

Application of the Electronic Communications and Transactions Act to Online Merchants From Other Jurisdictions

Hlengiwe Zondo-Kabini*

¶1 Online merchants looking at exciting electronic commerce opportunities in South Africa will be pleased to know that legally-protected electronic transactions are a reality in South Africa. The government has now passed legislation dealing with electronic commerce, namely, the Electronic Communications and Transactions Act¹ (“Act”). The object of the Act is to facilitate electronic transactions and communications, to inspire confidence in the use of such medium, and to encourage universal accessibility of e-commerce by all sectors of the population.

¶2 Foreign merchants should be aware of the provisions of the Act if they intend to provide goods or services online to the South African marketplace, in particular, how agreements are formed in South Africa using online transactions.

I. LEGAL RECOGNITION OF DATA MESSAGES

¶3 The Act places computer-generated documents on the same footing as traditional paper evidence. For example, a “data message” means data generated, sent, received, or stored by electronic means. Such information will not be regarded as devoid of any legal status merely because it is in this form. Information incorporated into an agreement will be regarded as being incorporated into a data message if such information is referred to in a way in which a reasonable person would have noticed the reference and the incorporation of such information; and such information is accessible by means of reading, storage, or retrieval by the other party, whether electronically or as a computer printout. In addition, a signature will not be regarded as devoid of any legal recognition merely because it is in an electronic form. A data message made by a person in the ordinary course of business, or a copy or an extract from such data message certified to be correct by an officer in the service of such person, will on mere production in any civil, criminal, administrative or disciplinary proceedings under any law or common law, be admissible in evidence against that person.

II. AUTOMATED TRANSACTIONS

¶4 Another important feature of the Act is the concept of automated transactions. This refers to electronic transactions conducted by means of data messages. For example, an

* Associate, Edward Nathan & Friedland (Proprietary) Limited. B.Proc, University of Durban Westville; LLB, University of Natal-Pietermaritzburg.

¹ No.25 of 2002.

agreement may be formed by parties where an electronic agent (computer program, electronic or other automated means) performs an action required by law for agreement formation. Alternatively, an agreement may be formed where parties to a transaction use the electronic agent. A party using an electronic agent to form an agreement will be presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement.

III. FORMATION AND VALIDITY OF THE AGREEMENTS

¶15 An agreement is concluded by parties by means of a data message at the time and place where the acceptance of the offer was received by the offeror. A data message used for concluding an agreement will be regarded as having been sent by the originator when it enters an information system outside the control of the originator, or if the originator and addressee are in the same information system, when the message is capable of being retrieved by the addressee.

¶16 In concluding agreements with South African consumers, merchants (foreign and local) should note the following provisions pertaining to consumer protection: Merchants are obliged to make certain information available to consumers on Web sites where such goods or services are offered. Examples of such information are:

- (1) merchant's full name and legal status;
- (2) physical address and telephone number;
- (3) security procedures, policies and any code of conduct that the merchant subscribes to; and
- (4) the manner of payment and the full price of goods or services, including transport costs, taxes and any other fees or costs.

¶17 Certain transactions are excluded from the ambit of the Act. Examples of excluded electronic transactions are:

- (1) financial services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;
- (2) auctions;
- (3) the supply of foodstuffs, beverages or other goods intended for everyday consumption; and
- (4) transactions where the price for the supply of goods or services is dependant upon fluctuations in the financial markets and which cannot be controlled by the supplier.

¶18 Merchants are also expected to provide consumers with an opportunity to review the entire electronic transaction, to correct any mistakes and to withdraw from the transaction, before finally placing any order. Should any merchant fail to comply with this obligation, the consumer can cancel the transaction within fourteen days of receiving the goods or services under the transaction.

¶19 Other than the exception of the excluded items mentioned above, the consumer is also entitled to a "cooling-off period" and can cancel without reason any transaction

within seven days from the date of receipt of the goods. Merchants should be aware that the protection given to consumers under this chapter applies irrespective of the legal system applicable to the agreement in question. Any provision in the agreement that excludes any rights guaranteed under this chapter is null and void.

¶10 There are also important provisions in the Act affecting merchants including foreign merchants offering goods or service online. The following provisions deal with technology used by merchants in conducting online business.

IV. CRYPTOGRAPHY PROVIDERS

¶11 The Act states that a cryptography provider is any service (which uses cryptographic techniques) that is provided to a sender, recipient of a data message, or to anyone storing a data message, and is characterized by four key elements: accessibility, authentication, integrity, and source. A cryptography service is expected to register its name in the register maintained by the Director-General of the Department of Communications and is also expected to furnish the Director-General with prescribed fees² as well as the following information:

- (1) the name and address of the cryptography service provider;
- (2) description of the type of cryptography service or cryptography product being provided; and
- (3) any other particulars which may be prescribed to identify and locate the cryptography service provider or its products or services adequately.

¶12 The cryptography service or cryptography product is regarded as being provided in South Africa if it is provided in one of the following forms:

- (1) from premises in South Africa;
- (2) to a person who is present in South Africa when that person makes use of the service or product; or
- (3) to a person who uses the service or product for the purposes of a business carried on in South Africa or from premises in South Africa.

¶13 It should be noted that in giving out particulars, the cryptography service is not expected to disclose confidential information or trade secrets regarding its products or services. Should any service provider fail to comply with any of the provisions of the applicable chapter of the Act, such service provider will be guilty of an offence and shall be liable on conviction to a fine or to imprisonment for a period not exceeding two years.

V. ACCREDITATION AUTHORITY

¶14 Accreditation in this context means recognition of an authentication product or service by the Accreditation Authority. Authentication products are described as products or services designed to identify the holder of an electronic signature to other

² Regulations detailing such fees have not yet been enacted.

persons. The Accreditation Authority is the Director-General of the Department of Communications. Unlike rules regarding cryptography services, accreditation is voluntary. Any service provider can sell or provide authentication products or services in South Africa. The Accreditation Authority has the power to do the following:

- (1) monitor the conduct, systems and operations of the authentication service provider to ensure that such service provider complies with the Act;
- (2) temporarily suspend or revoke accreditation of an authentication service provider; and
- (3) appoint an independent auditing firm to conduct periodic audits of the authentication service provider.

¶15 It should be noted that the Minister of Communications may, by notice in the Government Gazette, recognize the accreditation granted to any authentication service provider in any foreign jurisdiction. The Accreditation Authority will examine a number of factors before accrediting authentication products or services. The following are some of the factors taken into account:

- (1) the financial and human resources, including the assets of the service provider;
- (2) the quality of hardware and software systems of the service provider;
- (3) the procedures for processing of products or services; and
- (4) the regularity and extent of audits by an independent body.

¶16 The software and hardware systems and procedures of the service provider must at least:

- (1) be reasonably secure from intrusion and misuse;
- (2) provide a reasonable level of availability, reliability and correct operation;
- (3) be reasonably suited to performing their intended functions; and
- (4) adhere to generally accepted security procedures.

¶17 Different jurisdictions with enforceable data protection and electronic commerce legislation have specific provisions relevant to that jurisdiction. Merchants including foreign merchants should note the following provisions when dealing with South African consumers.

VI. UNSOLICITED GOODS, SERVICES, OR COMMUNICATIONS

¶18 A merchant who sends unsolicited electronic communication (“spam”) must provide the consumer with the option to cancel its subscription to the mailing list, and must identify the source from which that merchant obtained such consumer’s personal information. No agreement may be concluded if the consumer has not responded to the spam. Failure to comply with the Act will attract a fine or imprisonment for a period not exceeding twelve months.

VII. PROTECTION OF PERSONAL INFORMATION

¶19 In collecting personal information electronically, merchants should be aware that a data controller must comply with certain stringent requirements. The data controller must have the express written permission of the consumer for the collection, collation, processing or disclosure of any personal information on that consumer. Furthermore, the data controller may not electronically request, collect, collate, process or store personal information regarding a consumer that is not necessary for the lawful purpose for which the personal information is required. The Act stipulates a number of onerous requirements for the data controller that have not been covered in this Article. The Act is clear that the data controller is not allowed to “pick and choose” the obligations imposed by the Act. The rights and obligations of the parties regarding any breach of the obligations contained in the Act are governed by the terms of the agreement between such data controller and consumer.

VIII. POWER TO INSPECT, SEARCH, AND SEIZE

¶20 According to the Act the Director-General can appoint a cyber-inspector who will have the power to inspect any Web site or activity on any information system in the public domain and report any unlawful activity to the appropriate authority. The inspector has the power to investigate the activities of a cryptography service or authenticating service provider to see if they are compliant with the Act. The inspector may also demand the production and inspection of relevant licences and registration certificates as provided for in any law.

IX. WARRANTS OF ARREST

¶21 The Act enables magistrates or judges to issue warrants required by a cyber inspector where:

- (1) an offence has been committed within South Africa;
- (2) the subject of the investigation is a South African Citizen or resident in South Africa;
- (3) the subject of the investigation is present in South Africa at the time when the warrant is applied for; or
- (4) information pertinent to the investigation is accessible from the jurisdiction of the court.

X. JURISDICTION OF THE COURTS

¶22 The Act states that a South African court trying an offence in terms of this Act has jurisdiction where:

- (1) the offence was committed in South Africa;
- (2) any act or preparation towards the offence or any part of the offence was committed in South Africa, or where any result of the offence has had an effect in South Africa;

- (3) the offence was committed by a South African citizen or a person with permanent residence or carrying on a business in South Africa; and
- (4) the offence was committed on board any ship or aircraft registered in South Africa or on a voyage or flight to or from South Africa at the time the offence was committed.

¶23 It is strongly advisable that merchants wanting to engage in e-commerce in South Africa should ensure that they are fully cognizant of the provisions of the Act highlighted in this article, particularly the provisions relating to data messages, cryptography services, and the consumer protection.