

Guide to the ECT Act

The information contained in this document has been prepared by Michalsons Attorneys and is intended for general information purposes only. Do not make any business decisions on the basis of this information without consulting an appropriately qualified lawyer who can analyse your precise requirements. Lance Michalson was a member of the team responsible for drafting the Act on the instructions of the Department of Communications.

Last updated: 07 June 2005

Introduction

The Electronic Communications and Transactions Act 25 of 2002 ("the Act" / "ECT Act") became law on Friday, 30 August 2002. This marked the end of a process initiated by the South African Government in 1999 to establish a formal structure to define, develop, regulate and govern e-commerce in South Africa.

The ECT Act is one of many sources of law which impact on electronic communications and transactions and must not be read in isolation of relevant statutory and common law. It applies to any form of communication by e-mail, the Internet, SMS etc except for possibly voice communications between 2 people.

The Act is also "an enabling" piece of legislation in that it provides functional equivalents for paper-based concepts (including writing, original and signature), some of which are encountered in over 300 pieces of legislation identified by the Department of Communications in 1999 which were not suitable to the information age as they all had paper-based concepts within them.

The Act is also a very wide piece of legislation and also deals issues which are not related to electronic communications and transactions (such as cyber inspectors, liability of service providers and domain names). It also attempts to provide legal certainty in areas of law where there was legal uncertainty prior to August 2002 (e.g. the formation of contracts and the status of so-called "click wrap" agreements).

Key Issues Addressed

Key issues sought to be addressed in the Act include:

- **Maximising benefits** – creating a national e-strategy around the promotion of universal access to electronic transactions with a view to bridging the digital divide, especially for members from previously disadvantaged communities, SMMEs and differently abled people;
- **Legal certainty** – providing for the legal recognition of electronic contracts and signatures and facilitating record retention, electronic evidence and automated transactions;
- **E-government** – encouraging electronic communications between Government and citizens;
- **Security** – the registration of cryptography service providers, the accreditation of electronic signature technologies by authentication service providers and the protection of critical databases;
- **Protection of individuals** – the protection of the consumer by stipulating minimum information to be provided to consumers and the protection of personal information and critical data;
- **Illegal activities and enforcement** – the creation of new "cyber offences" and cyber-inspectors to administer certain provisions of the Act;
- **Effective management of internet-related issues** – the establishment of a proper management regime with regard to domain names in the Republic of South Africa and the limitation of liability of Internet Service Providers.

What you should keep in mind

What you should keep in mind:

- **It is not prescriptive:** Although the Act does contain certain provisions relating to use of “advanced electronic signatures”, the registration of cryptography products and services, essential information that has to be available to consumers of a website where goods or services are offered (in certain circumstances) and certain computer related activities which are now “cyber” crimes, it leaves it up to you to decide how you want to communicate electronically or conclude transactions electronically. The Act does not interfere with your business dealings and relationships.
- **You do not need to “comply” with the entire Act:** When one scrutinises the ECT Act, only six of its 14 chapters make mention of a fine or imprisonment for those convicted of an offence under the Act. These six chapters relate to cryptography providers, authentication service providers, unsolicited commercial communications (spam), critical databases, cyber inspectors and cyber crime. Regulations still have to be published regarding cryptography providers, authentication service providers and critical databases. Until those regulations are in place, there is nothing to comply with.
- **Identify what is relevant to you:** Although the Act comprises 14 chapters and 95 sections, only certain sections of the Act may impact upon your business.
- **The Act should make you re-orientate your thinking:** The impact of the widespread use of e-mail and electronic documents requires a paradigm shift in the way many of us think about documents. There are new risks associated with the use of electronic documents. As you can’t store an electronic document in a safe (unless it is on a CD ROM) you need to start thinking about whether or not your important documents will be electronic or paper-based. Further, you need to decide whether or not the “original” of a document will now be the paper-based or electronic version. These issues will impact upon your business processes in one way or another.
- **Legal certainty, but at a cost:** Whilst the Act provides legal certainty in places, this comes at a cost as there is a strong likelihood that litigants will have to make use of expert witnesses to assist a Court or arbitrator to interpret and understand the various interpretations that can be given to various technical expressions used in the Act (e.g. when can an electronic communication be said to have “entered” a “information system” for purposes of contract formation? When is an electronic document “capable of being retrieved” by the recipient).

Synopsis of the Act

Chapter I: Interpretation, Objects and Application

This part of the Act defines critical words and phrases and sets out the main objects of the Act.

Chapter II: Maximising Benefits and Policy Framework

The objective is to maximise the benefits the Internet offers by promoting universal access in under serviced areas and ensuring that the special needs of particular communities, areas and the disabled are duly taken into account. The Act requires the Minister to develop a 3-year national e-strategy for the Republic by no later than 30 August 2004. This must be submitted to the Cabinet for approval, which, on acceptance, must declare the implementation of the national e-strategy as a national priority. The national e-strategy must set out the electronic transactions strategy of the Republic, programmes and means to achieve universal access, human resource development and development of SMMEs, ways to promote the Republic as a preferred provider and user of electronic transactions in the international market, the utilising of existing Government initiatives in attaining the objectives of the e-strategy, the role expected to be performed by the private sector in the implementation of the new national strategy, the objectives, timeframes and resources required to achieve the objectives provided for in the national e-strategy.

Chapter III: Facilitating Electronic Transactions

This Chapter deals with the removal of legal barriers to electronic transacting and comprises 2 parts:

Part 1 provides for the legal requirements of data messages. Various sections are drafted from the perspective of where a requirement is prescribed by “law”. It also attempts to create technology neutrality in respect of the legal treatment of data messages. Part I gives legal recognition to electronic documents and recognises that electronic documents and signatures can serve as the electronic *functional equivalent* of their paper based counterparts. Provision is made for the legal recognition of “electronic signatures” and the Act does not prescribe what type of technology must be used. Examples of electronic signatures include your typed name at the end of your e-mail, a scanned image of your handwritten signature embedded into a Word document and a so-called digital signature. The Act also creates special type of electronic signature, known as an “advanced electronic signature” (AES), which is a particularly reliable form of signature (read our brochure “Advanced Electronic Signatures 1.01”). Where a law (such as the Credit Agreements Act) requires a signature, only an AES will be valid. Provision is made for the legal recognition of the electronic version of paper-based concepts and

electronic data will, subject to certain conditions, be regarded as “writing” and constituting a “original”. The Act permits the keeping of records in electronic form. However, the ECT Act states the general legal principle but does not provide details or guidelines on what organisations should implement in practice (speak to i-Forest, an information management consultancy which works closely with Michalsons, to find out what to do). Provision is also made for integrity being key to ensuring proper evidentiary weight of electronic evidence and the ability to notarise, acknowledge or certify electronic documents. The Part also permits one to send a document by e-registered post through the South African Post Office. Part 1 also recognises that information can be incorporated into a document through the use of hyperlinks and that contracts can be performed by machines functioning as electronic agents for parties to an electronic transaction.

Part 2 creates certain presumptions as to the time when and place where you are deemed to have received information. Part 2 also provides legal certainty as to the status of so-called “click wrap” (mouse-click-on-icon) and “web wrap” agreements. It also covers situations where data messages are deemed to have been sent by someone. The Part also provides for the acknowledgement of receipt of a data message, although there is not a legal requirement to do so.

Chapter IV: E-government

This Chapter facilitates electronic access to government services, such as e-filing. It lists the requirements for the production of electronic documents and the integrity of information. Provision is made for any public body to accept and transmit documents in the form of data messages, and to issue permits or licenses in the form of data messages or make or receive payment in electronic form or by electronic means. The public body may specify any requirements (such as security and authentication) in the Government Gazette.

Chapter V: Cryptography Providers

The Internet presents security challenges which, without an effective regulatory framework, would pose a threat to the security of consumers and the State. This Chapter requires that **suppliers** (not users) of “cryptography” services or products to register their names and addresses, the names of their products with a brief description in a register maintained by the Department of Communications. Unless the (local or foreign) supplier has registered, they cannot provide their services or products in South Africa. Registration will allow investigative authorities such as the SAPS, to identify which organisation provide the encryption technologies intercepted by them in terms of our monitoring and interception laws. This will enable the investigative authorities to approach these service providers to assist with deciphering the encrypted messages.

Chapter VI: Authentication Service Providers

Identification and authentication of the parties in cyberspace remains a challenge and poses threats to consumers and businesses. The Act seeks to provide for the establishment of an Accreditation Authority within the Department, allowing voluntary accreditation of electronic signature technologies in accordance with minimum standards. Once accredited, these Government endorsed “advanced” electronic signatures can be used by parties who have to sign by means of an “advanced” electronic signature where required “by law”. In addition, the legislature has created a presumption of integrity where “advanced” electronic signatures are used – i.e. they will allow a party to place reliance on its authenticity by shifting the burden of proof onto the signatory to disprove its authenticity. It has also created a benefit in favour of those processes which have been accredited, that are recognised as particularly reliable. The Regulations governing accreditation were released for public comment on 30 July 2004 and have not yet been promulgated (June 2005).

Chapter VII: Consumer Protection

Website categories of information: Suppliers of goods or services must provide consumers with a minimum set of information, including the price of the product or service, contact details and the right to withdraw from an electronic transaction before its completion. A consumer is defined as a *natural person* acting as end-user of the goods or services. Consumers are also entitled, under certain circumstances, to a “cooling off” period within which they may cancel certain types of transactions concluded electronically without incurring any penalty.

Spam: Consumers also have the right not to be bound to unsolicited communications (spam) offering goods or services and the sender of the unsolicited communication must at the request of the consumer provide the identifying particulars of the source from which it obtained the consumers personal information. A person who continues to send unsolicited communications to a consumer after having been advised that the unsolicited communications are not welcome, commits an offence.

The Act also seeks to place the responsibility on businesses trading on-line to make use of sufficiently secure payment systems. If a payment system is breached, the supplier must reimburse the consumer for any loss suffered.

Chapter VIII: Personal Information and Privacy Protection

This Chapter establishes a voluntary regime for protection of personal information. Personal information includes any information capable of identifying an individual. Collectors of personal information (data collectors) may subscribe to a set of universally accepted data protection principles. It is envisaged that consumers will prefer to deal with only those data collectors that have subscribed to the recorded data protection principles. The sanction for breach of these provisions is left to the parties themselves to agree on. Subscription to these principles is voluntary due to the fact that the South African

Law Commission's investigation into privacy in South Africa. An Issue Paper was released in October 2003 which is accessible from <http://www.privacylaw.co.za/home.htm>. Following an evaluation of Submissions on the Issue Paper which had to be submitted by 01 December 2003, the Law Commission may publish a Discussion Paper on privacy containing draft legislation in Q1 2006.

Chapter IX: Protection of Critical Data

In terms of its definition, critical data is information which, if compromised, may pose a risk to the national security of the Republic or to the economic or social well being of its citizens. The Minister may prescribe matters relating to the registration of critical databases and require certain procedures and technological methods to be used in their storage and archiving. In November 2003 the Minister of Communications awarded a tender to a consortium of Consultants to undertake an inventory of all major databases in South Africa. The purpose of this according to the press release is to assist the Minister to (i) put in place regulations, with respect to the development, maintenance, validity, integrity and security of these databases and related systems, (ii) review progress and compliance on an ongoing basis, (iii) refine policy, legislative and regulatory requirements where appropriate and (iv) ensure that databases and data, in the Republic of South Africa, that could negatively impact on companies and citizens, are developed, maintained and secured to meet appropriate standards.

Chapter X: Domain Name Authority and Administration

The Act has established a Domain Name Authority to assume responsibility for the .za domain name space, which must be incorporated as a section 21 company by no later than 30 August 2003. All citizens and permanent residents of the Republic are eligible for membership of the Authority and must be registered as members upon application and on payment of a nominal fee. The Act provides for certain issues that have to be provided for in the Memorandum and Articles of Association of the Authority, which will be managed and controlled by a board of directors consisting of 9 directors (see the Minister's Parliamentary Briefing on 12 September 2003). The directors are broadly representative of the demographics of the country and include stakeholders from the existing Domain Name Authority, academic and legal sectors, science, technology and engineering sectors, labour, business and the private sector, culture and language, public sector and the Internet user community. The functions of the Authority are provided for in the Act. Provision is made for finances and reporting and for disputes involving Domain Names to be settled by means of alternate disputes resolution methods.

Chapter XI Limitation of Liability of Service Providers

Chapter XI deals with the limitation of the liability of service providers or so-called "intermediaries" in cases where they may otherwise have been liable for third party data hosted on their servers. It creates a safe harbour for service providers who were previously exposed to a wide variety of potential liability by virtue of merely fulfilling their basic technical functions. The service providers may seek to limit their liability where they have acted as mere conduits for the transmission of data messages. In each situation the Act seeks to provide for specific requirements that the actions of the service providers must meet before the clause may be invoked to limit his or her liability.

Chapter XII: Cyber Inspectors

Chapter XII of the Act seeks to provide for the Department of Communications to appoint cyber inspectors. The cyber inspectors may monitor Internet websites in the public domain and investigate whether cryptography service providers and authentication service providers comply with the relevant provisions. The inspectors are granted powers of search and seizure, subject to obtaining a warrant. Inspectors can also assist the police or other investigative bodies, on request.

Chapter XIII - Cyber Crime

Chapter XIII of the Act seeks to make the first statutory provisions on cyber crime in South African jurisprudence. The Act seeks to introduce statutory criminal offences relating to the following:

- unauthorised access to data (e.g. so-called "hacking" and trading in passwords used to commit an offence);
- interception with data (e.g. tapping into data flows or denial of service attacks);
- interference with data (e.g. viruses and denial of service attacks);
- computer related extortion, fraud and forgery (e.g. where someone gains financially by undertaking to cease or desist from doing something using a computer).

Any person aiding or abetting another in the performance of any of these crimes will be guilty as an accessory. The Act prescribes the penalties for those convicted of offences which render a person liable to a fine or imprisonment for periods not exceeding 12 months in certain circumstances or five years in certain circumstances.

Chapter XIV: General Provisions

Chapter XIV contains certain “long arm” provisions which give a Court in the Republic jurisdiction to try an offence which was committed in the Republic, or where any active preparation towards the offence was committed in the Republic, where the offence was committed by a South African citizen or a permanent resident in the Republic or by a person carrying on business in the Republic, or was committed onboard any ship or aircraft registered in the Republic or on an aeroplane to or from the Republic at the time the offence was committed.

The Act repeals the Computer Evidence Act of 1983 and limits the liability of the State, the Minister of Communications and any employee of the State for any act or omission carried out by a person in good faith and without gross negligence.

“ECT Act” compliance

Please read our opinion piece published in the February 2004 edition of Brainstorm magazine titled “At best, ignorant ... at worst, charlatans” located at <http://brainstorm.itweb.co.za/online/ReadStory.asp?StoryID=140196> and a related article dated 27 July 2004 published at IT-Analysis.com titled “Regulatory and governance technology solutions: “marketing the fear factor”?” located at <http://www.it-analysis.com/article.php?id=12094&zz=669834644b231> .

The following issues may constitute compliance requirements for organisations:

- Incorporation by reference (s11.3)
- Electronic signatures (s13)
- Electronic evidence (s15)
- Production of information (s16)
- Record retention (s16)
- Automated transactions and website architecture (s20)
- Website content (ss 43,44)
- Contract formation (s 22)
- Cryptography service providers (ss29-32)
- Secure payment systems (ss43.5, 43.6)
- SPAM (s45)
- Protection of critical data (ss52-58)

ECT Act Offence and Penalty Quick Reference Table

ECT ACT	OFFENCE & PENALTY
CHAPTER V CRYPTOGRAPHY PROVIDERS (ss 29-32)	32(2) A person who contravenes or fails to comply with a provision of this Chapter is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.
CHAPTER VI AUTHENTICATION SERVICE PROVIDERS (ss 33-40)	37(3) A person falsely holding out its products or services to be accredited by the Accreditation Authority is guilty of an offence. 40(2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1), is guilty of an offence.
CHAPTER VII CONSUMER PROTECTION (ss 42-49) 45 Unsolicited goods, services or communications	45(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).
CHAPTER IX PROTECTION OF CRITICAL DATABASES (ss 52-58)	58(2) A critical database administrator that fails to take the remedial action within the period stated in the notice is guilty of an offence.

<p>CHAPTER XII CYBER INSPECTORS (ss 80-84)</p>	<p>80(5) Any person who-</p> <p>(a) hinders or obstructs a cyber inspector in the performance of his or her functions in terms of this Chapter; or</p> <p>(b) falsely holds himself or herself out as a cyber inspector,</p> <p>is guilty of an offence.</p> <p>82(2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence.</p> <p>84(1) Except for the purpose of this Act or for the prosecution of an offence or pursuant to an order of court, a person who has, pursuant to any powers conferred under this Chapter, obtained access to any information may not disclose such information to any other person.</p> <p>84 (2) Any person who contravenes subsection (1) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding six months.</p>
<p>CHAPTER XIII CYBER CRIME (ss 85-89)</p>	<p>89 (1) A person convicted of an offence referred to in sections 82 (2) or 86 (1) , (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.</p> <p>89 (2) A person convicted of an offence referred to in section 86 (4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.</p>

For further information please contact:

Lance Michalson

Tel: (021) 423-3332
 Fax: (011) 507-5284
 E-mail: lance@michalson.com
 Web site: www.michalson.com

Brendan Hughes

(021) 423-3332
 (011) 507-5284
brendan@michalson.com
www.michalson.com