The Electronic Communications and Transactions Act

Shumani L. Gereda[1]

[1] The author would like to extend his gratitude to Lisa Thornton for affording him the opportunity to be part of this project, and also thanks Advocate Patrick Mtshaulana for commenting on the chapter.

Introduction

A new communications revolution has created, and continues to create, a new economic and democratic landscape. Societies around the globe are drawing closer to each other and integrating into the global economy through electronic communication. This communications revolution has fundamentally changed the way the world operates.

However, the changes have happened so fast that their character and implications are neither clear nor well understood. People are buying and selling goods and services online, either directly or with the help of electronic agents. Businesses are increasingly doing business online and new forms of commercial cooperation are emerging. These transactions either have brought about or may bring about legal consequences for the parties involved as well as for third parties such as online intermediaries and Internet Service Providers (ISPs).

Conventional legal frameworks governing the offline world are proving to be inadequate in the online world. Therefore, it has become imperative for national governments to have in place a clear policy framework for this rapidly developing sector. It was for this and other related reasons, that the Minister of Communications commissioned a due diligence survey aimed at identifying laws that could constitute barriers to the development of electronic commerce (e-commerce).

The due diligence Report on E-commerce Legal Issues, prepared by a Johannesburg firm of attorneys, led to the launch of the Discussion Paper on Electronic Commerce in July 1999.[2] The report recommended, amongst other things, that the UNCITRAL Model Law on Electronic Commerce form the basis for introducing primary legislation on commercial transacting.[3] The Green Paper on Electronic Commerce followed in November 2000, which in turn led to the Electronic Communications and Transactions Act, 25 of 2002 (the ECT Act).[4]

The ECT Act regulates all forms of electronic communications in South Africa, but whether it facilitates electronic communications has hitherto been unclear. This chapter aims to investigate whether the ECT Act facilitates electronic communications. In so doing, it focuses on:

- A comparative analysis of international instruments that influenced the ECT Act, that is, the UNCITRAL Model Law on E-commerce, the OECD Guidelines on E-commerce, and the European Union Policy Directive on E-commerce;
- The background and overview of the ECT Act, as well as the outstanding provisions of the ECT Act;
- The electronic communication legislation of selected foreign countries, in particular the United States of America (US), Australia, the United Kingdom, and Canada; and
- A comparison of all of the foreign legislation dealt with as well as the international instruments vis-à-vis the ECT Act.

[2] Department of Communications *Discussion Paper on Electronic Commerce* (July 1999). (The Discussion Paper was launched with a specialised website: http://docweb.pwv.gov.za/Ecomm-Debate/myweb/docs/discuss01.html [07 September 2003].
[3] T James *An Information Policy Handbook for Southern Africa — A Knowledge Base for Decision-Makers* (IDRC, 2001) 147.
[4] GG 23708 dated 2 August 2002.

The conclusion of this chapter is that, comparatively speaking, the ECT Act does have the potential to facilitate the use of electronic communication.

1. INTERNATIONAL REGULATION OF ELECTRONIC COMMUNICATIONS

There are international guiding instruments that many states consult in developing their own appropriate state laws, such as the United Nations Commission on International Trade Law's Model Law on Electronic Commerce of 16 December 1996 (The Model Law)[5] and the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (The Guidelines). The United Nations General Assembly established the United Nations Commission on International Trade Law (Commission) in 1966 by resolution 2205(XXI) of 17 December 1966.[6]

During 2003, the commission increased its membership from 36 to 60.[7] It has established six working groups composed of all member states of the Commission. Working Group IV on e-commerce is responsible for the Model Law and the overall development of e-commerce relating to international trade.[8]

1.1. The Model Law

On 16 December 1996, the United Nations General Assembly passed a resolution that led to the adoption of the Model Law. The General Assembly stated that:

Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, which involve the use of alternatives to paper-based methods of communication and storage of information ...

Recommends that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information . . .[9]

The aim of the Model Law is to provide national legislatures with a template of internationally acceptable rules to remove legal obstacles and create a more secure legal environment for electronic commerce. The Model Law intends to facilitate the use of electronic communications by encouraging the international harmonisation of domestic legal rules for electronic communications.

Article 2 of the Model Law defines the originator of a data message as 'a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any; but it does not include a person acting as an intermediary with respect to that data message'. Article 2 of the Model Law further defines the addressee of a data message as a person who is intended by the

[5] The General Assembly Resolution 51/162 of 16 December 1996: Uncitral Model Law on Electronic Commerce in *United Nations Commission on International Trade Law (UNCITRAL) Status of Conventions and Model Laws*; available at http://www.uncitral.org/en-index.htm.

[6] General Assembly Resolution 2205(XXI) of 17 December 1966; available at http://www.uncitral.org/en-index.htm.

[7] Statement by Dr M Gandhi, Counsellor & legal adviser on agenda item 151: Report of the United Nations Commission on International Trade Law on the work of its thirty-sixth session at sixth committee of 58th Unga on 6 October 2003; available at http://secint04.un.org/india/ind809.htm.

[8] UNCITRAL Working Groups. The structure of the Working Groups and their responsibilities are provided in the UNCITRAL website at http://www.uncitral.org/en-index.htm.

[9] The General Assembly Resolution 51/162 of 16 December 1996: UNCITRAL Model Law on Electronic Commerce. The resolution is available online at http://www.uncitral.org/en-index.htm.

originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message.

1.2 The Model Law on e-Signatures

In 2001, the Commission adopted the Model Law on Electronic-Signatures with the intention of bringing additional legal certainty regarding the use of e-signatures.[10] The Model Law on e-signatures is built on the flexible principle contained in article 7 of the Model Law, which establishes a presumption that, where they meet certain criteria of technical reliability, electronic signatures shall be treated as equivalent to handwritten signatures. The Model Law on Electronic-Signatures applies where e-signatures are used in the context of commercial activities, without overriding any rule of law intended for the protection of consumers.[11]

1.3 The Organisation for Economic Co-operation and Development (OECD)

The OECD succeeded the Organisation for European Economic Co-operation (the OEEC), which was formed to administer American and Canadian aid under the Marshall Plan for the reconstruction of Europe after the Second World War. Since it took over from the OEEC in 1961, the OECD has set out to build strong economies in its member countries. In recent years, the OECD has moved beyond a focus on its member countries to offer its analytical expertise and accumulated experience to developing market economies.[12]

The OECD has 30 members and currently involves in its work approximately 70 non-member countries. These non-members subscribe to OECD agreements and treaties. The affiliation with 70 non-member countries gives the OECD a global reach.[13]

South Africa is one of the 70 non-members that maintain an active association with the OECD.[14] South Africa, like many other non-member countries, both from emerging market and developing economies, participates in the OECD's conferences and seminars. The OECD has several committees that deal with various issues. One of the committees is the Committee on Consumer Policy (CCP). The CCP developed the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (The Guidelines). The Guidelines set out the core characteristics for effective consumer protection for online business-to-consumer (B2C) transactions.

The Guidelines approved on 9 December 1999 are designed to help ensure that consumers are no less protected when shopping online than they are when they buy from their local store or order from a catalogue.[15] By setting out the core characteristics of effective consumer protection for online B2C transactions, the

[10] United Nations *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001* (2002); available at: http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.
[11] Ibid.
[12] OECD *Overview of the OECD: What is it? History? Who does what? Structure of the organisation? The OECD in 15 slides - PowerPoint Presentation (24 January 2003)*; available at http://www.oecd.org/document/18/0,2340,en_2649_201185_2068050_1_1_1_1,00.html.
[13] Overview of the OECD (note 12 above).
[14] South Africa is a non-member of the OECD. For more information, visit the OECD Website at Overview of the OECD (note 12 above).
[15] Ibid.

Guidelines are intended to help eliminate some of the uncertainties that both consumers and businesses encounter when buying and selling online.[16]

The Guidelines are expected to play a major role in assisting governments, business and consumer representatives with developing and implementing online consumer protection mechanisms without erecting barriers to trade. It is important to note that the OECD decisions and recommendations are as applicable to members as they are to non-members who contract electronically with members of the OECD. For this reason, the Guidelines have an effect on South Africa's conduct of its e-commerce transactions with OECD member countries. Non-compliance with the Guidelines might lead to South Africa's exclusion from certain e-commerce-related business relations with OECD member countries. The consumer protection provisions of the ECT Act (discussed below) reflect the OECDs core characteristics of effective consumer protection for online B2C transactions.[17]

1.4 The EU Directives on e-Commerce

The concept of the EU was conceived after the Second World War, when the process of European integration was launched on 9 May 1950, with six countries joining from the very beginning. The EU was created in 1993 with the aim of achieving closer economic and political union between member states of the European community. Today the EU has 15 member states, ten acceding states and three candidate countries.[18]

The EU is run by five institutions, each playing a specific role: the European Parliament; the Council of the Union; the European Council (the EC); the Court of Justice and the Court of Auditors. The European Parliament is the assembly of the EU. The EC is the executive body and driving force of the EU, formed in 1967; it initiates legislation, administers funds and ensures that union laws are enforced.[19]

While national law and EU laws are mutually dependent, EU law is an independent legal system that takes precedence over national law. The EU law is composed of three different types of legislation, ie primary legislation, secondary legislation and case law. Primary legislation includes treaties and other agreements having similar status, agreed upon by direct negotiation between member states. Secondary legislation comprises, amongst other things, directives. Directives bind member states to the objectives to be achieved within a certain limit while leaving the national authorities the choice of form and means to be used. Directives have to be implemented in national legislation in accordance with the procedures of the individual member states.

Directives are essentially instructions to the member states to introduce legislation. They indicate the goals to be achieved without laying down the manner of achieving these goals. In general, enforcement measures and remedies are left to the member states.

On 17 July 2000, the European Parliament passed Directive 2000/31/EC on

[16] Overview of the OECD (note 12 above).
[17] Chapter VII of the Electronic Communications and Transactions Act (ECT Act), 25 of 2002.
[18] European Union Member States. This information is available online at http://www.eurunion.org/states/home.htm.
[19] The commission is answerable to the European Parliament, which has the power to dismiss it by a vote of censure or no confidence. The commission attends all sessions of the European Parliament and must explain and justify its policies if so requested by members of the house. The European Community's core objective of achieving European unification is based exclusively on the rule of law.

certain legal aspects of information society services (the EU Directive).[20] The objective of the EU Directive is to establish a harmonised regulatory framework for electronic communication networks and services across the EU.

In terms of the provisions in article 5 of the EU Directive, member states must lay down in their legislation that information society services must render certain information easily accessible, in a direct and permanent manner, to their recipients and competent authorities, eg the name of the service provider and the address at which the service provider is established. This provision is similar to the consumer protection provisions in section 43 of the ECT Act. The comparison between the EU Directive and the ECT Act is discussed fully below.

The EU Directive does not apply to services supplied by service providers established in a third country (ie outside the EU Community). Article 25 of the Principles of the EU Directive, which deals with the transfer of personal data to third countries, provides that:

> (1) Member states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection . . . [21]

To the extent that it does business with EU member states, South Africa is affected by these provisions. It is therefore expected of South Africa to comply, albeit indirectly, with the EU Directive whenever a South African business transacts with a subject (or business establishment) that originates from an EU member state. The only qualified exception is that provided for in article 26 of the EU Directive's principles. Article 26 provides that: by way of derogation from article 25 and save where otherwise provided for by domestic law governing particular cases, member states shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of article 25(2) may take place on condition that the data subject has given his consent unambiguously to the proposed transfer.[22]

The EU Directive on Data Protection came into effect in October 1998 (Data Protection Directive). Its main aim is to prohibit the transfer of personal data to non-EU nations that do not meet the European 'adequacy' standard for privacy protection. While the US and the EU share a common goal of enhancing privacy protection for their citizens, the US has adopted a different approach to privacy from that taken by the EU. Because of these different privacy approaches, the Directive could have significantly hampered the ability of US companies to engage in many trans-Atlantic transactions.

In order to bridge these different privacy approaches and provide a streamlined means for US organisations to comply with the Directive, the US Department of

[20] Directive 2000/31/EC of the European Parliament and of the council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce) in *Official Journal of the European Communities* L178/1 (17 July 2000).

[21] Data Protection Directive 95/46/EC of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data in *Official Journal of the European Communities* L281 (23 November 1995).

[22] Ibid.

Commerce, in consultation with the EC, developed a 'safe harbor' framework.[23] On 26 July 2000, the EC adopted a decision on the adequacy of the level of data protection in the US with the Data Protection Directive. The decision entered into force on 1 November 2000.

The safe harbor framework provides for certain principles to which organisations must adhere in order to become members. South African organisations and businesses that have subsidiaries or branches in the US are indirectly affected, to the extent that their subsidiaries conduct business transactions with any of the 15 EU member states.

The US Federal Trade Commission (FTC) has established the safe harbor guidelines for its private-sector organisations that are affected. Joining the safe harbor is voluntary to US organisations of all sectors. However, organisations that fall under the auspices of the FTC and undertake to adhere to the safe harbor principles are penalised when they fail to do so. Therefore, South African companies that conduct business with organisations in EU member states through US organisations that are subject to the FTC jurisdiction and have undertaken to comply with the safe harbor principles are required to comply with these principles.[24]

2. THE ECT ACT

The ECT Act was promulgated on 2 August 2002 and came into force on 30 August 2002. The main objective of the ECT Act is 'to enable and facilitate electronic communications and transactions in the public interest'.[25] 'Electronic communications' is defined in the ECT Act as 'a communication by means of data messages'. In addition, 'data' is defined as 'electronic representations of information in any form'. 'Transaction' is defined as 'a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services'.[26] The ECT Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages.
The aims of the ECT Act, as provided for in section 2(1) are, inter alia:

- to remove barriers to electronic communications and transactions in the Republic;
- to promote legal certainty and confidence in respect of electronic communications and transactions;
- to promote technology neutrality in the application of legislation to electronic communications and transactions; and
- to ensure that electronic transactions in the Republic conform to the highest international standards.

2.1 National e-Strategy

Section 5 of the ECT Act requires the Minister to develop a three-year national e-strategy for the Republic of South Africa by 31 July 2004. This national e-strategy

[23] US Department of Commerce *Safe Harbor Overview*; available at http://www.export.gov/safeharbor/sh_overview.html.
[24] Federal Trade Commission *TRUSTe Earns 'Safe Harbor' Status*; available at http://www.ftc.gov/opa/2001/05/truste.htm.
[25] s 2(1) of the ECT Act.
[26] s 1 of the ECT Act.

must be submitted to Cabinet for approval. On acceptance of the national e-strategy, the Cabinet must declare its implementation a national priority.

The Minister is further required to invite comments from all interested parties by way of notice in the Gazette and consider any comments received, prior to prescribing the determined subject matters to be addressed in the national e-strategy and the principles that must govern its implementation.[27] Section 6 of the ECT Act requires that the national e-strategy must outline strategies and programmes to, inter alia, provide Internet connectivity to disadvantaged communities. Section 9 of the ECT Act provides that the Minister must, in consultation with the Minister of Trade and Industry, evaluate the adequacy of any existing processes, programmes and infrastructure providing for the use by SMMEs of electronic transactions.

2.2 Electronic Transactions Policy

Section 10 of the ECT Act provides that the Minister must, subject to this Act, formulate an electronic transactions policy in consultation with members of the Cabinet directly affected by such policy formulation or the consequences of it.

2.3 Legal recognition of data messages

Section 11(1) of the ECT Act provides that 'information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message'. Data messages are given the same legal status as information generated conventionally on paper. 'Data message' is defined as data generated, sent, received or stored by electronic means and includes voice where the voice is used in an automated transaction and a stored record.[28] An example of automated transactions where voice is used can be a contract entered into telephonically by a consumer as defined in the ECT Act with an automated voice answering machine.

In terms of section 11(3) of the Act, information can be incorporated by reference, provided that such information is referred to in a way in which a reasonable person would notice such reference and incorporation and provided further that such information is accessible in a form in which it may be retrievable and stored.[29]

It can therefore be reasonably assumed that the requirements of section 171 of the Companies Act that every business letter or trade circular, that the company sends or issues to any person in the Republic should state, thereon or therein in a retrievable form, the names of all the directors, are satisfied by mere compliance with this section.[30]

---

[27] Upon approval by the Cabinet, the Minister must publish the national e-strategy, as well any subsequent material revision of the national e-strategy, in the Gazette. s 5(9) of the ECT Act prohibits the Minister from amending or adapting the national e-strategy without the approval of the Cabinet. Without approval by the Cabinet, such amendment or adaptation will be ineffective. s 5(4)(c) of the ECT Act provides that the national e-strategy must, inter alia, 'set out . . . existing government initiatives directly or indirectly relevant to or impacting on the national e-strategy and, if applicable, how such initiatives are to be utilised in attaining the objectives of the national e-strategy.'

[28] s 1 of the ECT Act.

[29] s 11(3) of the ECT Act provides that:

> (3) Information incorporated into an agreement and that is not in the public domain 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.

[30] s 171 of the Companies Act, 61 of 1973 provides that:

> (1) A company shall not issue or send, irrespective of whether it is in electronic or any other format, to any person in the Republic

2.3.1 'In writing'

Section 12(a) and (b) of the ECT Act provides that:

> 'A requirement in law that a document or information must be in writing is met if the document or information is in the form of a data message; and accessible in a manner usable for subsequent reference.'

The legal requirement that a document or information must be 'in writing' will now be satisfied if the document or information is in electronic format. However, the document or information concerned must also be accessible in such a manner that the person retrieving it would be able to use it afterwards. Generally, all documents and agreements that previously had to be in writing can be generated electronically, except the following:

- Agreements for the sale of immovable property;
- A long term lease of immovable property for 20 years or more;
- The execution, retention and presentation of a will or codicil;
- The execution of a bill of exchange; and
- Documents or agreements, which by agreement between the parties may not be generated electronically.

The ECT Act does not compel anyone to use or receive information in electronic form, nor does it prohibit anyone specifying requirements for the manner in which they will accept data messages. The ECT Act may therefore not discriminate between papers and electronic documents. Effectively, the ECT Act does not create new ways of doing business; it only facilitates and gives legal recognition to the new ways of doing business that are emerging through the evolution of technology.

2.3.2. Signature

Section 13 of the ECT Act provides that:

> (1) 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.
> (2) Subject to subsection (1), an electronic signature is not without legal force and effect merely because it is in electronic form.

The effect of this section is to give legal recognition to electronic signatures. However, where the law requires a signature, only an advanced signature shall be used. It should be noted that an advanced electronic signature is an electronic signature that can be authenticated only by an agency that has been accredited by

---

any trade catalogue, trade circular or business letter bearing the company's name unless there is stated thereon or therein in a form capable of retrieving therefrom in respect of every director-
(a) his present forenames, or the initials thereof, and present surname;
(b) any former forenames and surnames not being those referred to in section 215(3);
(c) his nationality, if not South African.
(2) Any company which fails to comply with any provision of subsection (1), shall be guilty of an offence.

the Department of Communications (DoC) in terms of section 37 of the ECT Act.[31]

The ECT Act further provides that, where contracting parties failed or neglected to agree on the electronic signature to be used, the presumption is that the requirement of a signature is met if a method is used to identify the person (who has purportedly 'signed' the electronic communication) and to indicate such person's approval of the message. Such an expression of intent can be made by any means from which such person's intent can be inferred.[32]

2.3.3 Original

Section 14(1)(a) and (b) provides that:

> Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if — the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and that information is capable of being displayed or produced to the person to whom it is to be presented.

For purposes of this provision, it should be noted that a computer printout of an 'original' electronic document does not constitute an original. An original message remains in electronic form, and it is the first generated copy by the sender or an agent of the sender.

2.3.4 Evidential weight of data messages

Section 15 of the ECT Act provides that:

(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence — on the mere grounds that it is constituted by a data message; or if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

E-mail messages will therefore have an evidential weight in both civil and criminal proceedings. This is particularly important for employer — employee relations when the relationship terminates. Archived e-mail messages may come in useful as evidence for either the employer or the employee in workplace-related disputes.

[31] s 37(1) of the ECT Act provides that: 'The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.'
[32] s 13 of the ECT Act.

2.3.5 Retention

Section 16(1) of the ECT Act provides that 'where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message...'

Information can now be retained electronically, provided it is retained in the format in which it was generated, sent or received; or in the format that can be demonstrated to represent accurately the information generated, sent or received. This provision would undoubtedly make retention easier for those institutions required to keep records, either by virtue of the nature of their business or by law, for example, in accordance with the Promotion of Access to Information Act.[33]

2.3.6 Production of document or information

Section 17 of the ECT Act provides that, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if certain other requirements, including the integrity of the information, are met.

2.3.7 Notarisation, acknowledgement and certification

Section 18 provides that:

(1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message...

In terms of Section 18 of the ECT Act, a Commissioner of Oaths can sign a document by way of an advanced electronic signature. The effect of this is that an agreement that previously required the stamp of a notary can now be concluded, signed and notarised electronically. Section 19 provides, inter alia, that 'a requirement in law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single data message that is capable of being reproduced by that addressee'.[34]

2.3.8 Automated transactions

Section 20 of the ECT Act introduces the concept of an 'automated transaction' which is an electronic transaction conducted or performed by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person.

---

[33] s 50 of the Promotion of Access to Information Act, 2 of 2000.

[34] s 19 of the ECT Act further provides that:

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.

2.3.9 Formation and validity of agreements

Section 22 of the ECT Act provides that:

(1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.
(2) 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.

2.3.10 Time and place of communications, dispatch and receipt

In terms of section 23(a) of the ECT Act, there is a presumption that a data message has been sent when it enters an information system outside the control of the originator. If the originator and addressee are using the same information system, the presumption is that the message has been sent when it is capable of being retrieved by the addressee. Section 23(b) further 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 and used for that purpose by the addressee and is capable of being retrieved and processed by the addressee.
An electronic transaction is deemed to have been concluded at the time when and the place where the acceptance of the offer is received by the offeror. The ECT Act also introduces a further deeming provision that an acknowledgement of receipt of a data message is not necessary to give effect to that message.[35] This deeming provision could have negative implications; for example, an online supplier can claim that an order submitted by the buyer is binding on the buyer notwithstanding that the buyer never received the order. However, these deeming provisions apply only if parties to an agreement have not agreed otherwise.

2.3.11 Expression of intent or other statement

Section 24 of the ECT Act provides that, as between the originator and the addressee of a data message, an expression of intent or other statement is not without legal force and effect merely on the grounds that:

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

2.3.12. Attribution of data message to originator

Section 25 of the ECT Act provides that a data message is that of the originator if it was sent by -

(a) the originator personally;
(b) a person who had authority to act on behalf of the originator in respect of

[35] s 26 of the ECT Act.

that data message; or

(c) An information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

The ECT Act recognises, for example, that an agreement may be concluded with either party using an electronic agent. None the less, a party using an electronic agent to conclude an agreement is not bound if the terms of the agreement were not capable of being reviewed by a natural person representing that party prior to formation of the agreement.

2.4 e-Government services

Section 27 of the ECT Act provides that any public body that, pursuant to any law, inter alia, 'accepts the filing of documents, or requires that documents be created or retained . . . may, notwithstanding anything to the contrary in such law, accept the filing of such documents, or the creation or retention of such documents in the form of data messages; ...'

One notable practical effect of this requirement is that Court papers can now be filed with the Registrar or clerk of the Court by electronic means.

Section 28 of the ECT Act provides that in any case where a public body performs any of the functions referred to in section 27, such body may specify by notice in the Gazette, inter alia,

(a) the manner and format in which the data messages must be filed, created, retained or issued . . .

(d) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message or that such authentication service provider must be a preferred authentication service provider.

Section 28(2) provides that, for the purposes of subsection (1)(d), the South African Post Office Limited is a preferred authentication service provider and the Minister may designate any other authentication service provider as a preferred authentication service provider based on such authentication service provider's obligations in respect of the provision of universal access.

2.5 Cryptography providers

The development and growth of electronic commerce relies primarily on building the confidence of the consumer, business and government in the e-commerce environment. In order to provide a stable environment for conducting business online, consumer protection becomes critical. The reason is that, while the new environment provides new opportunities for business, it also brings new types of threats in the form of, for example, electronic fraud, cyber crime and forms of

[36] Vivienne A Lawack-Davids 'The cryptographic dilemma: possible approaches to formulating policy in South Africa' Local Academic Papers Commissioned by the Department of Communications; available at http://www.ecomm-debate.co.za.

cyber terrorism. Security of information becomes the backbone of conducting business online.[36]

Cryptography implies security online, to ensure consumers' and businesses' confidence in electronic commerce. Cryptography is also referred to as encryption. Encryption is a special mathematical formula or algorithm through which a message is transformed from the original or understandable text into a not understandable or illegible text.[37]

A widely used method of encryption is secret key cryptography, by which both the sender and the recipient of a message share the same secret key used in conjunction with an algorithm to both encrypt and decrypt the message. Unlike secret key cryptography, which uses one key, public key cryptography uses two paired keys.[38] The ECT Act seeks to regulate the use of public key cryptography by making provision for authentication infrastructures. The risk with public key cryptography is that a third party might intercept the other key before it reaches the intended receiver.

Cryptography providers have to be registered by the Director-General of the DoC in terms of section 30 of the ECT Act. In terms of section 29(3), a cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography services or products, except to government agencies such as cyber inspectors.[39]

Section 31 of the ECT Act prohibits the disclosure of information contained in the register provided for in section 29, to any person other than to employees of the Department who are responsible for the keeping of the register, except to government agencies responsible for safety and security or criminal investigations in the Republic, or to cyber inspector, pursuant to section 11 or 30 of the Promotion of Access to Information Act; or for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

2.6 Authentication service providers

Authentication can be defined as an assurance of the originality or authenticity and integrity of an electronic message. It serves to secure the identities of the parties to a transaction. To communicate securely, you need a way to verify the identity of the party or parties with whom you communicate. This is necessary to avoid revealing otherwise confidential information to impostors. In terms of chapter VI of the ECT Act, only an authorised or accredited authentication service provider (ASP) can provide digital signatures. It is widely believed that digital signatures are one of the primary ways in which public key cryptography can be used to make electronic communications safer.

The ECT Act appoints, in terms of section 28(2), the South African Post Office (SAPO) as a preferred authentication service provider. This is probably because of the public service that the SAPO already provides, as well as its ties with the

[37] S Andrews 'Who holds the key? A comparative study of US and European encryption policies' 29 February 2000 (2) *The Journal of Information, Law and Technology* Introduction para 1.

[38] Lawack-Davids (note 37 above).

[39] In terms of s 30(3) of the ECT Act, a cryptography service or cryptography product is regarded as being provided in the Republic if it is provided:

- from premises in the Republic;
- to a person who is present in the Republic when that person makes use of the service or product; or
- with regard to a business carried on in the Republic.

government as a 'parastatal'. Moreover, SAPO is in a good position to implement universal service through its widespread administrative centres. Still, the accreditation authority, that is, the Minister, must first accredit the SAPO in terms of the regulations published pursuant to section 41 of the ECT Act.

Section 33 of the Act defines 'accreditation' as recognition of an authentication product or service by the accreditation authority. Section 34 (1) provides that, for the purposes of this chapter, the director-general must act as the accreditation authority. Section 37 provides that the accreditation authority may accredit authentication products and services in support of advanced electronic signatures. In terms of section 37(3), a person falsely holding out its products or services to be accredited by the accreditation authority is guilty of an offence.[40]

Section 38(1) provides that the accreditation authority may not accredit authentication products or services unless the accreditation authority is satisfied that an electronic signature to which such authentication products or services relate satisfies the requirements listed under that section. Section 38(2) prescribes factors that the accreditation authority must have regard to prior to accrediting authentication products or services.

Section 39 of the ECT Act provides that the accreditation authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40. However, subject to the provisions of subsection (3), the accreditation authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1) unless it has given the authentication service provider a fair hearing.[41]

2.7 Consumer Protection

Section 1 of the ECT Act defines 'consumer' as any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier. Section 42 of the ECT Act provides that the consumer protection provision apply only to electronic transactions. In terms of section 42(3), the consumer protection chapter does not apply to a regulatory authority established in terms of a law, if that law prescribes consumer protection provisions in respect of electronic transactions.

Section 43 of the ECT Act provides that a supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make information listed under this section available to consumers on the website where such goods or services are offered. Such suppliers must, for example, provide their full details (i.e. full name, legal status, physical address, telephone numbers, e-mail address, physical address where they would receive legal service of documents (an impressive improvement on the conventional terminology of 'Domicilium citandi

[40] s 40 of the ECT Act provides that the Minister may, by notice in the Gazette and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.

[41] s 39(3) of the ECT Act provides that the accreditation authority may suspend accreditation granted under s 38 or recognition given under s 40 with immediate effect for a period not exceeding 90 days, pending implementation of the procedures required by subsection (2), if the continued accreditation or recognition of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in the Republic.

et executandi')) and generally a sufficient description of the goods/services so that a potential purchaser can make an informed decision about a potential purchase and the price of the goods/services.

Section 43(2) requires the supplier to provide a consumer with an opportunity:

(a) to review the entire electronic transaction;
(b) to correct any mistakes; and
(c) to withdraw from the transaction, before finally placing any order.

Section 43(3) provides that if a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

Section 43(5) requires the supplier of goods or services to utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned. In terms of section 43(6), the supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5). It can only be assumed that this is an objective test determined by the types of technological security standards available in the particular industry at a given time.

Section 44(1) provides that a consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply of goods within seven days after the date of the receipt of the goods, or after the conclusion of the agreement. Sections 44(2) and (3) provides that the only charge that may be levied on the consumer is the direct cost of returning the goods; and, further, that if payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund must be made within 30 days of the date of cancellation. However, it should be noted that section 44 does not apply to electronic transactions listed under section 42(2).

Section 45 of the ECT Act provides that any person who sends unsolicited commercial communications to consumers, generally and commonly referred to as 'spam', must provide the consumer -

(a) with the option to cancel his or her subscription to the mailing list of that person; and
(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

Section 45(2) further provides that no agreement is concluded where a consumer has failed to respond to an unsolicited communication. Section 45(4) provides that any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are not welcome is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1). It must be noted, however, that section 45(1) makes it clear that what is prohibited is not spam per se. Senders of spam are required to give the recipient of the spam the option to remove his or her subscription from the spammer's mailing list.

It is important to note, further, that the ECT Act does not provide for the absolute prohibition of the sending of commercial spam, let alone ordinary spam. It only prohibits the continuous sending of commercial spam despite a recipient or recipients' request to have their e-mail addresses removed from a 'spammer's' mailing list.[42] For both consumers and ISPs, this is not good enough. ISPs particularly are in an unfortunate position in that they stand to lose from the sending of one 'lawful' spam. ISPs serve thousands of individuals who are legally enjoined to tolerate at least one spam, before they can request to be removed from the spammer's mailing list. In terms of section 45 as it stands, it is lawful for retail stores and cell phone service providers to send unsolicited advertising SMSs to their customers, unless and until the consumer lodges a complaint. The implementation of the penalty provision also remains curious. International case law shows that regulating and fighting spam is necessary but not an easy task.[43]

In terms of section 46 of the Act, the supplier must execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise. Failure by the supplier entitles the consumer to cancel the agreement with seven days' written notice, in terms of section 46(2). Section 47 of the ECT Act provides that the protection provided to consumers in this chapter applies irrespective of the legal system applicable to the agreement in question. Therefore, even foreign suppliers will be required to comply with these requirements.

Section 48 further provides that any provision in an agreement that excludes any rights provided for in this chapter is invalid. In terms of the latter section, the consumer protection provisions cannot be contracted out, that is, parties cannot agree to exclude these provisions. In terms of section 49 of the ECT Act a consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of this chapter by a supplier. The ECT Act defines the Consumer Affairs Committee as a committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act, 71 of 1988.

2.8 Protection of personal information

Section 50(1) provides that the chapter on the protection of personal information applies only to personal information that has been obtained through electronic transactions. Subsection (2) provides that a data controller may voluntarily subscribe to the principles outlined in section 51 by recording such fact in any agreement with a data subject. However, a data controller who chooses to subscribe to the listed principles must subscribe to all the principles and not merely to parts of them.

Section 50(4) provides that the rights and obligations of the parties in respect of the breach of the principles outlined in section 51 are governed by the terms of any agreement between them. Section 51 lists the nine principles that a data controller must comply with, for example, section 51(4) provides that the data controller may not use the personal information for any other purpose than the disclosed purpose

[42] See G Ebersohn 'The unfair business practices of spamming and spoofing' July 2003 *De Rebus* and S Gereda 'The truth about spam' September 2003 *De Rebus*.

[43] *Ferguson v Friend Finders*, Inc 94 Cal App 4th 1255, 115 Cal Rptr 2d 258 (Cal App 1st Dist 2 January 2002), review denied (10 April 2002). *CompuServe Inc v Cyber Promotions*, AOL v Cyber Promotions 1997, *America Online v Over the Air Equipment, Inc* (1997).

without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

2.9 Limitation of service provider liability

Sections 70-79 of the ECT Act provide for the limitation of liability of service providers. The ECT Act limits the liability of service providers against their customers' liability arising from the services given by these providers. For example, ISPs are therefore protected against liability arising from individuals and entities to which they provide service and who or which send unsolicited commercial e-mails.

Section 73, in particular, provides that because service providers are merely conduits for the transmission of information or merely provide facilities for information systems, they cannot be held liable for, amongst other things, providing access to or operating facilities for information systems or transmission of data messages. This limitation is, however, subject to certain exceptions and applies only to service providers who adhere to certain requirements, namely, if the service provider becomes a member of an industry representative body for service providers as recognised by the Minister. Furthermore, services providers who render hosting services will be entitled to enjoy the limitation of liability provisions only if they have designated an agent to receive notifications of infringement of data stored by them and have made the name of the agent publicly available.[44]

2.10 Critical Databases

The ECT Act introduces the concept of critical databases. The Minister will determine the requirements and procedure for registering of these databases. The Minister is also empowered to designate critical databases in both the public and the private sector. Effectively, this provision means that if the Minister believes that 'Siyakhasonke Bank's database contains information that may be harmful to the welfare of the State, if and when divulged, she or he can designate such database as critical.[45] The Minister makes the final call on the type of information that is of importance to the protection of the national security of the Republic or the social well being of its citizens.

Section 53 of the ECT Act provides that the Minister may by notice in the Gazette:

(a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data for the purposes of this chapter; and
(b) establish procedures to be followed in the identification of critical databases for the purposes of this chapter.

Section 54(2) provides that, for the purposes of this chapter, registration of a critical database means the recording of information listed under this section in a

[44] 'Analysis of the Electronic Communications and Transactions Act, 25 of 2002' *Legislation Service Bulletin* vol 20 (Juta, 3 October 2002).
[45] s 53 of the ECT Act.

register maintained by the department or by such other body as the Minister may specify, for example, the full names, address and contact details of the critical database administrator; and the location of the critical database, including the locations of component parts of it where a critical database is not stored at a single location.[46]

2.11 Domain Name Authority and administration

Section 59 of the ECT Act provides that a juristic person to be known as the '.za Domain Name Authority' is established for the purpose of assuming responsibility for the .za domain name space as from a date determined by the Minister by notice in the Gazette and by notifying all relevant authorities.

The initial draft of this provision envisaged the State as the only member of the domain name authority (Authority). A compromise has been reached in the ECT Act that envisages a public organisation, representative of all South Africans including government, controlling and administering the domain name. Instead of the State being the sole member of the Authority, the amended Act provides that all citizens and permanent residents of South Africa may be members upon application.

However, the Minister retains the powers to appoint the selection panel for selecting members of the board, and may exercise an option to reject the panel's recommendations if she disagrees with them. Effectively, the panel is required to select individuals whom the Minister chooses to have on the board, but, ultimately, the Minister selects members of the board. The amended Act declares that the panel must recommend appointments from certain sectors of society, such as the existing domain name community, academic and legal sectors, the Internet user community and labour.[47] The Minister published names of members of the .za domain names board in the Government Gazette of 15 July 2003.

Section 65(1) provides that the Authority must, amongst other things, administer and manage the .za domain name space in compliance with international best practice in the administration of the .za domain name space. Section 65(7) provides that the authority must respect and uphold the vested rights and interests of parties that were actively involved in the management and administration of the .za domain name space at the date of its establishment, provided that certain requirements are met.

Section 69(1) provides that the Minister, in consultation with the Minister of Trade and Industry, must make regulations for an alternative mechanism for the resolution of disputes in respect of the .za domain name space. It is not clear so far how domain names will be allocated to individuals and companies, or whether such individuals will have property rights over their domain names. In terms of the Canadian Internet Registration Authority (CIRA), for example, a domain name registrant retains no property right on the domain name.[48] The only right of

[46] s 56 of the ECT Act provides that information contained in the register provided for in s 54 must not be disclosed to any person other than to employees of the department who are responsible for the keeping of the register, subject to exceptions listed under the section.
[47] s 60(1) of the ECT Act provides that the Minister must, within 12 months of the date of commencement of this Act, take all steps necessary for the incorporation of the authority as a company contemplated in s 21(1) of the Companies Act, 61 of 1973. s 60(2) further provides that all citizens and permanent residents of the Republic are eligible for membership of the authority. s 62(1) provides that the authority is managed and controlled by a board of directors consisting of nine directors, one of whom is the chairperson, appointed in terms of the process prescribed under s 62(2).

possession such registrant has is valid for a renewable period of registration.

2.12 Cyber inspectors

The ECT Act creates cyber policing in the form of cyber inspectors or cyber police. These cyber police will be employees of the DOC. They have the power to monitor, with no expertise required, any web page or information system in the public domain. In terms of section 80(1) of the ECT Act, the director-general may appoint any employee of the department as a cyber inspector empowered to perform the functions provided for in the chapter. Subsection (2) further provides that a cyber inspector must be provided with a certificate of appointment signed by or on behalf of the director-general in which it is stated that he or she has been appointed as a cyber inspector. Such a certificate provided for in subsection (2) may be in the form of an advanced electronic signature.

Section 81 of the Act provides that a cyber inspector may monitor and inspect any website or an information system in the public domain. Section 82 of the Act provides that a cyber inspector may, in the performance of his or her functions, at any reasonable time, without prior notice and on the authority of a warrant issued in terms of section 83(1)–

> enter any premises or access an information system that has a bearing on an investigation and -
> (a) search those premises or that information system;
> (b) search any person on those premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

Section 82(2) provides that a person who refuses to cooperate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence. Consumers and businesses can only hope that the ECT Act will be amended to cater for these people's qualifications, and also provide certain limits to their powers, considering the potential infringement of individual's and company's rights of privacy.

2.13 Cyber crime

Section 85 defines 'cyber crime' as the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence. In the case of *Douvenga*,[49] the Court had to decide whether an accused employee GM Douvenga of Rentmeester Assurance Limited (Rentmeester) was guilty of a

[48] CIRA policies, rules, procedures, and agreement applicable to registrants and registrars http://www.cira.ca/en/documents/q3/RegistrantAgreement-1.5-en.txt.

contravention of section 86(1) (read with sections 1, 51 and 85) of the ECT Act. It was alleged in this case that the accused, on or about 21 January 2003, in or near Pretoria and in the district of the Northern Transvaal, intentionally and without permission to do so, gained entry to data which she knew was contained in confidential databases and/or contravened the provision by sending this data per e-mail to her fiancée (as he then was) to 'hou' (keep).

The accused, through her legal representative, pleaded not guilty and further argued that she had the authority to access the database on the basis that Rentmeester had given her the passwords and codes to obtain such access. In answering the questions of whether the accused did have the authority to access the database and whether Rentmeester was therefore vicariously liable for the accused's actions (as claimed by the accused), the Court held (quoting from the judgment of Minister of Police v Rabie) that the accused had neither permission nor consent to access the information in the database for her own personal purposes.[50]

The accused could not give any explanation to the Court when asked about her reasons to access and send the information to another computer. The Court therefore concluded that the accused was on a frolic of her own when she gained access to Rentmeester's databases and that Rentmeester could therefore not be held responsible (vicariously liable) for her actions. The Court observed that the information remained confidential information that only Rentmeester has exclusive use over. It was further observed that the information and the data subject were attached to one another and had to be handled by the data controller in a manner that complies with section 51(4) of the ECT Act.[51]

The accused was found guilty of contravening section 86(1) of the ECT Act and sentenced to a R1 000 fine or imprisonment for a period of three months. When passing sentence, the Court considered various factors, such as the fact that the accused was a first-time offender and the fact that they were dealing with a very new piece of legislation, etc.

Section 86(2) of the ECT Act provides that a person who intentionally and without authority to do so interferes with data in a way that causes such data to be modified, destroyed or otherwise rendered ineffective is guilty of an offence.

Section 86(4) provides that a person who utilises any device or computer program mentioned in subsection (3) in order to overcome unlawfully security measures designed to protect such data or access thereto is guilty of an offence. Section 86(5) provides that a person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

---

[49] *Die Staat v M Douvenga (neé Du Plessis)* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported).

[50] In *Minister of Police v Rabie* 1986 (1) SA 117 (A) it was held that:
It seems clear that an act done by a servant solely for his own interests and purposes, although occasioned by his employment, may fall outside the course or scope of his employment and that in deciding whether an act by the servant does fall within the course and scope of employment, some reference is to be made to the servant's intention.

[51] In answering the question of whether by giving the accused passwords and codes to the databases Rentmeester had implicitly given her permission to access the databases, the Court cited the judgment of *R v Legwabe* 1949 TPD 872, where it was held that:
If, in the course of driving a motor vehicle within the limits of the consent or the instructions of the owner, a driver, by a change of intention, departs from the instructions or the terms of the consent of the owner and drives it for his own purposes, such driver is in my opinion guilty of a contravention of the Section. Likewise in the case of driving without the knowledge or consent of the owner if the stage arises where the driver departs substantially from the instructions or terms of consent of the owner the guilty mind may be inferred from misconduct.

Section 90 provides that a Court in the Republic trying an offence in terms of this Act has jurisdiction where the offence was committed in the Republic; by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

Section 91 provides that this chapter does not affect criminal or civil liability in terms of the common law.

3. SOME OF THE CRITICISMS LEVELLED AGAINST THE ECT ACT

There has been considerable interest in the ECT Act, which led to various experts and pseudo-experts in the area of information technology law to offer their differing interpretations of its provisions. Some critics of the ECT Act believe that the Act is rather prescriptive in the way in which electronic transactions will operate and that this could disrupt the way in which electronic transactions and e-commerce already operate within the market. This would be counter-productive and indeed contrary to the intent of the legislation, which is to stimulate growth and promote certainty in this area by actually slowing down rather than encouraging e-commerce, they say.[52]

Others, however, believe that the ECT Act is not prescriptive:

> although it does contain certain provisions relating to use of 'advanced electronic signatures', essential information that has to be available to consumers of a website where goods or services are offered (in certain circumstances), it leaves it up to you to decide how you want to communicate electronically or conclude transactions electronically. The ECT Act does not interfere with your business dealings and relationships.[53]

Some critics believe that the appointment of SAPO in terms of section 28(2) of the ECT Act[54] as a preferred ASP could be an impediment to the effective use of electronic communications. This could be a potential problem from an implementation and ongoing efficiency point of view, as the Post Office is notorious for its poor service and lack of efficiency, it is said.[55]

These critics believe that the provision on automated transactions is awkward:

> An exceptionally awkward provision unnecessarily affords contractual capacity to computers for the purposes of automated transactions, the purpose of which is unclear and suggests some muddled thinking. Indeed, the inclusion of unnecessary rules of offer and acceptance in the electronic context seems to suggest a failure to fully engage the common law principles of contract.[56]

[52] Cliffe Dekker Attorneys *Commentary on the Electronic Communications Act 25 of 2002*; available at http://www.mbendi.co.za/cliffedekker/literature/commentary/ect2002.htm.

[53] Department of Communications, Deloitte & Touche and Michalsons Attorneys Guide to the Electronic Communications and Transactions Act (24 March 2003); available at www.michalson.com/docs/guide.doc.

[54] s 28(2) of the ECT Act provides that '[w]here a law requires or permits a persons to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender'.

[55] Cliffe Dekker's TMT Unit *Comments on the New South African ECT Act* (2 August 2002); available at http://www.mbendi.co.za/a_sndmsg/news_view.asp?P=0&PG=24&I=38991&M=0&CTRL=S.

[56] *Comments on the new South African ECT Act* (note 56 above).

This could, however, be a misinterpretation of the ECT Act, in that the ECT Act does not regard the computer as an individual, but rather as an agent of an individual. The qualification is that the conduct of the electronic agent must be attributable to an individual. As it would appear below, legislation that regulates or seeks to regulate electronic communication in other countries does provide for automated transmission.

In the US, the E-Sign Act has a provision that a contract or other record relating to a transaction may not be denied legal effect solely because its formation, creation or delivery involves the action of an electronic agent, provided that the action of the electronic agent is legally attributable to the person to be bound by such contract. (An 'electronic agent' is a computer program or other automated means used to initiate an action or respond to electronic records or performances without review or action by an individual.[57])

It is further argued, by critics of the ECT Act, that while the protections afforded to consumers in terms of the ECT Act do so extensively protect consumers, these same provisions may have gone too far in protecting the consumer, with the result that many international suppliers may choose not to carry on an e-business helping South African consumers if they feel that it is not worth the trouble of having to comply with fairly onerous obligations with regard to South African consumers. It is said that, while the ECT Act specifically provides that the Act will apply in respect of consumer protection irrespective of the applicable law of the contract concluded, the enforceability of such a provision is highly unlikely.[58]

This appears to be a misconceived analysis of the provisions of the ECT Act, considering that electronic legislation in other countries also provides for 'onerous' consumer protection measures, as will be seen below. The ECT Act, like most electronic legislation in foreign countries, reflects the recommendations of the Model Law and the Guidelines.

4. OTHER RELEVANT SOUTH AFRICAN LEGISLATION

4.1 Privacy and data protection

Data protection is an aspect of safeguarding a person's right to privacy, which is enshrined in the constitutional Bill of Rights. The essence of data protection is to give a person (a degree of) control over his or her personal information. However, the law should also consider such competing interests as administering national social programmes, maintaining law and order, and protecting the rights, freedoms and interests of others. The task of balancing these opposing interests is a delicate one.

Section 14 of the Constitution of the Republic of South Africa (the final Constitution), provides that everyone has the right to privacy, which includes the right not to have their property searched or the privacy of their communications infringed.

The South African Law Commission is at present (March 2004) conducting an

[57] Alston & LLP Bird Law Firm *How the New E-Sign Act will affect E-Commerce* (26 April 2003); available at http://www.gigalaw.com/articles/2000-all/alston-2000-06-all.html.
[58] *Comments on the new South African ECT Act* (note 56 above).

investigation entitled 'Privacy and Data Protection' (Project 124). The investigation was included in the programme of the Commission at the request of the Minister for Justice and Constitutional Development. The Minister of Justice has appointed a Project Committee for this investigation to assist the Commission in its task. As a first step in its consultation process, the Commission intends to publish an issue paper for information and comment. The project is still at its infancy, and the issue paper was published on 28 August 2003.[59]

The idea of developing privacy legislation for South Africa is aligned with international trends. The United Kingdom (Data Protection Act, 1998); Canada (Privacy Act, 1983 and Personal Information Protection and Electronic Documents Act, 2000), Australia (Privacy Act, 1988 and The Privacy Amendment (Private Sector) Act, 2000), New Zealand (Privacy Act, 1993) and most European countries have already enacted privacy legislation.[60] It should be noted that the promulgation of data protection legislation in South Africa would necessarily result in amendments to other South African legislation, most notably the current privacy protection provisions in the Promotion of Access to Information Act, 2 of 2000 and the ECT Act. Both these Acts contain interim provisions regarding data protection in South Africa. The provisions of section 50 of the ECT Act are therefore transitional provisions, pending the promulgation of what would likely be the Privacy and Data Protection Act.

4.2 The Electronic Communications Security (Pty) Ltd Act

On 6 February 2003, the ECS (Pty) Ltd Act, 68 of 2003 (e-Company Act) was published in Government Gazette 24356. The main objective of the e-Company Act is to provide for the establishment of a company (Comsec) that will provide electronic communications security products and services to organs of State. Comsec will be registered in terms of the Companies Act, 61 of 1973 (the Companies Act); however, the Minister of Trade and Industry can, in terms of section 6 of the e-Company Act, exempt Comsec from the application of the Companies Act.

Section 7 of the e-Company Act provides that the functions of Comsec are, inter alia, to protect and secure critical electronic communications against unauthorised access or technical electronic or any other related threats. Comsec will therefore monitor the e-Government services provided for under the ECT Act. Section 7(7) further exempts Comsec from licensing in terms of both the Broadcasting Act, 4 of 1999 and Telecommunications Act, 103 of 1996. Comsec can operate a telecommunication or broadcasting service without the need for a licence.

5. COMPARATIVE STUDY OF SELECTED FOREIGN JURISDICTIONS

The following section deals with the regulation of electronic communication in other jurisdictions, in particular, Australia, the United Kingdom (UK), the United States of America (US), and Canada.

[59] The Issue Paper can be accessed from the Law Commission's website at http://wwwserver.law.wits.ac.za/salc/issue/issue.html.
[60] *Explanatory Notes to Electronic Communications Act, 2000*; available at http://www.hmso.gov.uk/cgi-bin2/hmso_hl?DB=hmso-new&STEMMER=en&WORDS=electron+commun+&COLOUR=Red&STYLE=s&URL=http://www.hmso.gov.uk/acts/en/2000en07.htm#muscat_highlighter_first_match.

5.1 Australia

The Australian Electronic Communications Act, 2000 (Australian Act), which came into operation from 1 July 2001, is based upon the Model Law. The Australian Act primarily relates to dealings between persons and the Commonwealth government agencies, not dealings between private parties. South Africa's ECT Act applies to both business-to-government agencies and B2C transactions. However, the ECT Act leans strongly towards B2C and its provisions on consumer protection and protection of personal information are evidence of this. Provisions such as the protection of a critical database, domain name authority and administration and limitation of liability of service providers, on the other hand, indicate the business-to-government agency application of the ECT Act.

The Australian Act does not cover the enforceability or admissibility of Internet contracts as evidence in Court proceedings; or determine whether an electronic agent can accept 'click through' terms that have not been seen by a human being. Section 20 of the ECT Act provides that in an automated transaction an agreement may be formed where an electronic agent performs an action required by law for agreement formation, unless the agent commits a material error without providing the other person with an opportunity to prevent or correct the error.

The Australian Act gives business and the community the option of using electronic communications when dealing with government agencies. The ECT Act also has an e-government services provision in terms of which any public body that accepts the filing of documents, or requires that documents be created or retained, may, notwithstanding anything contrary in the applicable law, accept the filing of such documents, or the creation or retention of such documents in the form of data messages.[61]

In terms of the Australian Act, a person must consent to receiving electronic communications. Consent can be inferred from a person's conduct. The consent provisions do not extend to Commonwealth entities. It is believed that extending these provisions to Commonwealth entities would be inconsistent with the Australian government's commitment to delivering all appropriate Commonwealth services electronically.

The Australian Act does not state what standard will constitute an electronic signature. Parties are free to agree on what is acceptable under the circumstances. Section 13 of the ECT Act provides that: '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.' However, in terms of section 13(3) of the ECT Act, parties can agree between themselves on the type of the electronic signature to be used.

The Australian Act provides that an electronic signature must identify the originator sufficiently for the purpose of that communication. The Australian Act does not require that the signature itself provide a means of verifying the integrity of the communication. Section 13(3)(a) of the ECT Act and article 7 of the Model Law provide that a method must be used in an electronic signature to identify the person and to indicate the person's approval of the information contained in the data message.

[61] s 27 of the ECT Act.

5.2 The United Kingdom (UK)

The UK Electronic Communications Act, 2000 (UK Act) received Royal assent on 25 May 2000. The main purpose of the UK Act is said to be to help build confidence in electronic commerce and the technology underlying it by providing for, inter alia, the legal recognition of electronic signatures and the process under which they are verified, generated or communicated; and the removal of obstacles in other legislation to the use of electronic communication and storage in place of paper.[62] The broad aim of the UK Act is to facilitate electronic communication and thus e-commerce.[63]

The UK also has other electronic communications regulatory instruments, such as the Electronic Commerce (EC Directive) Regulations 2002. The main purpose of these regulations is to implement the main requirements of the EU Directive into UK law — aimed at encouraging greater use of e-commerce. The UK also has the Directive on Privacy and Electronic Communications, 2002, which updates the existing EU Telecoms Data Protection Directive of 1999.

5.3 The United States of America

In the summer of 1999, the National Conference of Commissioners on Uniform State Laws (NCCUSL) promulgated the Uniform Electronic Transactions Act (UETA).

5.3.1 The Uniform Electronic Transactions Act (UETA)

The UETA is modelled on the Model Law. The purpose of the UETA is to create the legal recognition of electronic records, electronic signatures, and electronic contracts. The fundamental premise of this Act is that the medium in which a record, signature, or contract is created, presented or retained does not affect its legal significance.[64] In terms of section 7(a) and (b) of the UETA, a record or signature may not be denied legal effect or enforceability solely because it is in electronic form, nor can a contract be denied legal effect or validity simply because an electronic record was used in the formation of the contract.

5.3.2 The Electronic Signatures in Global and National Commerce Act (e-Sign Act)

On 30 June 2000, the US President signed the e-Sign Act into law. Unlike the UETA, which is an instrument for adoption by individual states, the E-Sign Act is a federal statute that is binding on every state. The E-Sign Act is applicable to a country for facilitating the use of electronic records and signatures in interstate and foreign commerce. However, the basic scope of the two Acts is similar.

Under the E-Sign Act, e-signatures and electronic documents may be used in

[62] *Explanatory Notes to Electronic Communications Act 2000* (note 61 above).
[63] Ibid.
[64] The New United States Uniform Electronic Transactions Act: Substantive Provisions, Drafting History and Comparison to the UNCITRAL Model Law on Electronic Commerce available at http://www.unidroit.org/english/publications/review/articles/2000-4.htm.

most commercial transactions, both B2B and B2C. This is in line with the EU member states, whose respective appropriate laws are required to comply with the EU Directive that applies to both B2B and B2C transactions. The purpose of the e-Sign Act is to facilitate the use of electronic records and signatures by affording the same legal status to an electronic document or to a document signed electronically as to its paper counterpart. This covers both data messages and electronic signatures.

The e-Sign Act provides protections for B2C transactions in e-commerce that are not similarly required for B2B transactions. In particular, the consumer must consent to the use of an electronic record or signature.[65] The e-Sign Act aims to create a consistent legal framework throughout the US, and would automatically invalidate any regulation that denies validity to a record solely because it is an electronic record.[66] In practical terms, the e-Sign Act grants online contracts the same legal weight as their paper counterparts. The e-Sign Act attempts to facilitate commercial transactions by providing a uniform legislative framework throughout the US.[67]

5.4 Canada

On 30 September 1999, the Uniform Law Conference of Canada adopted the Uniform Electronic Commerce Act (Uniform Act) of 1999, which was created as a model electronic transactions law. The Uniform Act is based upon the Model Law and it was recommended that all the provinces of Canada as well as the federal government adopt it.

Section (3) of the Uniform Act provides that the Act does not apply in respect of (a) wills and their codicils; (b) trusts created by wills or by codicils to wills; (c) powers of attorney, to the extent that they are in respect of the financial affairs or personal care of an individual; (d) documents that create or transfer interests in land and that require registration to be effective against third parties; and, further, that, it does not apply in respect of negotiable instruments.

Section (5) of the Uniform Act provides that information shall not be denied legal effect or enforceability solely by reason that it is in electronic form.[68] Section 7 of the Uniform Act provides that a requirement under enacting jurisdiction law that information be in writing is satisfied by information in electronic form if the information is accessible to be usable for subsequent reference.

Section 10 provides that an electronic signature in respect of documents to be submitted to the government can be satisfactory only if the government has consented to accepting electronic signatures; and, further, that the electronic signature should meet technology standards the government has put in place.[69]

Section 19 of the Uniform Act also recognises an electronic agent, and defines it as a computer program or any electronic means used to initiate an action or to respond to electronic documents or actions in whole or in part without review by a natural person at the time of the response or action.

This policy took effect on 1 April 2002 with the purpose of ensuring that

[65] Kelley Drye Law Firm *Electronic Contracting under the E-sign Act*; available at http://www.kelleydrye.com/resourcecenter/Internet-E-Commerce/ElectronicContractinga1.htm.
[66] Ibid.
[67] *Electronic Contracting under the E-sign Act* (note 66 above).
[68] s 6 of the ECT Act, on the other hand, provides that:

communications across the Government of Canada are well coordinated, effectively managed and responsive to the diverse information needs of the public.

It requires that institutions must:

- ensure that Internet communications conform to government policies and standards; and that Government of Canada theme and messages must be accurately reflected in electronic communications with the public and among employees.
- ensure congruence with other communication activities, an institution's Web sites, sub-sites and portals must be reviewed regularly by the head of communications, or his or her designate, who oversees and advises on Web content and design.
- respect privacy rights and copyright ownership in all online publishing and communication.[70]

Canada also has the Personal Information Protection and Electronic Documents Act to support and promote e-commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act. However, this Act prescribes no specific technology for electronic signature. It vaguely provides that secure electronic signature is required for documents as evidence or proof, seals, or statements made under oath, etc.

Canada, in addition, has several international bilateral agreements on e-commerce, signed with the EU on 16 December 1999, with Australia on 9 February 2000 and with the UK on 22 February 2001.[71]

6. COMPARISON AND ANALYSIS OF THE INTERNATIONAL INSTRUMENTS

South Africa's ECT Act is to some extent based on the Model Law and the EU Directive. Chapter 3 of the Green Paper on e-commerce specifically recognised the Model Law on e-commerce as a source to be used in the development of South African law on e-commerce. The Green Paper also set out provisions of the

(1) Nothing in this Act requires a person to use or accept information in electronic form, but a person's consent to do so may be inferred from the person's conduct.
(2) Despite subsection (1), the consent of the Government to accept information in electronic form may not be inferred by its conduct but must be expressed by communication accessible to the public or to those likely to communicate with it for particular purposes.

[69] s 10(1) of the ECT Act provides that a requirement under [enacting jurisdiction] law for an electronic signature satisfies the signature of a person.

(3) For the purposes of subsection (1), where the signature or signed document is to be provided to the Government, the requirement is satisfied only if:
(a) the Government or the part of Government to which the information is to be provided has consented to accept electronic signatures; and
(b) the electronic document meets the information technology standards and requirements as to method and as to reliability of the signature, if any, established by the Government or part of Government, as the case may be.

[70] Communications Policy of the Government of Canada (April 2002); available at http://www.tbssct.gc.ca/pubs_pol/sipubs/comm/comm1_e.asp#leg.

[71] On 9 February 2000, Canada and Australia signed a bilateral and multilateral co-operation on e-commerce, endorsing a shared vision of policy principles aimed at encouraging the growth of global e-commerce. On 16 December 1999, Canada and the EU signed a bilateral and multilateral cooperation on e-commerce, detailing a shared vision for the development of a global information society and economy. On 22 February 2001, Canada and the UK signed a bilateral and multilateral cooperation agreement on e-commerce, acknowledging a shared vision to encourage e-commerce and e-government. South Africa does not appear to have any bilateral cooperative agreement on electronic communications.

European Directive on Distance Contracts, which ultimately influenced the consumer protection provisions in chapter VII of the ECT Act.[72]

6.1 The Model Law and the ECT Act

The ECT Act reproduces the Model Law's definitions of 'originator' and 'addressee' as they are. This similarity is not surprising, considering that the Model Law influenced the ECT Act.

However, there are differences in certain definitions between the ECT Act and the Model law; for example, the Model Law defines an 'intermediary' as 'a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message'. The ECT Act, on the other hand, defines an intermediary as 'a person who, on behalf of another person, whether as an agent or not, sends, receives or stores that data message or provides other services with respect to that data message'.[73] The definition in the ECT Act therefore adds the words 'whether as an agent or not', which words do not appear in the Model Law's definition. The importance of this difference is highlighted in a situation where an impostor claims to be representing 'another person' and an innocent third party is lured into conducting e-business transactions with an impostor to the third party's own detriment. For purposes of the ECT Act, such an impostor will be held liable as an intermediary to a particular data message.

There are other differences in wording, article 7 of the Model Law provides 'that where the law requires a signature of a person, that requirement is met in relation to a data message if, (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message'. Section 13(1) of the ECT Act emphasises 'only' if an advanced electronic signature is used. There is no such qualification in article 7 of the Model Law. Section 37 of the ECT Act requires that only persons whose authentication products are accredited by the Accreditation Authority can provide advanced electronic signatures. It therefore follows that, in situations where a signature is required by law, such signature must be performed through a registered authentication service provider.

On the issues of legal requirements for data messages, writing, retention of information, formation and validity of agreements and recognition by parties of data messages, the ECT Act and the Model Law contain the same provisions. Article 13 of the Model Law provides that:

(1) A data message is that of the originator if it was sent by the originator itself.
(2) As between the originator and the addressee, a data message is deemed that of the originator if it was sent:
(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

[72] Department of Communications Green Paper on e-Commerce (November 2000).
[73] s 7 of the ECT Act.

Section 25(c) of the ECT Act goes further to provide that such data message will, however, not be regarded as that of the originator, if it can be proved that the information system of the originator, did not properly execute such programming. This is simply another generous provision of the ECT Act — a safeguard. Although not all of the provisions of the ECT Act are verbatim repetitions of the Model Law, they are substantially similar. It is also true to say that all of the provisions covered in the Model Law are also covered in the ECT Act, with the exception of provisions in the Model Law concerning contracts with regard to the carriage of goods.

6.2 The Model Law on e-Signatures and the ECT Act

The Model Law on e-signatures defines 'electronic signature' as 'data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message'.

Section 1 of the ECT Act, on the other hand, defines 'electronic signature' as data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature. The definition of an 'electronic signature' in the Model Law on e-signature differs from that of the ECT Act in that the ECT Act's definition does not require that the signatory's e-signature should indicate the signatory's approval of the information contained in the data message. Unlike the Model Law on e-signatures, the ECT Act requires only that the signatory should intend for the e-signature to serve as a signature. The effect of this difference is that, in terms of the ECT Act, a signatory may dispute the accuracy of the information contained in the data message, whereas in terms of the Model Law on e-signatures, a signatory may not dispute the information contained in the data message. This is so because by virtue of appending their signature, a signatory has approved the information contained in the particular data message.

6.3 The EU Directive on e-Commerce and the ECT Act

Article 11 of the Directive provides that the contract will be considered concluded when the recipient has received from the service provider, electronically, an acknowledgement of receipt of the recipient's acceptance and has confirmed receipt of the acknowledgement of receipt. This provision is similar to sections 22 and 26 of the ECT Act, except that in terms of the ECT Act the recipient does not receive an acknowledgement of receipt from the service provider, but rather from the sender.

To remove existing legal uncertainties the EU Directive establishes an exemption from liability for intermediaries where they only transmit information between third parties. Internet Service Providers (ISPs) have only limited liability for other 'intermediary' activities such as the storage of information (hosting) or enhancing onward transmission (caching). This implies that, in certain circumstances, as long as ISPs are not actively involved in the information they are transmitting and are not aware they are transmitting illegal content, they are not liable for transmitting it. The ECT Act also provides for the limited liability of ISPs in its chapter XI for, inter alia, activities such as mere conduit, caching and hosting.

6.4 The US UETA and the ECT Act

Section 8(a) of the UETA provides that, if parties agree to conduct their transactions electronically and there is a law that requires a person to provide, send or deliver information in writing to another, then that requirement is met if the information is provided, sent or delivered in an electronic record, but only if that information can be retained and later retrieved by the receiver when it is received. Section 12 of the ECT Act provides for the same requirement except that it does not specifically provide that parties should agree to conduct their transactions electronically.

Section 8(c) of the UETA further provides that an electronic record may not be sent, communicated or transmitted by a system that inhibits the ability to print or download the information in the electronic record. The ECT Act's version of this provision is the qualification that such an electronic communication should be capable of being retrieved by the recipient.

Another important issue raised by electronic transactions is attribution - that is, when and under what circumstances an electronic record or electronic signature is attributable to an individual. The UETA responds to this with a rule that if the electronic record or signature resulted from a person's action, then the record or signature will be attributed to that person. The ECT Act has a similar provision in section 25, except that instead of a simple requirement of action, the ECT Act requires that the originator should have sent the message in person or through his/her authorised agent or through a programmed information system.

Most, if not all, of the UETA provisions are similar to those provided for in the ECT Act. The reason for this is that both Acts resembles the recommendations of the Model Law.

6.5 The e-Sign Act and the ECT Act

An electronic signature, as that term is defined in the e-Sign Act, encompasses, but is not limited to, a 'digital signature', which refers solely to those signatures created and verified by cryptography. The ECT Act refers to electronic signatures and advanced electronic signatures, only a person accredited in terms of section 37 can provide the latter.

Specifically, the e-Sign Act provides that (1) signatures, contracts, and other records shall not be denied legal effect merely because they are in electronic form; and (2) a contract shall not be denied legal effect merely because it is signed electronically. Thus, an online electronic signature intended to create a legal agreement or a commercial transaction will have the same legal status as a written signature, and online contracts will have the same legal force as equivalent paper contracts. All of these provisions are covered in sections 11 to 15 of the ECT Act.

However, the e-Sign Act does not apply to documents to the extent that they are governed by, inter alia, any of the following: (1) a statute, regulation, or other rule of law addressing the creation and execution of wills, codicils or testamentary trusts; (2) a State statute, regulation, or other rule of law addressing adoption, divorce or other matters of family law. (3) The e-Sign Act also does not apply to critical notices such as the following: (1) Court orders or notices, or official Court

documents (including briefs, pleadings, and other writings); (2) notice of cancellation or termination of utility services, health insurance or benefits, or life insurance benefits; (3) product recall; (4) default, acceleration, repossession, foreclosure, eviction, right to cure or a rental agreement for a primary residence of an individual; and (5) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

This is quite a broad exclusionary provision, as compared to the ECT Act, which excludes only agreements for alienation of immovable property, agreements for the long-term lease of immovable property in excess of 20 years, the execution, retention and presentation of a will or codicil and the execution of a bill of exchange. It is important to note that the EU Directive, which also has a broader exclusion list than the ECT Act, does not exclude things such as rentals. The EU Directive expressly includes rentals as a form of agreement that can be entered into electronically, whilst the e-Sign Act expressly excludes it.

Conclusion

Generally, the ECT Act is a welcome piece of legislation, having regard to the previous lack of legislative direction on many of the more important and pressing e-commerce issues, including the validity of electronically concluded agreements, the legal validity of electronic data, the admissibility of electronic documents in Courts of law and the legal status given to electronic signatures.[74]

Other than the powers that the ECT Act confers on the Minister, all of the electronic communication legislation dealt with above, including the ECT Act, contains similar provisions. They are all modelled largely in terms of the Model Law and the OECD Guidelines. The ECT Act is therefore comparatively in line with foreign legislation from developed countries. The ECT Act has many commendable provisions — for instance, it does not exclude the common law, nor does it limit the operation of any law that expressly authorises, prohibits or regulates the use of data message. Most importantly, the ECT Act does not prohibit any person from establishing his or her own requirements in respect of the manner in which they will accept data messages. It also does not require any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form.

Nor does the ECT Act require persons to change the way in which they do business; it merely gives full legal force and status to transactions that may already be taking place electronically. Moreover, the Act gives full legal status to information that is electronically transmitted, generated, received or stored. In terms of the Act, agreements that are concluded wholly or partly by transmitting data messages have the same legal status as written agreements.

The ECT Act does not, however, dispense with any of the common-law requirements for valid contracting, for instance, requirements such as that the

[74] *Comments on the New South African ECT Act* (note 56 above).
[75] s 7 of the ECT Act.

parties contracting must have the necessary capacity to contract; that they must reach consensus on the terms of their agreement; and that the contract in question must be legal. Section 22 of the ECT Act also acknowledges the common-law reception theory of acceptance instead of the expedition theory of acceptance.

South Africa is also in the unique position of having components of developed and developing economies in one country, with the majority of its citizens living in Third World conditions. The emergence of the information economy in a country such as South Africa provides significant challenges to the public and private sectors. Owing to this unique position, the ECT Act provides for matters such as the provision of ways to maximise the benefits of electronic transactions to historically disadvantaged individuals (HDIs), and the provision of processes, programmes and infrastructure for using electronic transactions by SMMEs.

Considering the fact that South Africa's communications sector is in a developing stage, the ECT Act therefore has, in comparison with the other jurisdictions, the potential to facilitate the use of electronic communications.[75]