducting any business under the domain name private-sale.co.za. The adjudicator concluded that no ''reverse hijacking'' could have existed (ibid). The adjudicator thus interpreted the requirements not to refer to the complainant's bad faith in instituting the complaint under the ADR procedure, but to the complainant's conduct in registering and using the domain name.

The appellants in ZAAP2007-0005 *Telkom SA Ltd & TDS Directory Operations (Pty) Ltd v The Internet Corporation* <*http://www.domaindisputes.co.za/downloads/decisions/ZAAP2007-0005.pdf*> appealed against all the initial adjudicator's findings and especially against the finding of reverse domain name hijacking. The appeals panel noted that it had some difficulty in understanding the precise aim and scope of this concept (and hence the nature and scope of the onus that a party seeking to invoke it is required to discharge). It requires,

in the view of the Adjudication Panel, legislative intervention if it is to serve a meaningful purpose (ZAAP2007-0005 pp 16-17).

The appeals panel noted that the registrant made the allegation in its Response that the complainants were using the Regulations in bad faith but the adjudicator was not requested to make a ruling on reverse domain name hijacking. The panel noted that litigants and their legal advisers must be free to launch proceedings to protect rights -even if incorrectly perceived - without fear of castigation. A majority of members of the Adjudication Panel were of the view that a reverse domain name hijacking complaint should require suitable evidence of unlawful intent, for example as proven in *Bress Designs (Pty) Ltd v GY Lounge Suite Manufacturers (Pty) Ltd*, 1991 (2) SA 455 W (ZAAP2007-0005, p 17).

The Appeals Panel's ruling on reverse domain name hijacking is completely out of step with foreign decisions. Foreign decisions have developed four scenarios where sufficient grounds may exist for a finding of reverse domain name hijacking. The first ground is based on the registrant's ability to prove that the complainant does not have a right in the mark used in the disputed domain name; secondly where the registrant can prove the complainant initiated the dispute well aware of the registrant's rights or legitimate interests in the domain name; thirdly, where the registrant can prove that the complainant knew that the registrant did not act in bad faith and; fourthly, a lack of candour on the part of the complainant (Bazerman & Georget, 2003, pp 2-3).

In D2005-0309 (*Jazeera Space Channel TV Station v AJ Publishing aka Aljazeera Publishing*) it was noted that neither ''bad faith'' nor ''abuse'' is defined in the Rules but both concepts are known to most, if not all, legal systems. Generally, ''bad faith'' connotes a mental element such as malice or dishonesty. In D2004-0848 (*Kiwi European Holdings BV v Future Media Architects Inc*) a complete lack of evidence that the disputed domain name, a generic term, was registered or was being used for reasons related in any way to complainant or its mark, led to a finding of reverse domain name hijacking.

Bad faith encompasses both malicious intent and recklessness or knowing disregard of the likelihood that the registrant possessed legitimate interests (D2000-0993, *Smart Design*, supra). Reverse domain name hijacking has been upheld in circumstances where a reasonable investigation would have revealed the weaknesses in any potential complaint under the Policy (D2006-0645 *Rohl, LLC v ROHL SA*). Similarly, it has been held:

> ''in a case where the trademark, although a well-known supermarket brand, is a common English phrase used as a

> mark by other businesses, the failure to conduct a cursory investigation seems especially unreasonable'' (AF-0170a0170c, *Loblaws*, supra)

As for ''abuse of process'', using the Policy to harass the domain-name holder is an example that is provided by the Rules. In DRS 00538 (*Cardpoint plc v Riga Industries*) the adjudicator held that the complainant pursued the Complaint out of frustration at the Respondent's refusal to negotiate terms for a transfer of the domain name, rather than out of any genuine belief that the registration was an Abusive Registration under the Policy. There was no obligation upon the Respondent to negotiate terms for a transfer, and to invoke the Policy in such circumstances amounts to an abuse of process (DRS 00538, p 5).

Initiating domain name dispute resolution proceedings necessarily causes considerable expenditure of time and cost. A complainant must have a reasonable and credible belief that he is entitled to succeed, before commencing with a dispute. In particular, proceedings must not be misused in an unjustifiable attempt to pressure a domain name owner to transfer the domain name to a complainant (D2006-0905 *Proto Software, Inc. v Vertical Axis, Inc/PROTO.COM*; D2002-0535 *Sustainable Forestry Management Limited v SFM.com and James M. van Johns ''Infa dot Net'' Web Services*).

The proper function and purpose of reverse domain name hijacking must still find a foothold amongst the .za adjudicators. It is noted that reverse domain name hijacking should not be viewed as a foreign concept – Intellectual property laws have long provided relief for groundless claims (Munden, p 52). Its main purpose is to balance the rights of trade mark owners and that of domain name owners. Bad faith is not an argument that is available to the complainant only (Rodhain, 2002, p 4). In the end, bad faith may be attributed to registrants and trade mark proprietors alike.

4. Concluding remarks

The first few .za ADR cases have illustrated the SAIIPL service provider's ability to successfully implement and manage an ADR system for the benefit of both right holders and domain name owners. The decisions have built on and incorporated foreign decisions. The Appeals Panel's refusal to recognise established foreign decisions on reverse domain name hijacking is in stark contrast to this trend. Reverse domain name hijacking emphasises the differences between domain name ADR and traditional trade mark infringement actions. Not every case of trade mark infringement is actionable under the ADR rules. It has been noted that bringing the wrong case to the UDRP, and arguably

the .za ADR forum may lead to a finding of reverse domain name hijacking (Bazerman & Georget 2003, p 4).

Marx (2004, p 127) questioned the wisdom of the development of an indigenous ADR system for .za domain name disputes. It was noted that the adoption of the UDRP Policy and Rules and the use of WIPO panels and existing infrastructure may have been more cost effective. However, I am of the opinion that the adoption of the UDRP for the .za DNS would only have been cost-effective in the short term. The development of an indigenous .za ADR system was advantageous, as ADR Regulations drafters avoided some of the problematic features of the UDRP Policy. The drafters of the .za ADR Regulations had the benefit of hindsight as they benefitted from the experiences of other ADR providers, such as Nominet. Secondly, the ADR Regulations opened the basis of complaints to cultural, personal and commercial rights. The third advantageous home-grown feature is the adoption of complaints geared towards offensive registrations. The South African procedure is cost-effective compared to the UDRP costs.

6.8 CONCLUSION

The domain-naming system has vast advantages for the e-trader. A carefully selected domain name is an important element of successful trading on the Internet. However, the use of domain names which are substantially similar or identical to trade marks poses a challenge yet to be addressed by South African law.

STUDY UNIT 7

The implications of e-commerce on income tax

Annet Oguttu and Sebo Tladi

OVERVIEW

In this study unit we shall explore the implications of e-commerce on income tax. Some international initiatives that have been taken to implement new tax rules that govern income tax in cyberspace will be explored. Emphasis will be placed on the challenges posed by e-commerce on the jurisdiction to tax income (the residence and source based taxation), and the administration and enforcement of tax laws.

LEARNING OUTCOMES

After completion of this study unit, you should be able to do the following:

- explain the impact of e-commerce on income tax in both domestic and foreign law, and also the initiatives taken by governments and/or organisations with regard to this issue
- explain the impact of e-commerce on the concepts used to determine the residence status of individuals (ordinary residence and physical presence test) and persons other than individuals (for example, the place of effective management) in South Africa
- explain the impact of e-commerce on the source basis of taxation that is applied in respect of nonresidents
- explain the impact of e-commerce on the rules used to determine the source of different characters or types of income
- explain what constitutes a ''permanent establishment'' of an enterprise in a given jurisdiction, and whether an ISP, telecommunication facilities, website and web server can be considered a permanent establishment of an enterprise

SETTING THE SCENE

TVS Corporation is now an established business, with more than three web sites on the Internet. It offers a variety of goods and services to its customers worldwide (customers in this case refers to both individuals and businesses). Delivery of goods and services takes place on the Internet and payments for purchases are made electronically. TVS's offices are situated in South Africa. Their management board sits in the United Kingdom and decisions are often taken in the US.

7.1 INTRODUCTION

Prescribed reading: Oguttu and Van der Merwe ''Electronic Commerce: Challenging the Income Tax Base'' *SAMLJ* (2005) 17 n3 305-322

As e-commerce changes the way of doing business (from traditional ways to cyberspace), new electronic products and delivery systems result. Taxation is an aspect of law that is also affected by this move. This does not, however, mean that existing tax laws have to be repealed, but the present legislation governing taxation rules must adapt its application of existing tax principles, practices and procedures to an e-commerce environment. The South African Revenue Service (hereinafter referred to as SARS), which is responsible for the administering and enforcing of tax laws, is also affected by the challenges e-commerce poses to taxation. This led SARS to draft a *Discussion document on electronic commerce and taxation in South Africa* (2000) (hereinafter referred to as the SARS doc).

There is a legitimate concern by governments that the development of the Internet may have the effect of shrinking the tax base and hence reducing fiscal revenue. The reasons for these concerns are on the one hand the difficulties inherent in defining jurisdiction in cyberspace; and on the other hand, the problem of the administration and enforcement of tax laws. In addressing these problems, it is necessary to develop a taxation framework that ensures that taxation systems are fair, predictable and do not distort the conduct of business. Care should also be taken to ensure that no separate taxes are applied to e-commerce. The challenge for South Africa is therefore to develop a taxation policy that is not isolated from its e-commerce partners (Green Paper at 22). Some organisations and governments (for example, the OECD, EU, and countries such as Canada, USA and Australia) have issued reports or discussion documents on the tax aspects of e-commerce. Problems highlighted by these reports have been identified, but no proposed legislative changes have yet been made.

The areas most affected by the tax base erosion in the short term are those where products are easily digitised and easily available via electronic media, such as books, music, software and information. On the Internet, the sheer scale of online activities could make discovery of transactions very difficult. The collection of taxes that depends on the voluntary disclosure of the information by individuals and businesses to the tax authority is also challenged by e-commerce.

7.2 CHALLENGES POSED BY E-COMMERCE ON THE JURISDICTION TO TAX INCOME

source principle of taxation

A tax is a compulsory contribution, payable in money (or in kind) to a specific taxing authority, aimed primarily at funding public expenditure. Before any country can levy a tax on income, a connection or tax nexus must be established between itself and that income. The two main connecting factors (principles) underlying the taxation of income are the residence and the source principles of taxation. Under the source principle, persons (individuals and non-individuals like companies) are taxed on income that originates within the territorial jurisdiction or geographical confines of the country, regardless of the taxpayer's country of residence. Under the residence principle of taxation, residents are taxed on their worldwide income regardless of the fact that the income may have its source from another country. Most jurisdictions, including South Africa, have adopted a combination (hybrid system) of these two taxation principles.

E-commerce poses challenges to the above principles upon which countries' jurisdiction to tax income is based. This is because these principles are governed by national sovereignty, having been developed in the days of ''bricks and mortar'' when physical presence in a jurisdiction was necessary to enforce tax laws and where cross-border transactions involved mostly tangible products. South Africa uses the residence principle of taxation to tax South African residents, and the source principle of taxation to tax nonresidents.

7.2.1 Residence principle of taxation

Definition: resident

Under the residence principle of taxation, a South African resident's worldwide income is taxable in the Republic irrespective of where it is earned. The definition of ''resident'' in s 1 of the Income Tax Act (58 of 1962) distinguishes between natural persons and persons other than natural persons (for instance companies and trusts). We will now examine the effect of e-commerce on the concept used to determine the residence of natural persons and persons other than natural persons.

ACTIVITY 7.1

Tim, Vusi and Sina are the directors of TVS. This corporation is based in South Africa. The business sells books that Tim authors, craft and art work that Sina designs and consultancy services for mechanical engineering that Vusi offers. Sina is a South African resident, but Tim and Vusi are residents of Botswana. TVS generates income by supplying its products electronically to customers over the world who logs onto the Internet and browse TVS's website, which is located on a server in Mauritius.

If South Africa is to assert the authority to tax TVS on the income generated in South Africa, what is the basis for exercising such taxing jurisdiction?

FEEDBACK

TVS is incorporated in South Africa, therefore the residence basis of taxation will be applicable.

7.2.1.1 Natural persons

In terms of s 1 of the Income Tax Act, a natural person is a resident of South African if he or she is ''ordinarily resident'' or ''physically present'' in this country.

(a) Ordinary residence: challenges posed by e-commerce

The concept ''ordinary residence'' is not defined in the Income Tax Act. The meaning of the term can be deduced from court decisions. In *Levene v IRC* [1928] AC 217 it was held that an individual is ordinarily resident in South Africa if South Africa is his or her habitual and normal country of residence, in the sense of living here with some degree of continuity. In *Cohen v CIR* 1946 AD 174, 13 SATC 362 at 371 the court proposed that a person's ordinary residence ''would be the country to which he would naturally and as a matter of course return from his wanderings'' (see also *CIR v Kuttel* 54 SATC 298, 1992 (3) SA 242 (A)). From these cases it appears that the term ''ordinary residence'' requires a degree of physical presence (living, working, socialising, gathering assets) in a certain geographical location. In the view of the SARS, ''ordinary residence'' also requires one to have a mind set or intention to live in a particular place with a degree of permanence (Income Tax Interpretation Note 3 of 4/2/2002). Thus even if an individual is physically absent from South Africa, he or she does not lose ordinary residence status where the absence, although lengthy, is merely casual and temporary.

Technology now enables an individual to carry out many facets of life in another jurisdiction. For instance, an individual can do the following: work via the Internet, have e-mail addresses in different jurisdictions, shop, market products and do banking activities without leaving the chair on which he or she is sitting. Technology can also make it possible for a person's mode of life to be such that it cannot be said that he or she has a real home anywhere. This could be the case where a person's work requires him or her to travel on such a regular basis that he or she can be classified as a permanent wanderer.

permanent wanderer

The question that arises is whether an individual who conducts his business on the Internet or one who adopts the lifestyle of a permanent wanderer can be liable to tax in South Africa on the basis of being ordinarily resident here. With reference to the definition of the term ''ordinary residence'', it is impossible to conclude that just because an individual conducts business on the Internet, such an individual has acquired a real home on the Internet. An individual's Internet activities are carried out on a computer, inside a building that is in a physical location. It can thus be concluded that cyberspace ''presence'' should have no effect on a country's jurisdiction to tax an individual who is ordinarily resident in that country.

Likewise, adopting the lifestyle of a permanent wanderer with no intention to be ordinarily resident in one specific country should have no major effect on a country's jurisdiction to tax an individual who is ordinarily resident in that country. Adopting such a lifestyle would be too extreme a measure for most people, as it would imply that they would not have a home to return to from their wanderings, cannot form and maintain meaningful relationships, accumulate personal belongings or maintain a place of business in a specific location.

ACTIVITY 7.2

Sina's work as a director of TVS requires her to move from country to country. She rarely stays in one country for more than two months, but she regards South Africa as her home. Having adopted the lifestyle of a 'permanent wanderer', she uses the Internet to shop, bank, work and recreate through an Internet site located on a server in Mauritius.

(a) Does South Africa have jurisdiction to tax Sina's income, considering the fact that Sina conducts much of her economic activities outside South Africa?
(b) What are some of the challenges that the tax authorities would be faced with in taxing Sina's income?

FEEDBACK

(a) Sina considers South Africa to be her home. She is ordinarily resident in South Africa and will be liable for taxes on her worldwide income in South Africa (residence basis of taxation).
(b) Identifying taxable transactions and verifying the amount that has to be taxed, etc.

(b) The physical presence: challenges posed by e-commerce

In terms of s 1 of the Income Tax Act, a natural person who is not ordinarily resident in South Africa will be considered a resident if he/she is physically present in South Africa for more than 91 days in aggregate during the year of assessment, and for a period exceeding 91 days in aggregate in each of such three preceding years, or for a period exceeding 549 days during the preceding three years.

It has been suggested that it is possible for an individual to avoid numerical residence rules based on periods of physical presence by absenting himself from a given jurisdiction for the necessary number of days while continuing to work for the same employer in an uninterrupted fashion through telecommunications. Although theoretically possible, this lifestyle would be difficult to maintain if its only purpose was tax avoidance, and it will probably rarely be encountered in practice.

7.2.1.2 Persons other than natural persons (companies)

According to the definition of the term ''resident'' in s 1 of the Income Tax Act, persons other than natural persons (such as companies) are considered residents in South Africa if they are *incorporated, established or formed* in the Republic or if they have a *place of effective management* in South Africa. Incorporation, establishment or formation are technical requirements, verifiable from for instance the Registrar of Companies in the case of companies. In order to avoid high taxes, a company's place of incorporation, establishment or formation can be easily relocated to a low tax jurisdiction. Relocating of companies is enhanced with the developments in telecommunications.

place of effective management

It is however the residence of companies based on the concept ''place of effective management'' that faces major challenges when trade is conducted electronically. The phrase ''place of effective management'' is commonly used in international double tax agreements to prevent double taxation of income when an entity is considered a resident in two states, that is, a dual resident (for instance one state attaches importance to the

incorporation of the company in that state while another state places importance on the place of effective management of the company, which may be in that other state). In order to avoid double taxation on the income of that entity, article 4(3) of the OECD Model Tax Convention states that ''the taxing power is accorded to the state in which the place of effective management of the entity is situated.''

Interpretation Note 6: place of effective management

The Income Tax Act does not define the phrase: place of effective management, and South African case law does not provide guidance for the interpretation of the phrase. SARS has however issued Interpretation as guidance for interpreting the phrase. According to this Interpretation Note, the place of effective management is regarded as the place where the company is managed on a regular or day-to-day basis by its directors or senior managers. The Note indicates that this is the place where the board of directors executes and implements policy and strategy decisions, irrespective of where the over-riding control is exercised or where the board of directors meets. If management functions are exercised at a single location, that location will be the place of effective management. This location might or might not correspond with the place from where the day-to-day business operations are actually carried out.

With developments in telecommunications, it is possible for management functions not to be exercised in one place. This could be the case where the directors or senior managers exercise their management functions by using distance communication methods such as video conferencing. In such cases, it is SARS's opinion that the place of effective management will best be reflected as the place where the day-to-day operational management and commercial decisions taken by the senior managers are actually implemented, in other words, the place where the business operations are actually carried out. Determining where the actual business of a company is carried out is generally not too difficult where the company is involved in the manufacture and/or sale of tangible goods, since the manufacturing plant has to be located to a fixed location. When the company deals in intangible goods and services it is possible to manipulate the concept of ''place of effective management'' by conducting business operations and activities from various locations. Furthermore, heightened international competition may force companies to move their place of effective management from high tax jurisdictions to low tax jurisdictions.

ACTIVITY 7.3

For purposes of this question, assume that TVS is not incorporated in South Africa. TVS has no offices or other premises where it conducts its business. Its business activities are carried out on a server located on an offshore island with a low tax jurisdiction. TVS's customers have access to TVS's server through the Internet. Since most of TVS's customers are South Africans, TVS has established a place of contact in South Africa that only consists of a leased room with modems and switching and routing equipment. There is no need for employees to be present at this place of contact. If customers experience any practical problems, TVS usually hires an independent expert. TVS's directors, Tim, Vusi and Sina, normally use video conferencing from their respective home bases if they have to make management decisions about the company. If a management meeting requires their personal presence, the directors meet at the place of contact in South Africa.

(a) On what basis would South Africa tax TVS's income, if at all?
(b) What are some of the difficulties that South Africa would face in exercising the jurisdiction to tax that income?

FEEDBACK

(a) South Africa uses the residence principle to tax the worldwide income of South African residents. Juristic persons other than natural persons are resident in South Africa if they are incorporated, established or formed in the Republic, or if they have a place of effective management in South Africa. In terms of the SARS Interpretation Note 6, the place of effective management is regarded as the place where the company is managed on a regular day-to-day basis, by the directors or senior managers. The Note indicates that it is the place where they execute and implement policy and strategy decisions made by the board of directors, irrespective of where the overriding control is exercised, or where the board of directors meets. If management functions are exercised at a single location, that location will be the place of effective management. This location might or might not correspond with the place from where the day-to-day business operations are actually carried out. If these management functions are not exercised in one place, for example if the directors or senior managers exercise their management functions by using distance communication methods, it is SARS's opinion that the

place of effective management is the place where the day-to-day operational management and commercial decisions taken by the senior managers are actually implemented. In other words, it is the place where the business operations are actually carried out. If a company avoids the day-to-day management in a specific location through the use of modern technology then, in terms of SARS's approach, the place of effective management will be where the business operations are actually carried out.

(b) Where a company is involved in the manufacture and/or sale of tangible goods, it is easy to locate a place of effective management as there will be no need to look for a physical place where the day-to-day business of a company is carried out. When a company deals in intangible goods and services it becomes easier to manipulate the place of effective management by conducting business operations and activities from various locations. The heightened international competition may force companies to move their places of effective management from high tax jurisdictions to low tax jurisdictions.

7.2.2 The source principle of taxation

South Africa uses the source principle of taxation to tax the income of nonresidents that has its source in South Africa. The term ''source'' is not defined in the Income Tax Act, so its meaning has to be deduced from court decisions. In *CIR v Lever Brothers and Unilever Ltd* 1946 AD 441 at 442, it was decided the source of income is established by first determining the originating cause of income (this is what the taxpayer does to produce the income) and then by locating the originating cause.

The location of the source of income has traditionally been linked to a geographical presence in a specific country. The challenge of locating the source of income from e-commerce is that global access to websites and the high mobility of electronic transactions mean that e-commerce transactions can generate income without necessarily using any infrastructure in a given physical location.

Source rules, both nationally and internationally, often rely on a distinction between different types of income or the ability to characterise a specific type of income. This is because the character or nature of income has a significant impact on the way in which it is taxed. E-commerce causes income characterisation problems. When goods or services are supplied electronically, it may be difficult to determine whether the income

derived is for the performance of a service, royalty for the use of a copyrighted intangible or the sale of a product. The courts have developed different rules for determining the source of different types of income, and there are differences in the tax treatment of the different types of income. These differences can be used to exploit the most favourable treatment of the income concerned. The effect of e-commerce on the source of certain types of income is considered below.

7.2.2.1 The effect of e-commerce on the source of service income

The ''originating cause'' of income from services rendered is the service or the work done, and it is located where the service is performed or rendered or where the work is done (*CIR v Epstein* 1954 (3) SA 689 (A)). Locating the source of service income, even in traditional commerce, has always been difficult and will be more so when the services are performed electronically. When services are provided electronically, for instance, financial consulting services, the question that arises is whether the source of service income is located where the services are performed, rendered or done, where the inputs are produced, where the benefit of the service is received or where the service is used. If all these aspects occur in one country there is no conflict. Problems arise when they take place in different countries, each claiming jurisdiction to tax the service income.

Where conflicts prevail, apportionment between jurisdictions has traditionally been allowed on a time basis where income is derived from services rendered in different jurisdictions. Apportionment has however always been a contentious issue and will become more so in an e-commerce environment due to the inherent difficulty in locating the source of Internet services and the fact that time may not be the only measure of apportionment. A distinction may have to be made between several variables, for instance, where the input is produced, the role of the server in providing the input to the customer, or where the program interacts with the customer.

Then there is the problem of determining if the income derived is for service rendered or for the sale of goods. Many websites today offer on-line access to databases where access is restricted by a fee. This fee can be based on a number of factors ranging from a flat monthly rate for time spent on line or the number of searches invoked. This would include databases such as on-line libraries, encyclopaedias, share trading and investments sites etc. Where customers can customise the output to suit their unique requirements, it may be difficult to determine whether it is a sale of goods or services.

ACTIVITY 7.4

Tim, one of the directors of TVS who is a resident of Botswana, is the author of a number of novels. If a customer wishes to buy the books, he or she may browse the website, pay electronically and then download copies of the book. Software can also be bought in this way. If the customer cannot download the book, TVS will ship a copy to him or her. The customer may then download the payment receipt and the shipping information.

(a) What is the nature of the income from the books that are shipped to the customers?
(b) Discuss the different natures of income that could be derived from the copies that are downloaded from the website.
(c) Why is the nature or character of the income important in determining its taxation?

FEEDBACK

(a) Income from the sale of a tangible good.
(b) An amount paid to download information or software for personal enjoyment could be considered as income resulting from business profits resulting from the sale of a product. Where a transaction permits the making of copies of the information or software, then the payment should be seen as royalty income (payment for the use of the copyright).
(c) The character or nature of income has a significant impact on the way in which it is taxed. As e-commerce causes income characterisation problems, the difference in treatment for different types of income can be used to exploit the most favourable treatment of the income concerned. This is because internationally countries tax different types of income differently.

7.2.2.2 The effect of e-commerce on the source of income from sale of movable goods

The ''originating cause'' of income derived from the sale of movable goods is the conclusion of the contract of sale and its performance by the seller. The location of the contract of sale is where the activities or the business of the seller is located or carried on. In *CIR v Epstein*, a South African resident contracted with an Argentinian company to supply it with South African asbestos for resale in Argentina. The profits from these transactions were split between the two parties. The court decided that the profit accruing to the South African resident had its source in South Africa and not in Argentina, as the

income was mainly the result of his business activities in South Africa and not the result of the sale of the asbestos in Argentina.

Sometimes the activities of the seller may take place in more than one tax jurisdiction, especially when the transaction is not a ''pure'' sale but the result of a combination of transactions, for instance, manufacturing and selling or producing and selling. When this is the case, the dominant or main source has to be determined. In *Transvaal Associated Hide and Skin Merchants (Pty) Ltd v Collector of Income Tax (Botswana) (Court of Appeal Botswana)* (1967) 29 SATC 97, a South African company acquired raw hides from Botswana in order to sell them in South Africa. In determining the source of income from these business activities that extended over two countries, the court decided that the source of income had its dominate cause and source in Botswana as it was in Botswana that the process of salting and preparing the hides took place. The court held that in cases of this nature the manufacturing or production is considered the main or dominant originating cause.

The problems mentioned above are intensified when the sale of goods is conducted over the Internet. For instance, a non-resident company may generate income through sales arising out of a web page accessed by South African customers. The product may either be in tangible format or digitised (for example, computer software, music, video clips, photographs and a whole range of written text). If for example, an order for goods is placed by a buyer in one country, then the order is processed through a server in another, payment is effected in a third country and the delivery is processed from a fourth, it is difficult to apply the activities test (*Epstein's* case) or the dominant cause test (*Transvaal Associated Hide's* case) to determine the source of income. This is because e-commerce obscures the elements involved in the performance of a given transaction and makes it difficult to link the activities of a taxpayer or an item of income to a specific geographical location.

7.2.2.3 The effect of e-commerce on the source of royalty income

Definition: royalties

The term ''royalties'' is defined in article 12 of the OECD Model Tax Convention to include: all payments made as consideration for the use of, or right to use, any copyright of literary, artistic or scientific work including cinematograph films, any patent, trade mark, design or model, plan, secret formula or process or information concerning industrial, commercial or scientific.

In South Africa, it has been held that the source of royalty income is where the manufacturing or producing activity is done. In *Millin v CIR* 1928 AD 207, Sarah GertrudeMillin wrote

books in South Africa but gave the right to print and publish the books to publishers in England. They agreed to pay her royalties for the price of the books. The court decided that the application of her talent and labour was the originating cause of the royalties and since she had applied them in South Africa, the source of the royalties was South Africa. The Internet however, makes it possible for one to apply their talent and labour from various jurisdictions. This makes it difficult to determine the source of income from the royalty income that arises from the sale of the books.

Determining the source of royalty income also poses problems. According to s 11B of the Copyright Act 98 of 1978, the owner of copyright may also let copies of the computer program and earn royalty income. Digitised information can be easily and perfectly reproduced. A person desiring to purchase five copies of an electronic book may simply buy one copy of the book, and he may acquire a further right to make four copies of the book. By allowing the buyer to make reproductions, the payment is at least in part for the exploitation of copyright rights. But it may also fall under the category of service income or the income from the sale of goods.

In an endeavour to resolve characterisation problems the OECD proposed that an amount paid to download information or software for personal enjoyment or use should be seen as income resulting from business profits. Where a transaction permits the making of copies of the information or software, the payment should be seen as income for the use of the copyright, and it therefore, qualifies as a royalty. The practicality of this clarification in complex e-commerce transactions has, however, yet to be proved.

7.2.2.4 Determining the source of income of multinational enterprises that have a branch or agency in a given jurisdiction

Multinational enterprises can transact business in a given jurisdiction by using various means. The enterprise may have a subsidiary company in a jurisdiction. A subsidiary company is a separate legal entity that can be subject to tax on its worldwide income if it is in South Africa. The enterprise could also operate in a given jurisdiction by opening up a branch or an agency in that jurisdiction. A branch or agency is not a separate legal entity and so it is not considered a resident of any given jurisdiction. To ensure taxation, branches or agencies are considered ''permanent establishments'' that are taxable under the source basis of taxation. The term: permanent establishments is commonly used in double taxation agreement whereby, in terms of article 5 of the OECD Model Tax Convention, a country can apply the source basis of taxation if it can establish

that the business profits of the enterprise are to be attributed to or effectively connected to a permanent establishment located in the source country.

Definition: permanent establishment

For South African income tax purposes, the term: permanent establishment is defined with reference to the definition of the concept in article 5 of the OECD Model Tax Convention which defines a permanent establishment as: a fixed place of business through which the business of an enterprise is wholly or partly carried on. Examples, could include a place of management, a branch, an office, a factory, a workshop, a mine, an oil or gas well, a quarry or any other place for the extraction of natural resources. But it excludes the use of facilities for activities of a preparatory or auxiliary character such as storage, display or delivery.

A fixed place of business will exist where any premise, facility, installation or space is used regularly by the enterprise for business purposes. There has to be a link between the place of business and a specific geographical point, and the business of the enterprise must be carried on through the fixed place of business. The phrase ''carried on through'' indicates that the business activities are carried on at a particular location that is at the disposal of the enterprise for that purpose.

A permanent establishment will also be deemed to exist where a non-resident person habitually transacts business in South Africa through an authorised dependent agent, in respect of any income attributable to the dependent agent's activities. It is clear from the above that the term: permanent establishment applies to either a fixed place of business or the presence of an agent in a given jurisdiction.

(a) The effect of e-commerce on fixed place of business or ''permanent establishments''

website as permanent establishment

If business is conducted through a website or a server, can these be considered to be a fixed place of business or permanent establishment? An Internet website is what appears on the computer screens when a web address is accessed. It consists of the software and electronic data stored on the server and allows an enterprise to interact directly with its customers. A website is a virtual office. It is intangible property and does not provide a regular link between the place of business and a specific physical geographical point. It cannot be deemed to be a fixed place of business for purposes of the meaning of the term: permanent establishment.

ACTIVITY 7.5

TVS offers a wide variety of goods and services. They are now contemplating entering the market for the customers in Mauritius. TVS plans to have no offices, warehouses, factories, or other facilities in Mauritius. No employees of TVS will work in that country either. However, residents of Mauritius will be able to acquire goods and or services from TVS, by logging onto the TVS website via the Internet. Can Mauritius tax the income from these transactions on the basis that TVS has a permanent establishment in Mauritius?

FEEDBACK

An Internet website is the software and electronic data stored on a server. As a virtual office, it is intangible property and cannot be deemed to be a fixed place of business for purposes of the term ''permanent establishment''. A website can also not be considered a dependent agent of a permanent establishment as it is does not fit the definition of a dependent agent which specifically refers to ''a person … acting on behalf of an enterprise …''. It can also be argued that the activities of a website are limited to the supply of information of a preparatory or auxiliary nature and are consequently excluded from the definition of permanent establishment.

Server as permanent establishment

A server, on the other hand, is automated equipment on which an Internet website is stored and through which the website is accessible. It has a physical location, and if it is used regularly for enterprise business it might constitute a permanent establishment if it is at the disposal of the enterprise for that purpose. When an enterprise conducts its business through a website that is hosted on the server of an Internet Service Provider (ISP), such hosting arrangements do not result in the server and its location being at the disposal of the enterprise even though the website of the enterprise is hosted on a specific server at a specific location. This is because the enterprise does not have a physical presence at the location of the server, since the website through which it operates is not tangible. However, if the enterprise owns (or leases) and operates the server on which the website is stored and used, then the place where that server is located could constitute a permanent establishment, as the server and its location is at the enterprise's disposal. Even if the enterprise has a server at its disposal, the server must be

fixed at some location to constitute a permanent establishment. In other words, the server needs to be located at a certain place for a sufficient period.

Even if the enterprise has control over the server that is located at a fixed place of business in another country, the meaning of the term: permanent establishment still requires that the business of the enterprise should be wholly or partly carried on through the place where the server is located. Further still, a server will not be considered a permanent establishment of the enterprise if the activities carried on through a server in a given location are restricted to preparatory or auxiliary activities. Such activities would include the provision of a communication link between supplier and customer, advertising of goods or services (eg a display of a catalogue of certain products), relaying of information through a mirror server for security and efficiency purposes, gathering market data for the enterprise and supplying such information. However if such functions go beyond preparatory or auxiliary activities in that they form the main function of the enterprise and they are an important and significant part of its business activities, then a permanent establishment will be deemed to exit.

From the above, it can be concluded that a permanent establishment based on a fixed place of business will only be deemed to be present when the enterprise is carrying on business through a website that has a server at its own disposal and in a fixed location, and the business of the enterprise is not of a preparatory or auxiliary nature. However, very few enterprises carry on business through their own servers and consequently they would not be liable to tax as they will be considered not to have permanent establishment in that country. In this regard e-commerce poses challenges that can provide opportunities for the avoidance of taxes.

ACTIVITY 7.6

Bear in mind the facts in activity 7.5 while going through this activity. TVS arranges with an Internet service provider (MaurISP) to establish a connection to the Internet. TVS might maintain its own web server which is connected to MaurISP, use web hosting services on MaurISP's server, or use web hosting services on a third parties server that is connected to the Internet. TVS might maintain the web server in South Africa, in Maurituis or in some other third country with low tax rates. Does the mere fact that TVS chose MaurISP to be its Internet service provider mean that it has a permanent establishment in Mauritius?

FEEDBACK

A server is automated equipment on which an Internet website is stored and through which the website is accessible. It has a physical location and if it is used regularly for business it may constitute a permanent establishment if it is at the disposal of the enterprise for that purpose. If an enterprise owns (or leases) and operates the server on which the website is stored and used, then the place where that server is located could constitute a permanent establishment as the server and its location are at the enterprise's disposal. Even if the enterprise has control over the server, the meaning of permanent establishment still requires that the business of the enterprise should be wholly or partly carried on through the place where the server is located. Further more, a server will only be considered a permanent establishment of the enterprise if the activities carried on through a server in a given location are restricted to preparatory or auxiliary activities.

(b) E-commerce and ''dependent agent'' permanent establishments

dependent agent

In terms of article 5(5) of the OECD Model Tax Convention, a ''dependent agent'' is a person who habitually acts on behalf of an enterprise and has the authority to conclude contracts in the name of the enterprise in the other contracting state. Can an ISP be deemed a dependent agent due to its hosting of the website of a specific enterprise through servers owned and operated by the ISP? According to the OECD Commentary, the ISP will not constitute a dependent agent of the enterprise to which the server belongs, because it does not normally have authority to conclude contracts in the name of these enterprises. ISPs are normally independent enterprises acting in the ordinary course of their own business, which entails hosting web sites of many different enterprises.

ACTIVITY 7.7

TVS is now contemplating several different ways of providing Internet access for their Mauritian customers. Once TVS has set up a server with an IP address, TVS customers may choose an Internet service provider (ISP) which enables access to all IP addresses on the Internet. Having gained access, the customers are free to visit TVS's website (eg http://www.tvsall.com). TVS makes arrangements with Petros, an online service provider that provides Internet access to customers in Mauritius, to feature the TVS cybermall prominently to users who visit the website.

Petros has his own local telephone numbers in Mauritius which are supplied directly by the telecommunication companies, or it subleases local access numbers from third party vendors.

Can TVS be regarded as having a permanent establishment in Mauritius?

FEEDBACK

TVS can be considered to have a dependent agent permanent establishment in Mauritius. In terms of Article 5(5) of the OECD Model, a dependent agent is a person that habitually acts on behalf of an enterprise and has the authority to conclude contracts in the name of the enterprise in the other contracting state. If the activities of Petros are limited to the supply of information of a preparatory or auxiliary nature, then TVS cannot be considered to have a permanent establishment in Mauritius.

7.3 EXAMPLE OF SOUTH AFRICA'S SPECIFIC ANTI-AVOIDANCE PROVISIONS AFFECTED BY E-COMMERCE

7.3.1 Transfer pricing

transfer price

The term: transfer pricing describes the process by which related entities set prices at which they transfer goods or services between each other. Transfer pricing is also described as the systematic manipulation of prices in order to reduce profits or increase profits artificially or cause losses and avoid taxes in a specific country. A transfer price is a price set by a taxpayer when selling to, buying from, or sharing resources with a related or connected person. It is usually contrasted with a market price, which is the price set in the marketplace for transfers of goods and services between unrelated persons where each party strives to get the utmost possible benefit from the transaction. Transfer prices are usually not negotiated in a free, open market and so they may deviate from prices agreed upon by nonrelated trading partners in comparable transactions under similar circumstances.

Transfer pricing between subsidiaries of one enterprise which are all resident in one country usually poses minimum tax avoidance problems since the tax laws are the same for all the subsidiaries in the group. Transfer pricing is most problematic when it comes to multinational corporations trading in various jurisdictions. A multinational corporation is usually composed of a number of legally autonomous but interrelated companies

or subsidiaries operating in different countries but being directed by a parent company. Since related companies operate in different countries, they are not subject to the same laws and regulations, especially in tax matters. Related companies in a multinational group may thus resort to fictitious transfer pricing in order to manipulate profits so that they appear lower in a country with higher tax rates and yet higher in a country with lower tax rates. Most developed countries that impose income taxes at significant rates are concerned about the loss of tax revenue that results through transfer pricing and so they have some kind of transfer pricing provisions in their tax laws. These laws protect their tax base from transfer pricing schemes that multinationals get involved in, and are of the utmost importance. In South Africa the transfer pricing provision is set out in s 31(2) of the Income Tax Act. In brief, the section provides that the Commissioner of SARS can adjust the consideration for goods or services supplied in terms of an international agreement if the actual price paid is either less or greater than the price that would have been paid if the supply of goods or services had been between independent parties dealing on an arm's length basis. In other words, the adjustment is based on the conditions that would have existed between unconnected persons under comparable circumstances.

arm's length price

The Commissioner of SARS determines an arm's length price by using certain methods that are set out in SARS Practice Note 7. Generally these methods are based on measuring a multinational's pricing strategies against a benchmark of the pricing strategies of independent entities in uncontrolled transactions. The Commissioner of SARS uses the most appropriate method depending on the particular situation and the extent of reliable data. The suitability and reliability of a method thus depends on the facts and circumstances of each business and the market realities applicable to each individual case.

7.3.2 Effect of e-commerce on the transfer pricing provision

E-commerce impacts on transfer pricing because e-commerce has the effect of removing physical boundaries, making it significantly more difficult for tax administrators to identify, trace, quantify and verify cross-border transactions.

Applying the transfer pricing provisions requires evidence of an international agreement having been entered into by the parties. In e-commerce it is difficult to procure an international agreement as there is usually no paper trail of e-commerce transactions. The available information may not be reliable, as it can be easily altered without trace as a means of avoiding taxes. E-commerce also makes it easy to split the various risks

and activities in a multitude of ways that may make it hard to obtain relevant data.

In terms of s 31(2) the acquirer of the goods and services in an international agreement has to be connected to the supplier, and the price of the supplied goods or service has to be a non arm's length price. In terms of s 1 of the Income Tax Act the term: ''connected person'' in relation to a company includes: its holding company, its subsidiary, and any other company where both such companies are subsidiaries of the same holding company.

connected person

In traditional commerce, tax administrators can establish a link or connection between taxpayers and related parties from documentation that relates to the registration of the relevant companies. However in e-commerce it is not easy to determine whether the companies concerned are connected. This is because the identity of the buyers and sellers who participate in Internet-based transactions is often irrelevant. Currently, it is not easy to link activities on the Internet to the parties associated with such activities. An Internet address (domain name) only indicates who is responsible for maintaining that address. It provides no links to the computer, its user who is corresponding on that address or even where the computer is located. In such circumstances, it is difficult to apply the arm's length principle, as the connected parties who could be involved in transfer pricing schemes might not be easily identifiable so as to determine if they are connected.

In order to apply s 31(2), the price for the goods or services that are supplied between the connected parties must be either less than or greater than the price which the goods or services might have been expected to fetch if the parties to the transaction had been independent persons dealing at arm's length. In other words, before applying the arm's length price, the Commissioner has got to know the non arm's length price at which the goods or services were sold. Finding this price in a traditional commerce transaction is often not difficult as the parties concerned often keep paper trails of the transactions they are involved in. E-commerce transactions, however, do not normally reveal the value of a given transaction and this makes it difficult to determine how the prices charged for the relevant transactions were arrived at. Finding the price of goods or services is further complicated by the anonymous nature of electronic transactions and the anonymous electronic money or digital cash which is used to effect payment.

In order to apply the methods that are used so as to arrive at an arm's length price, there must be a comparable uncontrolled transaction. There cannot be an adjustment in the absence of a transaction. The comparisons that are made between the

relevant transactions are based on verifying the dealing of each separate entity. In traditional commerce, applying the separate entity approach to multinational enterprises has always posed certain difficulties. This is because multinationals are often integrated enterprises dealing in highly specialised goods and services or in intangibles. It is through integration that the multinational enterprises achieve economies of scale in aspects such as brand development and logistics. These measures of integration cannot be duplicated in the context of independent transactions conducted by two nonintegrated businesses performing the same or similar transactions and selling the same or similar products. In the context of e-commerce, applying the separate entity approach is made even more difficult as it is difficult to identify the precise transaction each entity is involved in. This is because e-commerce makes transactions increasingly unique and not comparable to others. Even for those transactions that could be identified, e-commerce creates situations where separate transactions are so closely linked or continuous that they cannot be evaluated adequately on a separate basis. This is further augmented by the nearly instantaneous transmission of information, the speed at which transactions are concluded and the increase in the bulk of transactions concluded. This makes it very difficult to find comparables for determining the value of a single electronic contribution in a highly integrated Internet transaction.

ACTIVITY 7.8

TVS has subsidiary companies in countries A, B and C. TVS produces electronic products that require inputs from all these companies. The final product requires a high level of integration among all the companies involved. Basically the product is manufactured by a company in country A, then marketed in by the company in country B and shipped by a company in country C.

What are some of the challenges that South Africa might be faced with in preventing transfer pricing resulting from the above transactions?

FEEDBACK

The following are the challenges that South Africa might be faced with in preventing transfer pricing:

- E-commerce impacts on transfer pricing because e-commerce has the effect of removing physical boundaries,

making it significantly more difficult for tax administrators to identify, trace, quantify and verify cross-border transactions.
- E-commerce poses characterisation problems.
- It is often difficult to determine whether an international agreement has been entered into.
- There is virtually no paper trail.
- E-commerce also makes it easy to split the various risks and activities in a multitude of ways that may make it hard to obtain relevant data.
- It becomes difficult to verify whether the parties are connected.
- It is difficult to determine the price for the goods or services that are supplied between the connected parties.
- It is difficult to apply the methods that are used to arrive at an arm's length price. These methods require a separate-transaction approach. In the context of e-commerce, applying the separate-transaction approach is made even more difficult as it is difficult to identify precisely what the transaction is. The nearly instantaneous transmission of information, the speed at which transactions are concluded and the increase in the bulk of transactions concluded make applying the arm's length principle difficult.
- It is difficult to find comparables for determining the value of a single electronic contribution in a highly integrated Internet transaction.

7.4 THE EFFECT OF E-COMMERCE ON TAX ADMINISTRATION AND ENFORCEMENT IN SOUTH AFRICA

Apart from the fact that e-commerce challenges a country's jurisdiction to tax income in certain instances, it also encumbers the enforcement of tax laws. The ability to collect taxes is based on the ability to: identify and locate taxpayers (the tax system must have access to the taxpayer or the taxpayer's assets to ensure the collection of taxes payable); identify and verify taxable transactions; establish a link between taxpayers and their taxable transactions.

E-commerce transactions not only obscure the identity and location of the buyers and sellers who participate in Internet-based transactions, but often make them irrelevant. Anonymity is a unique feature central to e-commerce transactions. The use of electronic money or digital cash enhances this feature and leads to increased enforcement problems as there is usually no trace of the identity of the person spending the electronic money. For instance, a consumer can download electronic tokens from an on-line bank and use these tokens to make

purchases, leaving no paper or electronic trace as to the date and or the value of the transaction. This renders South Africa's tax and auditing methods, which are based on the physical evidence of a taxpayer's financial records, prone to tax avoidance and the loss of revenue can be enormous where electronic money that is unaccounted for is used.

Furthermore, e-commerce makes it difficult to obtain the reliable transaction information necessary to determine the value of the taxable element of a given transaction. This is because electronic records can easily be altered without trace. Currently, it is not easy to link activities on the Internet to the parties associated with such activities. An Internet address (domain name) only shows who is responsible for maintaining that address, and provides no links to the computer, its user or even where the computer is located. The anonymous nature of electronic money also makes it easy to move money instantaneously and virtually undetectable.

ACTIVITY 7.9

What are some of the challenges that the tax authorities face in taxing e-commerce transactions?

FEEDBACK

The ability to collect taxes is based on the ability to:

- identify the location of taxpayers
- identify and verify taxable transactions
- establish a link between taxpayers and their taxable transactions

7.5 INTERNATIONAL AND NATIONAL RESPONSES TO THE TAXATION OF E-COMMERCE

Because e-commerce creates opportunities for tax avoidance and evasion as a result of the challenges it posses to a country's jurisdiction to tax income and the difficulties of enforcing tax laws, a number of countries and international bodies have come up with suggestions on how e-commerce transactions should be taxed.

7.5.1 The OECD

The OECD has taken a lead on the international front of e-commerce with a conference held in Turku, Finland in November 1997. This conference was followed by the Ottawa

conference in Canada in October 1998. It was in the last conference that a principles based approach was adopted in developing a framework for taxation. In the OECD Report by the Committee on Fiscal Affairs (CFA), entitled *A borderless world: realizing the potential of electronic commerce* (8 October 1998) (see http//:www.oecd.org), the following framework was highlighted as widely accepted general tax principles that should apply to the taxation of e-commerce:

- *Neutrality*. Taxation should seek to be neutral and equitable between forms of electronic commerce and between conventional and electronic forms of commerce. Business decisions should be motivated by economic rather than tax considerations. Taxpayers in similar situations carrying out similar transactions should be subject to similar levels of taxation. This means that there is no need for a special new tax such as a ''flat rate'' or a ''bit tax''.
- *Efficiency*. Compliance costs for taxpayers and administrative costs for the tax authorities should be minimised as far as possible.
- *Certainty and simplicity*. The tax rules should be clear and simple to understand so that taxpayers can anticipate the tax consequences of a transaction in advance, including knowing when, where and how the tax is to be accounted.
- *Effectiveness and fairness*. Taxation should produce the right amount of tax at the right time. The potential for tax evasion and avoidance should be minimised while keeping counteracting measures proportionate to the risks involved.
- *Flexibility*. The systems for the taxation should be flexible and dynamic to ensure that they keep pace with technological and commercial developments.

The above-mentioned framework is not at odds with the views held by SARS. Nevertheless, care should be taken to ensure that the existing South African tax base is not eroded by later international decisions favouring nations with sophisticated and developed economies (SARS Doc at 8). It was also agreed at the 1998 OECD conference that in taxing e-commerce transactions, the fiscal sovereignty of countries should be maintained so that each country is able to protect its tax base and at the same time be able to avoid double taxation and unintentional nontaxation of e-commerce transactions. In the 2001 OECD 6th global forum, it was agreed that e-commerce is a global phenomenon affecting a large percentage of world trade and therefore it required a global solution. It was suggested that there was consequently a need for dialogue between governments and businesses to build up international consensus on the taxation of e-commerce, and the maintanance of national sovereignty and neutrality of taxation. In an endeavour to offer guidance in the taxation of e-commerce, it was emphasised that solutions

offered in this regard must be geared to promoting foreign economic growth as well as safeguarding governments' tax bases. Emphasis was especially put on neutrality in the taxation of e-commerce, stressing that it should not be given more or less favourable treatment than that given to conventional commerce (see http://www.oecd.org).

7.5.2 European Union (EU)

The European Union Commission released its communication on 15 April 1997, *A European initiative in electronic commerce,* in which it summarises its tax policy as follows:

- To allow electronic commerce to develop, it is vital for tax systems to provide legal certainty (so that tax obligations are clear, transparent, and predictable).
- Tax neutrality (so there is no extra burden on these new activities as compared to traditional commerce)
- The potential speed and anonymity of electronic transactions may also create new possibilities for tax avoidance and evasion (these need to be addressed in order to safeguard the revenue interests of government and to prevent market distortions)

7.5.3 The USA

In November 1996 the US Department of Treasury compiled a document entitled *Selected tax policy implications of global electronic commerce*. This document highlighted the following points:

- New technologies, such as the Internet, have effectively eliminated national borders on the information highway. As a result, crossborder transactions may run the risk that countries will claim inconsistent taxing jurisdiction, and taxpayers will be subject to quixotic (impractical) taxation.
- In order to ensure that these new technologies are not to be impeded, the development of substantive tax policy and administration in this area should be guided by the principle of neutrality.
- Transactions in cyberspace will probably accelerate the current trend to de-emphasise traditional concepts of source based taxation, increasing the importance of residence based taxation.
- Another major category of issues involve the classification of income arising from transactions in digitised information.
- The major compliance issue posed by e-commerce is the extent to which electronic money is analogous to cash and thus creates the potential for anonymous and untraceable transactions.

In 1998 on 21 October, the Internet Tax Freedom Act was signed into public law 105-277 in the USA. Section 1101 of that Act places a moratorium on any new taxes on Internet access, and created a commission to study and make recommendations about domestic and foreign policies towards the taxation of e-commerce. A number of proposals have been made, mostly calling for the Internet to be free from sales and usage tax. It should be noted that the Internet Tax Freedom Act is in respect of new taxes and has no bearing on existing tax legislation, for example, the taxing of Internet sales for income tax purposes.

7.5.4 Australia

The Australian Taxation Office (ATO) released a discussion paper on tax and the Internet in August 1997. This report contained detailed recommendations relating to the tax environment affecting electronic commerce. These recommendations were based on the principle of achieving neutrality between the treatment of businesses engaged in traditional physical commerce and the treatment of those engaged in electronic commerce.

The ATO Electronic Commerce Project states that there are many challenges for the tax administration. These include:

- difficulties in identifying the parties behind Internet businesses
- the ability of these businesses to store tax records offshore, or to encrypt them or alter them without trace
- the possibility that some type of electronic money would exacerbate the problems of the physical cash economy
- the removal of efficient tax-collection points such as intermediaries in the distribution chain from producer to consumer, in an effect known as disintermediary
- the ability of technologies to change the nature of products, through digitisation, and hence the taxation treatment of the income from the sale of those products

The ATO project concludes that countries will encounter real problems in determining the source of income, residence, and permanent establishment of global electronic businesses and that existing international rules in this area may need to be substantially revised. The project also raises concerns about increased scope for tax planning, especially using tax havens, and for increased accidental noncompliance, as small and medium-sized enterprises (SMEs) engage in international trade and become subject to international taxation obligations with which they may not be familiar (see, http://www.ccra-adrc.gc.ca/tax/business/ecomm/ecom3-e.html).

7.5.5 Canada

In the report on *The implications of electronic commerce on taxation*, Canada states the principles of tax policy as a guide concerning the appropriate form of taxation for e-commerce. These principles include:

- Economic neutrality and equity. A fundamental principle of sound tax policy is that a tax should be economically neutral as well as equitable. A tax is neutral (or efficient) when it does not induce taxpayers to change their behaviour in response to the tax. A tax will be considered equitable if the tax burden is distributed fairly among similarly situated taxpayers. Thus a tax narrowly focused on only one industry or on certain taxpayers within that industry would not be equitable.
- Ease of administration. Taxes should be easy to administer and collect. If a tax is difficult to understand, no matter how perfect it may be in theory or design, or if compliance burdens are excessive and the costs of administering the tax are unreasonable, the tax will fail to serve the intended function as a reliable source of revenue.
- No multiple taxation. This principle is a logical corollary of the principles of tax neutrality and tax equity. The tax treatment of electronic commerce transactions and of traditional transactions must not confer a competitive advantage on one way of carrying business.
- Fair allocation of tax base and revenue. Electronic commerce raises significant fiscal impacts between jurisdictions. Although revenue neutrality is desired, such concepts as residency and permanent establishment may result in shifting of revenue between countries and between provinces. Although the total amount of revenue collected by all jurisdictions may remain the same, there may be significant shifts in revenues between jurisdictions. The effect in Canada is not clear.

This framework suggests that the best way to implement these principles is to follow existing concepts and principles wherever possible. It also notes that the challenges facing the tax system are the result of three basic characteristics of the Internet, namely, the anonymity of buyers and sellers, the capacity for multiple small transactions, and the difficulty of associating online activities with physically defined locations (see http://www.ccra-adrc.gc.ca/tax/business/ecomm/ecom3-e.html)

7.5.6 South Africa

In South Africa, the Katz Commission report (the Commission of Inquiry into certain aspects of the tax structure of South Africa of 1997) on e-commerce recognised the need of protecting South

Africa's tax base. The Commission noted that e-commerce impacts on the basic methods of today's international taxation, making irrelevant the concept of physical presence in order to trade, that current residence notions can be manipulated through the hypermobility of an entire office or management capacity, and that the manner in which goods and services can be contracted for, advertised and even delivered via electronic means can lead to the erosion of South Africa's tax base. The Commission recommended that South Africa should not seek to pioneer a whole new tax regime to cope with the changes brought about by e-commerce, but rather that South Africa should internationalise its laws affecting international trade and investment.

In the Green paper on e-commerce, a consultative document designed to raise questions on issues that needed to be addressed by the government policy formulation process on e-commerce, it was pointed out that the legal framework in South Africa is currently insufficient to deal with e-commerce issues. The current legislation was basically tailored for paper based commercial transactions, and there was therefore a need to formulate a new legal framework that includes those transactions that are conducted electronically.

In 2002 the Electronic Communications and Transactions Act was enacted to provide for (among other provisions) ''the facilitation and regulation of electronic communications and transactions''. Some of these provisions, if complied with and effectively enforced, may alleviate some of the identification and reliability issues identified above. For instance, s 38 of the ECT Act provides that the authentication of the products or services of service providers will only be accredited if the electronic signature to which the authentication products or service relates is uniquely linked to the user, is capable of identifying the user, is created using means that can be maintained under the sole control of that user, and will be linked to the data message to which it relates so that any change of the data can be detected. It also has to be based on face-to-face identification of the user. Sections 42 and 43 provide that a supplier of electronic goods and services must display certain information on the website where the goods are offered, for instance, its full name and legal status, its physical address and telephone number, its web site address and e-mail address, its registration number, place of registration, names of office bearers, membership of any self regulatory body and the physical address where the supplier will receive legal documents. Sections 80 and 81 deals with the appointment of cyber inspectors, who have the power to inspect any web site activity and information in the public domain. Sections 85 and 86 deals with the penalties of cyber crime. The practicality and

effectiveness of these provisions are yet to be determined. On the whole this Act does not deal with the taxation aspects of e-commerce.

7.6 CONCLUSION

From the above, it can be noted that countries are caught up in the dilemma of either not taxing e-commerce and risk the depletion of their tax bases or taxing e-commerce and risk the stifling of its development. In South Africa's case, the government is of the view that access to the Internet and information technology is the key to the upliftment of its people, especially those in rural areas and those involved in small or medium-sized enterprises. Traditionally, only big companies with substantial capital could make significant sales outside the Republic. Now even the smallest e-commerce enterprise can trade in national and international markets. If e-commerce is not regulated and taxed, the loss of revenue can be tremendous in a situation where anybody and any enterprise that engages in e-commerce will not be taxed. There is therefore a need for balance in the government polices in respect to development and the taxation of e-commerce. South Africa should work hand in hand with other developed nations in order to come up with a feasible way of taxing e-commerce transactions so that the tax avoidance opportunities that e-commerce has created can be curbed.

APPENDIX

Glossary of terms*

Analog: Technology used primarily for broadcasts and phone transmissions.

Application: a computer program, which performs a set of tasks forming a defined function or service.

Authentication: a mechanism of using information resources to verify the claimed identity of a party to a transaction or an entity involved in a transaction.

Authorisation: an authentication process whereby predetermined rights, including access to information resources, are granted to users or entities

Bandwidth: measure of the capacity of a communications channel, expressed in bits per second

Bit: A minimum unit of binary information as stored in a computer memory. A bit has only two states — on or off — which are called ''ones'' (1's) and ''zeros'' '' (0's).

Broadband: this transmission medium allows transmission of voice, data and video simultaneously at higher transfer rates. Broadband transmission media generally can carry multiple channels.

Browser: software on the client's PC used to fetch/read documents from the Web, display them on-screen and print them, jump to others via hypertext, view images and listen to audio files

Bulletin-board system (BBS): An information communication system for sharing information and experiences via the dial-up message centre.

ccTLD: country code Top Level Domain refers to a high level Internet Protocol address to identify a country e.g, za for South Africa

Cache: A temporary storage are for instructions and data near a computer's processing unit, usually implemented in high-speed memory. It replicates information from main memory or storage in a way that facilitates quicker access, using fewer resources than the original score.

Certificate: a certificate is a public key that has been digitally signed by a trusted authority to identify the user of the public key. SET uses certificates to encrypt for example payment information.

Certification Authority: a secure third party organisation or company that issues digital certificates used to create digital signatures and public key pairs. Certificate authorities guarantee that the two parties exchanging information are really who they claim to be.

Click wrap contracts: Contracts concluded in an online environment, usually the Internet, where the terms of a contract are set out and ''offered'' by one party on a website and the other party indicates ''acceptance'' of those terms by for example clicking on an ''accept'' button or icon and hence concluding the contract

Confidentiality: reasonable assurance that online or stored data cannot be viewed and interpreted by any person other than an authorised one.

Connectivity: The capability to provide, to end users, connections to the Internet or other communications networks

Click wrap contracts: Contracts concluded in an online environment, usually the Internet, where the terms of a contract are set out and ''offered'' by one party on a website and the other party indicates ''acceptance'' of those terms by for example clicking on an ''accept'' button or icon and hence concluding the contract

Content provider: A trader with information-based products. Services to access and manage the content are also included.

Country-code top-level domain: see the definition for ccTLD.

Cryptography: Practice of digitally ''scrambling'' a message, using (a) secret key(s).

Digital: the representation of data by the bits and bytes of binary code. Vinyl records and cassette music tapes carry analogue media

Digital Certificate: See ''certificate''.

Digital Divide: a term used to reflect the technological gap between countries that have fully exploited ICT and those that have not. The digital divide is often associated with the resulting gap in terms of economic development.

Digital Signature: Digital codes that can be attached to an electronically sent message to uniquely identify the sender.

Domain name: A unique name, designed to be humanly intelligible and which is linked to an IP address

Domain-name-system: The system to translate domain names into IP addresses

EDI: Electronic Data Interchange — is a de facto standard format for exchanging business data between companies computer application in a standardised form, but usually refers to as proprietary system of delivery.

Electronic Fund Transfer: the electronic movement of money over secure private networks between banks' accounts

Electronic Money: means of retail payments executed over Internet, which leaves other traditional electronic payments outside of its scope. Alongside with most commonly used smart card, the term include: e-cards, trade cards, traditional credit, debit and stored value cards, as well as e-cash, digicash, digiwallet, e-credit, e-loans etc.

Electronic payments system: an array of institutions and mechanisms ensuring the cash flow through electronic communications and timely provision of credit and settlements of debts at much less than traditional system could provide costs

Encryption: the coding of data for the purpose of security or privacy

Extranet: a website links businesses to customers, suppliers, etc. for electronic communications.

File Transfer Protocol (FTP) Transmission Control Protocol/Internet Protocol (TCP/IP): A standard used to log onto a network, list directories and copy files.

Gateway: the link between networks and computers which allows

messages to be routed across. Often associated with security measures.

Hardware: the physical pieces of computer equipment needed to make up a system.

Hosting: the storage and maintenance of the data making up the content of Websites.

Hyperlink: a reference link that can be made from a point in one web page (traditionally in blue and underlined) to any other point on any web page on the World Wide Web.

HyperText Markup Language (HTML): A document-formatting language, predominantly used to create WWW pages. The user's browser interprets the HMTL commands and formats the page layout, fonts, and graphics on the screen. HTML can also create hyperlinks.

ICT: Information and Communication Technologies a generic term used to express the convergence of information of information technology and communications. One prominent example is the Internet.

Information-based economy: refers to a country or region where ICT is used to develop economic foundation and market transactions

Integrity: reasonable assurance that stored or online data which its intended destination without being modified in any unauthorised manner.

Interconnection: The connection with each other of the telecommunications networks of different operators so that signals or services are transported over such interconnected networks.

Internet: the Worldwide collection of networks communicating through common languages and protocols. Also the basic infrastructure for the new economy over which information can be transferred, transactions made and work done

Internet Protocol (IP): A protocol that tracks the address of nodes, routes outgoing messages and recognises incoming messages.

Internet Protocol address (IP address): a unique set of alphanumerical characters identifying the location of computers on the Internet.

Internet Service Provider: companies that specialise in linking organisations and Individuals to the Internet as well as providing services to them

Intranets: using the same Internet technology, but hosted by private servers not accessible by the public over the Internet. Companies are using Intranets to facilitate their internal knowledge management, communication, collaboration on projects, HR functions, etc.

Multimedia: an interactive combination of text, graphics, animation, images, audio and video displayed by and under the control of a PC

Network: Any number of computers (such as PCs and servers) and devices (such as printers and modems joined together by a physical communication link.

Permanent Establishment: a fixed place of business through which the business of an enterprise is wholly or partly carried on.

Personal data: is any data, which refers to an identified or identifiable

individual, which is not otherwise readily available via a public source(s).

Portal: website which aims to be the starting point though which one enters the Web.

Private key: A key that is known only to the recipient and that is used to encrypt and decrypt messages. It is also known as a ''secret key''.

Public key cryptography: this encryption method requires two unique software keys for decrypting data, one public and one private. Data is encrypted using the published public keys and the unpublished private keys are used to decrypt the data.

Public-Key Infrastructure (PKI): The software and hardware components necessary to manage and enable the effective use of public-key encryption technology.

Server: usually computer hub of a network, fulfilling servers' functions to client computers connected to it, such as storing files and databases and running applications.

Shrink wrap contracts: Same as click wrap contracts except for the fact that the accept icon is actually a shrinked box containing the actual product or service itself e.g. software. Accepting this type of a contract results in an immediate on-line consumption

Smart Card: card containing memory and a microprocessor, that can serve as personal identification, credit card, ATM card, telephone credit card, critical medical information record and as cash for small transactions.

Software: computer programming which gives the hardware its usefulness through various functions the software can perform.

Teledensity: teledensity refers to the number of telephone lines per 100 people, s rough measure of the ubiquity of the public switched telephone network in a country.

URL (''Universal Resource Locator''): the string of characters which identifies the communication protocol used (http) and the IP address of the server site.

VPN: Virtual Private Network — a VPN is a part of the public Internet to which access is controlled by firewalls and secure tunnels to enable private and secure use by authorised users

Web browser: A client, system or program use din accessing the WWW.

Web hosting: The storage of data on a server for later access.

Web server: Webpages or websites are hosted on a Web server. A Web server is a centrally located computer that enables remote ''clients'' (system or program) to access the page or site content.

Website: pages of information linked to one another by hyperlinks (usually organised around a menu), with the main page (usually including the menu) bearing the domain address. These pages are on a Web server and are accessible from any browser on the World Wide Web.

World Wide Web: a collection of information located in many Internet servers that can be accessed with a browser or by navigating via hyperlinks.

Bibliography

ARTICLES

Akhtar & Cumbow ''Why domain names are not generic: an analysis of why domain names incorporating generic terms are entitled to trademark protection'' 2000 *B C Intell Prop & Tech F* 110501

Bagrain ''Transacting in cyberspace'' 6(2) *JBL* 50

Barrett D & Coulter C ''Proposed Council Directive on the Legal Protection of Databases'' (1992) 8 *Computer Law & Practice* 34

Bastian MJ 'Protection of ''noncreative'' databases: harmonization of United States, foreign and international law' (1999) 22 *Boston College Environmental Affairs LR* 425

Bazerman, Steven and Georget, Richard (2003), 'The Obverse of Cyber squatting', *World eBusiness Law Report* available at: INK ''http://www.ipcounselors.com/wblr20030410.htm''*http://www.ipcounselors.com/wblr20030410.htm*

Bradfield, Owen (2001), 'Domain Names in Australia Legal and Contractual Dispute Resolution', 12(1) *Journal of Law & Information Science*, p 234.

Caffarelli DJ ''Crossing virtual lines: trespass on the Internet'' (1999) *Boston Univ J of Science and Technology* 6

Christie A ''The ICANN domain name dispute resolution system: a model for other transborder intellectual property disputes on the Internet?'' — paper delivered at the International Conference on Dispute Resolution in Electronic Commerce (6–7 Nov 2000) in Geneva

''Contracts'' 5(1) *LAWSA*

Cornish ''1996 European Community Directive on Database Protection'' (1996–1997) 21 *Columbia-VLA Journal of Law & the Arts* 1

Davies C ''Electronic commerce — practical implications of Internet legislation'' (3) 3 (1998) *Communications Law*

Du Toit (2007), 'New domain name regulations', *ITWeb* 16 August 2007, *http://en.newspeg.com/actualite/Economy/New%20domain%20name%20regulations-3627098.news*

Donahey ''Current developments in on-line dispute resolution'' — paper presented at the International Conference on Electronic Commerce and Intellectual Property: Online Dispute Resolution Workshop, published by WIPO (1999)

Dworkin ''Exceptions to copyright exclusivity: article 9(2) (Berne) and article 13 (TRIPs): what is fair use in the new international order?'' — paper delivered at the Fifth Annual Conference on International Intellectual Property Law and Policy (3–4 Apr 1997) in New York, US

Dreier ''Unsolved copyright issues in digital and network environment'' (1995) March *Copyright World* 36

Evans G ''Opportunity costs of globalizing information licences:

embedding consumer rights within legislative framework for information contracts'' (1999) 10 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1.

Forhan MA ''*Tasini v New York Times*: the write stuff for copyright law?' (1999) 27 *Capital University LR* 863

Greene, KJ (2004), 'Abusive trademark litigation and the incredible shrinking confusion doctrine – trademark abuse in the context of entertainment media and cyberspace', *Harvard Journal of Law & Public Policy*, p 615

Hayes DL ''Advanced copyright issues on the Internet'' (1998) 7 *Texas Intellectual Property LJ* 1

Hurter E ''Dispute resolution in cyberspace: a futuristic look at the possibility of online intellectual property and e-commerce arbitration'' (2000) 1 *South African Mercantile Law Journal* 199–208

Hurter, Eddie (2007), 'Evaluation of Selected Aspects of the Alternative Dispute Resolution Regulations for the resolution of domain name disputes in the .za domain name space', (19) 2 *SA Mercantile aw Journal*, p 165

Kerever Intellectual property: Determination of the law applicable to digitized transmissions''

Koelman K & Hugenholtz B ''Online service provider liability for copyright infringement'' — paper delivered at a Workshop on Service Provider Liability presented by the World Intellectual Property Organization (10 Dec 1999) in Geneva (OSP/LIA/1)

Lavenue LM ''Database rights and technical data rights: the expansion of intellectual property for the protection of databases'' (1997) 38 *Santa Clara LR 1*

Loundy, David J (1997), 'A Primer on Trademark Law and Internet Addresses', 15(3) *John Marshall Journal of Computer & Information Law*, p 465

Lui ''Recent developments in copyright, database protection and (online) licensing'' (1999) 7 *International J of Law and Information Technology* 73

Mann ''The doctrine of jurisdiction in international law'' 1964 (111) *RPC*

Marx (2004), 'Domain name protection in South Africa', *Obiter,* pp 125127

Morton ''Draft EC Directive on the Protection of Electronic Databases: comfort after *Feist*'' (1992) 8 *Computer Law & Practice* 38

Munden, Richard A J () 'Reverse Domain Name Hijacking'': Setting the limits of Trade Mark Protection in Cyberspace', available at: *http://users.ox.ac.uk/˜edip/munden.pdf*

Murray, Andrew (1998), 'Internet Domain Names: The Trade Mark Challenge', 6(3) *International Journal of Law and Information Technology*, p 285

Namespace ZA 'Comments on the Electronic Communications and Transactions Bill Draft ECT bill submission 2002-04-24', available at: *www.namespace.org.za*

Nelson RG ''Recent development: seeking refuge from a technology storm: the current status of database protection

legislation after the sinking of the Collections of Information Anti-Piracy Act and the Second Circuit Affirmation of *Matthew Bender & Co v West Publishing Co*'' (1999) 6 *J of Intellectual Property Law* 453

Oktay B & Wrenn G ''A look back at the notice-takedown provisions of the US Digitial Millennium Copyright Act one year after enactment'' — paper delivered at a Workshop on Service Provider Liability presented by the World Intellectual Property Organization (9–10 Dec 1999) in Geneva (OSP/LIA/2)

Olivier, D and Jearey, S 'New finding on domain name parking good news for brand owners', available at: http://www.bowman.co.za/LawArticles/Law-Article.asp?id=2132417342

Olmesdahl ''Unheralded demise of *Wolmer versus Rees*'' 1984 *SALJ* 545

Pattison M ''The European Commission's Proposal on the Protection of Computer Databases'' [1992] 4 *European Intellectual Property Review* 113

Pistorius ''Formation of Internet contracts: an analysis of the contractual and security issues'' 1999 *SA Merc LJ* 282

Pistorius ''Shrink-wrap and click-wrap agreements'' 7(3) *JBL* 79

Radloff ''The advent of the point and click contract'' Jan 2000 *De Rebus* 27

Al Ramahi, Mohammad S (2006), 'Internet Domain Names & Trademark Law: Does the Current Legal Scheme Provide and Adequate Protection to Domain Names under the US & UK Jurisdictions?', Paper delivered at the 21st BILETA Conference: Globalisation and Harmonisation in Technology, April 2006, Malta, available at: *http://www.bileta.ac.uk/Document%20Library/1/Internet%20domain%20names%20and%20trademark%20law%2020does%20the%20current%20legal%20scheme%20provide%20an%20adequate%20protection%20to%20domain%20names.pdf*>

Reichman JH & Samuelson P ''Intellectual property rights in data?'' (1997) 50 *Vanderbilt LR* 51

Reichman JH & Uhlir PF ''Database protection at the crossroads: recent developments and their impact on science and technology'' (1999) 14 *Berkeley Technology LJ* 793

Reichman JH & Franklin J ''Privately legislated intellectual property rights: the limits of article 2B of the UCC'' — paper delivered at the Berkeley

Rodhain, Philippe (2002), 'Reverse Doamin Name Hijacking', available at: *http://www.findlaw.com.au/articles/6596.htm*

Rutherford (2000), 'Well-known marks on the Internet', 12 *SA Mercantile Law Journal*, p 175

Ryan (2001), 'Playing by the rules', (5) *De Rebus*, p 27

Samuelson P ''Digital media and the changing face of intellectual property law'' (1990) 16 *Rutgers Computer & Technology LJ* 323

Samuelson P ''Licensing information in the global information market: freedom of contract meets public policy'' — paper delivered at the Seventh Annual Conference on International Intellectual Property Law and Policy (8–9 Apr 1999) in New York, US)

Sharrock, Lisa M (2001), 'The Future Of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions From Within The UDRP Framework', 51(2) Duke Law Journal, p 817

Smith GP ''Tear-open licences' are they enforceable in England?'' (1986) 2 *Computer Law and Practice* 128

Stern RH ''Shrink-wrap licences of mass marketed software: enforceable contracts or whistling in the dark?'' (1985) 11 *Rutgers Computer & Technology Law Journal* 51

Stone RL & Pernick JD ''Protecting databases: Copyright? We don't need no stinkin' copyright'' (1999) 16 *The Computer Lawyer* 17

Szafran E ''Regulatory issues raised by cryptography on the Internet'' (1998) 3(2) *Communications Law* 38

Van der Merwe ''Cybercontracts'' 6(4) *JBL* 138 Wendland W ''Dig that digital'' (1996) 4(2) 1996 *JBL* 49–50

Viljoen, Mariette (2007), 'In pursuit of the Cyberpirates The new ADR System for .co.za Domain Name Complaints', October *De Rebus* available at: *http://www.derebus.org.za/nxt/gateway.dll/bsxha/ibpxa/zsd2a/4sd2a/0ol3a*

Wilbers ''Online arbitration of electronic commerce disputes'' (1999) 27 *International Business Lawyer* 273

BOOKS

Bainbridge B *Software copyright law* 3 ed (1997)

Barlow JP ''Selling wine without bottles: the economy of mind on the global net'' in Brownlie *Principles of public international law* 4th ed (1990)

Buys R (ed) *Cyberlaw @ SA Law* (1999)

Christie *The law of contract in South Africa* 3 ed (1996)

Cornish *Intellectual property: patents, copyright, trade marks and allied rights* 4 ed (1999)

Dean OH *Handbook of South African copyright law* (1999 rev)

De Wet & Van Wyk *Kontraktereg en handelsreg* 5 ed (1992)

Forsyth CF &Bennet TW *Private international law* (1981)

Greenberg (2004), ''Trademarks, Domain Names And Meta Tags'' in Buys, R (ed.) *Cyberlaw @ SA The law of the Internet in South Africa*, (2nd ed.) (Pretoria: Van Schaik Publishers)

Gringras C *Nabarro Nathanson*: the laws of the Internet (1997)

Halberstam, Simon et al. (2002), *Tolley's Domain Names: A Practical Guide* (London: Tolley Publishing)

Hance O Dionne Balz S *Business and law on the Internet* (1996)

Hart RJ *Guide to intellectual property in the IT industry (1998)*

Institute for Information Law *IMPRIMATUR, contracts and copyright exemptions* (1998)

Hugenholtz B (ed) *The future of copyright in a digital environment* (1995)
Hughes T ''Intellectual property and browsing the Web'' in *Internet laws analogy, prospect media*
Joubert *General principles of the law of contract* (1987)
Kahn *Contract and mercantile law: a source book* 2 ed (1988)
Kerr *The principles of the law of contract* (1998)
Lai S *The copyright protection of computer software in the United Kingdom* (2000)
Lewis EAL *Legal ethics: a guide to professional conduct of South African attorneys* (1982)
Migga Kizza J *Ethical and social issues in the information age* (1998)
Motion, Paul (2005), ''Article 17 ECD: Encouragement of Alternative Dispute Resolution On-line Dispute Resolution: A View from Scotland'' in Edwards, L (ed.) *The New Legal Framework for E-commerce in Europe* (Oxford and Portland, Oregon: Hart Publishing)
Oppenheim *International aw* vol 1 9 ed (1992) Sharrock *Business transactions law* 2 ed (1998)
Pistorius, T (2008), ''Domain Names and Infringement of Trade Marks on the Internet'' in Van der Merwe (ed.) *Information Communications Technology Law* (Durban: LexisNexis)
Ramappa, T (2003), *Legal Issues in Electronic Commerce* (New Delhi: MacMillan India Ltd)
Samuelson P ''A case study on computer programs'' in *Global dimensions of intellectual property rights in science and technology* (1993)
Schlechtrien *Commentary on the UN Convention on the International Sale of Goods (CIGS)* (1998)
Singleton, Susan (2003), *eCommerce: A Practical Guide to the Law* (2nd Ed.) (Hampshire: Gower Publishing Ltd.)
Smith GJH *Internet law and regulation* (1996)
Symon S *Legal aspects of computer contacts from a user perspective* MBA dissertation Wits (1983)
Van der Merwe *Contract: general principles* (1994)
Webster & Page (2004), *South African Law of Trade Marks, Unlawful Competition, Company Names and Trading Styles* (4th Ed.) (Durban: Butterworth)
Wright *The law of electronic commerce, EDI, fax and e-mail: technology, proof, and liability* (1991)

CASE LAW

South Africa

A to Z Bazaars (Pty) Ltd v Minister of Agriculture 1975 (3) SA 468 (A)
Atari Inc v JB Radio Parts (Pty) Ltd (TPD) (case no 17419/83)
Aziza (Pty) Ltd v Aziza Media 2002 4 SA 337 C 396
Bergkelder Bpk v Shoprite Checkers (Pty) Ltd 2006 (4) SA 275 (SCA)
Bloom v The American Swiss Watch Co 1915 AD

Bok Clothing Manufacturers (Pty) Ltd v Lady Land Ltd 1982 2 SA 565 (C)
Bosal Africa (Pty) Ltd v Grapnel (Pty) Ltd 1985 (4) SA 882 (C)
Bremer Meulens (Edms) v Bpk v Floros 1966 (1) PH A36 (A)
Bress Designs (Pty) Ltd v GY Lounge Suite Manufacturers (Pty) Ltd, 1991 (2) SA 455 W
Cape Explosive Works Ltd v South African Oil and Fat Industries; Cape Explosive Works Ltd v Lever Brothers (South Africa) Ltd 1921 CPD
Cecil Jacobs (Pty) Ltd v Mcleod & Sons 1966 (4) SA 41 (N)
Collen v Rietfontein Engineering works 1948 (1) SA 413 (A)
Conradiev Rossouw 1919 AD 279
Crawley v R 1909 TS
Driftwood Properties (Pty) Ltd v McLean 1971 (3) SA 591 (A)
Hawker v Life Offices Association of South Africa 1987 (3) SA 777 (C)
Hawkins v Contract Design centre (Cape Divison) (Pty) Ltd 1983 (4) SA 296 (T)
Kerguelen Sealing and Whaling Co Ltd v Commissioner for Inland Revenue 1939 AD
Laugh It Off Promotions CC v SAB International (Finance) BV 2006 (1) SA 144 CC
Levben Products (Pvt) Ltd v Alexander Films (SA) (Pty) Ltd 1959 (3) SA 208 (SR)
Long John International Ltd v Stellenbosch Wine Trust (Pty) Ltd 1990 (4) SA 136 (D)
McKenzie v Van der Merwe 917 AD
Omega, Louis Brandt et Frere SA & another v African Textile Distributors 1982 (1) SA 951 (T)
R v Nel 1921 AD
R & I Laboratories (Pty) Ltd v Beauty Without Cruelty International (South African Branch) 1990 (3) SA 746 (C)
S v Henckert 1981 (3) SA 445 (A)
Smeiman v Volkersz 1954 (4) SA 170 (C)
Standard Bank of SA Ltd v Efroiken and Newman 1924 AD
Tel Bal v Van Staden 1902 TS
Tel Peda Investigation Bureau (Pty) Ltd v Van Zyl 1965 (4) SA 475 (E)
Waylite Diary CC v First National Bank Ltd 1995 (1) SA 645 (A)
Wolmer v Rees 1935 TPD 319
Yeats v Dalton 1938 EDL 177

Germany

Incassoprogramm (Federal Supreme Court 9 May 1985)

Netherlands

Church of Religious Technology v Dataweb BV, decision of the District Court of the Hague, 12 March 1996
Coss Holland BV v TM Data Nederland BV

United Kingdom

Beta v Adobe (1996) FSR
British Telecommunications Plc v One in a Million Ltd (1998) FSR 265
Carlill v Carbolic Smoke Ball Company [1893] 1 QB 256 (CA)
Entores Ltd v Miles Far East Corporation, (1955) 2 All ER 493 (CA)
Prince v Prince Sports Group 1998 FSR 2
Reddaway v Banham (1886) RPC 218, 224
Shetland Times v Wills and Zeine Ltd Sess Cas, 24 Oct 1996
Waterlow Publishers Ltd v Reed Information Services Ltd *(The Times, 11 Oct 1990)*
Waterlow Publishers Ltd v Rose (*The Times*, 8 Dec 1989)
World Wide Fund for Nature v World Wrestling Federation Entertainment Inc (Court of Appeal 27 February 2002, *Times Law Report* 12 March 2002

United States

Bensusan Rest. Corp. v King, 126 F.3d 25, 27 (2d Cir. 1997)
Feist Publications Inc v Rural Telephone Services Co (499 US 340 (1991)
Jeweler's Circular Publication Co v Keystone Publication Co 281 F 83 (2d Cir 1922)
Leon v Pacific Telephone & Telegraph Co 91 Fd 484 (9th Cir 1937)
National Basketball Association v Motorola Inc (105 F 3d 841 (2d Cir 1997))
Playboy Enterprises Inc v Frena 839 F.Supp.1552 (M.D. Fla 1993)
ProCD Inc v Zeidenberg (86 F 3d 1447 (7th Cir 1996))
Religious Technology Centre v Netcom On-Line Communication Services, Inc WL 707167 (N.D. Cal.1995
Sega Enterprises Limited v MAPHIA 857 F.Supp 679 (N.D. Cal 1994)
Sony Corp v Universal Studios Inc (464 US 417 (1984))
Warren Publishing Inc v Microdos Data Corp (115 F 3d 1509 (11th Cir 1997))

UDRP decisions

Telstra Corporation Limited v Nuclear Marshmallows D2000-0003
Mondich & American Wine Biscuits Inc v Brown D2000-0004Allocation Network GmbH v Steve Gregory D2000-0016
Barney's Inc v BNY Bulletin Board D2000-0059
Technologies Inc. v International Electronic Communications Inc *D2000-0270*
Sydney Opera House Trust v Trilynx Pty Ltd D2000-1224
CBS Broadcasting Inc v Dennis Toeppen D2000-0400
Revlon Consumer Products Corporation v Yoram Yosef aka Joe Goldman D2000-0468

Video Networks Limited v Larry Joe King D2000-0487
Jupiters Limited v Aaron Hall D2000-0574
Uitgeverij Crux V W Frederic Isler Skattedirektoratet v Eivind Nag D2000-0575
Asphalt Research Technology Inc v National Press & Publishing Inc D2000-1005
Amsec Enterprises LC v Sharon McCall D2000-1314
Smart Design LLC v Hughes D2000-0993
Nike Inc. v Azumano Travel D2000-1598
Recordati SPA v Domain Name Clearing Company D2000–194
Australian Trade Commission v Matthew Reader D2001-0083
Sydney Markets Ltd v Shell Information Systems D2001-0932
Cream Holdings Limited v National Internet Source Inc D2001-0964
Ladbroke Group Plc v Sonoma International LDC D2002-0131
Gorstew Limited v Worldwidewebsales.com D2002-0744
Sibyl Avery Jackson v Jan Teluch *D2002-1180*
Sustainable Forestry Management Limited v SFM.com and James M. van Johns ''Infa dot Net'' Web Services D2002-0535
Delta Sir Transport NV (trading as SN Brussels Airlines) v Theodule de Souza *D2003-0372*
Transfer Imperial College v Christophe Dessimoz D2004-0322
Kiwi European Holdings BV v Future Media Architects Inc D2004-0848
Hexagon v Xspect Solutions Inc D2005-0472
Jazeera Space Channel TV Station v AJ Publishing aka Aljazeera Publishing D2005-0309
Champagne Lanson v Development Services D2006-0006
Rohl LLC v ROHL SA D2006-0645
Proto Software Inc. v Vertical Axis Inc/PROTO.COM D2006-0905

Nominet DRS decisions

Cardpoint plc v Riga Industries DRS 00538
Loans.Co.Uk Ltd v Abbeyway Contracts Limited DRS01399
Nokia Corporation v Nokia Ringtones DRS01493
Nike International Limited v Robert Morrison DRS04601

National Arbitration Forum Decisions

Treeforms Inc v Cayne Industrial Sales Corp NAF 0095856
Energy Source Inc v Your Energy Source NAF 96364
Ultrafem Inc v Warren R Royal NAF 97682

Arbitration Forum decisions

Loblaws Inc v Presidentchoice.inc/Presidentchoice.com (eResolution June 7 2000) AF-0170a–0170c

.za ADR decisions

Mr. Plastic Mining and Promotional Goods v Mr Plastic CC ZA2007-0001 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0001.pdf>*

Telkom SA Ltd v Cool Ideas CC ZA2007-0003 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0003.pdf*

Telkom SA Limited v Customer Care Solutions (Pty) Ltd ZA2007-0004 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0004.pdf*

Telkom SA Ltd & TDS Directory Operations (Pty) Ltd v The Internet Corporation ZA2007-0005 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0005.pdf>*

Telkom SA Ltd & TDS Directory Operations (Pty) Ltd v The Internet Corporation ZAAP2007-0005 *http://www.domaindisputes.co.za/downloads/decisions/ZAAP2007-0005.pdf>*

Standard Bank of South Africa Ltd v Cox ZA2007-0006 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0009.pdf*

FIFA v X Yin ZA2007-0007 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0007.pdf>*

Homefront Trading 272 CC v Ian Ward ZA2007-0008 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0008.pdf*

Holistic Remedies (Pty) Ltd & Amka Pharmaceuticals (Pty) Ltd v Oxygen For Life (Pty) Ltd ZA2007-0009 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-0009.pdf>*

Multichoice Subscriber Management Services (Pty) Ltd v JP Botha

ZA2007-0010*http://www.domaindisputes.co.za/downloads/decisions/ZA2007-00010.pdf>*

Newcote International Limited v iLogic (Pty) Ltd ZA2007-00011 *http://www.domaindisputes.co.za/downloads/decisions/ZA2007-00011.pdf*

Automobiles Citroën v Mark Garrod ZA2008-00014 *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00014.pdf>*

Luxottia U.S. Holding Corporation v Preshal Iyar ZA2008-00015 *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00015.pdf>*

Aqua Divers International (Pty) Ltd v Divetek (Pty) Ltd ZA2008-00016 *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00016.pdf>*

Mxit Lifestyle (Pty) Ltd v Andre Steyn ZA2008-00020 *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00020.pdf>*

Sun International (IP) Ltd v Will Green ZA2008-00021 *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00021.pdf>*

Samsung Electronics Co. Ltd v Sean Elsworth ZA2008-00022

http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00015.pdf
Sun International South Africa Ltd. v Blue Chip Accommodation CC ZA2008-00023 *http://www.domaindisputes.co.za/downloads/decisions/ZA2008-00023.pdf*

LEGISLATION

Australia

Electronic Transactions Act 1999 (available at http://www.e-commerce@ag.gov.au)
Spam Act 129 of 2003
(available at http//www:spamlaws.com)

Canada

Evidence Act
Statute Revision Act (assented to on 13 Apr 2000)
Statutory Instruments Act
Uniform Electronic Commerce Act 1999 (available at http://www.law.ualberta.ca/alri/ulc/acts/eueca.htm)

Ontario

An Act with Respect to Electronic Information, Documents and Payments (Bill 70 2000) (short title:E-Commerce Act 2000)

European Union

Council Directive 91/250 of 14 May 1991, 1991 *Official Journal* (L 122) 42 (the ''Software Directive'')
Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data (Council Directive 95/46 of 24 Oct 1995, 1995 *Official Journal* (L 281) (the ''Privacy Directive'')
Council Directive 96/9 of 11 March 1996, 1996 *Official Journal* (L 77) 20 (''the Database Directive''))
Directive on the Protection of Consumers in Respect of Distance Contracts (*Official Journal* C288/1) (1997)
A Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market (18 Nov 1998)

Singapore

Electronic Transactions Act 25 of 1998

South Africa

ADR Regulations (Regulation Gazette 8587 of Government Gazette 29405 of 22 November 2006)
Close Corporations Act 69 of 1984
Computer Evidence Act 57 0f 1983
Department of Communications Discussion paper on the estab-

lishment of an independent Domain Name Authority (1999) *http://www.ecomm-debate.co.za*
Discussion Paper on Electronic Commerce (Jul 1999)
Electronic Communications and Transactions Act 25 of 2002
Green Paper on E-Commerce ''Making it your business'' (available online at: <http://www.ecomm-debate.co.za>)
Trade Marks Act 194 of 1993
Zadna Policies and procedures for the .za name space (2006) *www.zadna.org.za/policy/za.policy.and.procedures.20070802-GM.pdf*

United Nations

Commission on International Trade Law
UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

United States

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) (available at http://www.spamlaws.com)
Uniform Commercial Code (UCC)
Uniform Electronic Transactions Act (''the UETA'' (4 Aug 1999 draft), adopted by the US National Conference of Commissioners on Uniform State Laws (UNCCUSL) at its Annual Conference Meeting in its One-Hundred-And-Eighth Year (23-30 Jul 1999) Denver (Col)
White Paper on Intellectual Property and the National Information Infrastructure (Sept 1995)

Illinois

Electronic Commerce Security Act

Utah

Digital Signature Act of 1998

World Intellectual Property Organization

WIPO Arbitration and Mediation Centre *Wipo Overview of WIPO Panel Views on Selected UDRP Questions http://arbiter.wipo.int/domains/search/overview/index.html*