THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2009

ARRANGEMENT OF SECTIONS

Copies of this Act may be obtained from the Government Printer, P.O. Box 30136, 10101 Lusaka. Price K36,000 each.

PART IV

CRYPTOGRAPHY PROVIDERS

PART V

ACCREDITATION AND RECOGNITION OF AUTHENTICATION SERVICE PROVIDERS

PART VI

CONSUMER PROTECTION

PART VII

PROTECTION OF PERSONAL INFORMATION

PART VIII

PROTECTION OF CRITICAL DATABASES

PART IX

DOMAIN NAME REGULATION

PART X

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

PART XI

INTERCEPTION OF COMMUNICATION

PART XIV

CYBER INSPECTIONS

PART XV

CYBER CRIME

PART XVI

GENERAL PROVISIONS

GOVERNMENT OF ZAMBIA

ACT

No. 21 of 2009

Date of Assent: 28th August, 2009

An Act to develop a safe, secure and effective environment for the consumer, business sector and the Government to conduct and use electronic communications; promote legal certainty and confidence, and encourage investment and innovation, in the electronic communications industry; facilitate the creation of secure communication systems and networks; establish the Central Monitoring and Coordination Centre and define its functions; repeal the Computer Misuse and Crimes Act, 2004; and provide for matters connected with or incidental to the foregoing.

[31st August, 2009

ENACTED by the Parliament of Zambia. Enactment

PART I

PRELIMINARY

1. This Act may be cited as the Electronic Communications and Transactions Act, 2009, and shall come into operation on such date as the Minister may, by statutory instrument, appoint. Short title and commencement

2. In this Act, unless the context otherwise requires— Interpretation

" access " in relation to a computer system or electronic communication system, means the right to use or open the whole or any part of the computer system or electronic communication system, or to see, open, use, get or enter information in the computer system or electronic communication system, with authorisation from the owner or operator thereof;

" addressee " in relation to a data message, means a person who is intended by the originator of the data message to receive it, but not a person acting as an intermediary in respect of that data message;

" advanced electronic signature " means an electronic signature that is unique to the user, capable of verification, under the sole control of the person using it, and linked to the data in such a manner that if the data is changed, the signature is invalidated;

" Anti-Corruption Commission " means the Anti-Corruption Commission established under the Anti-Corruption Commission Act; Cap. 91

" aural transfer " means a transfer containing the human voice at a point between, and including, the point of origin and the point of reception;

" authentication products or services " means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services are accredited by the Accreditation Authority under section *twenty-nine* or recognised by the Minister under section *thirty-two*;

" Authority " means the Communications Authority continued under section *four* of the Information and Communication Technologies Act, 2009; Act No. 15 of 2009

" automated transaction " means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct of data messages of one or both parties are not reviewed by a natural person in the ordinary course of the natural person's business or employment;

" browser " means a computer program which allows a person to read a hyperlinked data message;

" cache " means high speed memory that stores data for relatively short periods of time, under computer control, in order to speedup data transmission or processing;

" call-related information " includes switching, dialing or signaling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment, facility or service provided by a service provider and, where applicable, the location of the user within the telecommunications system;

" ccTLD " means country code domain at the top level of the internet's main system signed according to the two-letter codes in the International Standard ISO 3166-1, Codes for Representation of Names of Countries and their Subdivision;

" certification service provider " means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with, a data message;

" communication " means oral, wire or electronic communication;

" computer " means an electronic, magnetic, optical, electro-chemical or other high speed data processing device, performing logical, arithmetic or storage functions, or any data storage facility or communications facility directly related to, or operating in conjunction with, such device;

" computer data " means a representation of facts, information or concepts in a form suitable for processing in a computer system, or a program which is able to cause a computer system to perform a function;

" computer system " means a device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

" computer virus " means a written software which is willfully spread for purposes of causing damage to a computer system;

" consumer " means any natural person who enters, or intends to enter, into an electronic message with a supplier as the end-user of the goods or services offered by that supplier;

" content " in relation to an electronic communication, includes any information concerning the substance, purport or meaning of that communication;

" cracking " means an illegal act of decoding a password;

" critical data " means data that is declared by the Minister under section *forty-four* to be important for purposes of national security or the economic and social well-being of the citizens of Zambia;

" critical database " means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted;

" critical database administrator " means the person responsible for the management and control of a critical database;

" cryptograph product " means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—

(a) that such data can be accessed only by relevant persons;

(b) the authenticity of the data;

(c) the integrity of the data; or

(d) that the source of the data can be correctly ascertained;

" cryptography provider " means a person who provides, or who proposes to provide, cryptograph services or products in Zambia;

" cryptograph service " means any service which is provided to a sender or a recipient of a data message, or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(a) that such data or data message can be accessed, or can be put, into an intelligible form only by certain persons;

(b) that the authenticity or integrity of such data or data message is capable of being ascertained;

(c) the integrity of the data or data message; or

(d) that the source of the data or data message can be correctly ascertained;

" cyber " means the use, simulated environment or state of connection or association with electronic communications or networks including the internet;

" cyber inspector " means a person appointed as such under section *ninety-three*;

" damage " means an impairment to the integrity or availability of data, a program, a system orinformation;

" data " means electronic representations of information in any form;

" data controller " means any person, either alone or in common with other persons, who controls and is responsible for keeping and using of personal information on a computer, or in structured manual files, and electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

" data interference " means the corruption, damaging, deletion, deterioration, alteration or suppression of computer data without authority;

" data message " means data generated, sent, received or stored by electronic means and includes—

(a) a voice, where the voice is used in an automated transaction; and

(b) a stored record;

" data subject " means any natural person from, or in respect of whom, personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

" decryption " means the electronic transformation of data or communication that has been encrypted;

" delayed access message service " means a method by which a communication intended for a person can be submitted using a communications system, without the person being in direct contact with anyone submitting the communication and can be subsequently accessed by the person, whether or not other persons are able to access it;

" denial of service attacks " means rendering a computer system incapable of providing normal services to its legitimate users;

" device " means an apparatus which can be used to intercept a wire, oral or electronic communication other than—

(a) a telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of business and—

(i) used by the subscriber or user in the ordinary course of business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of business; or

(ii) used by a provider of wire or electronic communication service in the ordinary course of business, or by a law enforcement officer in the ordinary course of the law enforcement officer's duties; or

(b) a hearing aid or similar device;

" digital signature " means an electronic signature consisting of a transformation of an electronic record using an asymmetriccrypto-system such that a person having the initial untransformed electronic record and the signer's public key can accurately be determined—

(a) whether the transformation was created using the private key that corresponds to the signer's public key; or

(b) whether the initial electronic record has been altered since the transformation was made;

and includes voice recognition features, digital fingerprinting or such other biotechnology feature or process, as may be prescribed;

" distributed denial of service " means an attack that makes use of the user or server technology to multiply the effectiveness of the denial of service attack on one or more computer systems;

" domain name " means an alpha-numeric designation that is registered or assigned in respect of an electronic address or other resource on the internet;

" domain name system " means a system to translate domain names into IP address or other information;

" Drug Enforcement Commission " means the Drug Enforcement Commission established under the Narcotic Drugs and Psychotropic Substances Act; Cap. 96

" e-government service " means any public service provided by electronic means by any public body;

" electronic agent " means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

" electronic signature " means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

" electronic communication " means a transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by radio, electromagnetic, photo-electronic or photo-optical system, but does not include—

(a) any wire or direct oral communication;

(b) any communication made through a tone-only paging device;

(c) any communication from a tracking device; or

(d) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

" electronic communications system " means a radio, electro-magnetic, photo-optical or photo-electronic facility for the transmission of electronic communications, and any computer facility or related electronic equipment, for electronic storage of such communications;

" electronic communication service " means any service which provides the ability to send or receive electronic communications to users;

" electronic storage " means—

(a) a temporary or intermediate storage of an electronic communication incidental to the electronic transmission thereof; and

(b) a storage of any communication by an electronic communication service for purposes of backup for protection of such communication;

" electronic surveillance " means—

(a) the installation or use of an electronic, mechanical or other surveillance device for acquiring information, by intentionally directing surveillance at a particular known person who is located within Zambia under circumstances in which that person has a reasonable expectation of privacy; or

(b) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy;

" electronic user " means a known person who isexpected to possess, control, transmit, or receive electronic information

while the person is within Zambia;

" e-mail " means electronic mail or a data message used, or intended to be used, as a mail message between the originator and addressee in an electronic communication;

" encryption " means the electronic transformation of data in order to obscure or hide its content;

" hacking " means to access a computer illegally from a remote location, or without the authority of the owner;

" home page " means the primary entry point web page of a website;

" hyperlink " means a reference or link from some point in one data message or other technology or functionality, directing a browser or other technology or functionality, to another data message or point therein or to another place in the same data message;

" ICANN " means the Internet Corporation for Assigned Names and Numbers, a California non-profit public benefit corporation established under the laws of the State of California in the United States of America;

" illegal trade and commerce " means any internet fraud-related activity, or the use of the internet as a medium for illegal trade or any other illegal activity;

" information system " means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages, and includes the internet;

" information system services " includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the request of the recipient of the service;

" infringement " means the illegal use of copyright and other intellectual property rights;

" intelligence " means—

(a) information, whether or not concerning an electronic user within or outside Zambia, that relates to the ability of the Republic of Zambia to protect against—

(i) an actual or potential breach, attack or any grave or hostile act on a wire or electronic communication system;

(ii) any breach, sabotage or terrorism on a wire or electronic communication system by a person within or outside Zambia, a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service, a network of a foreign power or an agent of a foreign power;

(b) information, whether or not concerning a citizen of Zambia or an electronic user with respect to a foreign power or foreign territory, that relates to the national defence or the security of the Republic of Zambia; or

(c) the conduct of the foreign affairs of Zambia;

" intercept " means to access or acquire the contents of a communication through an electronic, mechanical or other device;

" interception device " means a device or process which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached;

" intermediary " means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

" internet " means the interconnected system of networks that connects computers around the world using the TCP/IP or other protocols, and includes future versions thereof;

" IP address " means the dynamic or static number identifying the point of connection of a computer or other device to the internet;

" judge " means a judge of the High Court;

" law enforcement officer " means—

(a) a police officer above the rank of sub-inspector;

(b) an officer of the Anti-Corruption Commission;

(c) an officer of the Drug Enforcement Commission;

(d) an officer of the Zambia Security Intelligence Service; and

(e) any other person appointed as such by the Minister for purposes of this Act;

" misuse of device " means the production, sale, procurement for use, distribution, possession or otherwise making available, of a computer password, access code or data by which the whole or any part of a computer system is capable of being accessed, or a device or computer program designed or adapted primarily for the purpose of committing an offence;

" Monitoring Centre " means the Central Monitoring and Coordination Center established pursuant to section *sixty-five;*

" natural person " means an individual;

" oral communication " means a verbal communication or any communication through sign language, but does not include any electronic communication;

" originator " means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;

" person " includes a public body;

" personal information " means information about an identifiable individual, including, but not limited to—

(a) information relating to the race, gender, pregnancy, marital status, nationality, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual, or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than twenty years;

" private body " means—

(a) a natural person who carries, or has carried on, any trade, business or profession, but only in such capacity;

(b) a partnership which carries, or has carried on, any trade, business or profession; or

(c) any former or existing juristic person, other than a public body;

" plain text " means decrypted or unencrypted data;

" pornography " means material that visually depicts images of a person engaged in explicit sexual conduct;

" public body " means—

(a) any department of the Government or any local authority; or

(b) any other functionary or institution exercising—

(i) a power, or performing a duty, under the Constitution; or

(ii) a power, or performing a function, under any other law;

Cap. 1

" recovery agent " means a person or entity who provides recovery information for storage services;

" recovery device " means hardware or software, that allows plaintext to be obtained, even if attempts are made to protect it through encryption or other security techniques or devices, by enabling a modification of any part of a computer or other system;

" recovery information " means a parameter that can be used with an algorithm, other data or object, which can be used to decrypt data or communications;

" registrant " means an applicant for, or holder of, a domain name;

" registrar " means an entity which is licensed by the Authority to update a repository;

" Register " means the Register of cryptography providers established under section *twenty-two;*

" registry " means an entity licensed by the Authority to manage and administer a specific sub-domain;

" remote computing service " means the provision of computer storage or processing services to the public by means of an electronic communications system;

" second level domain " means the sub-domain immediately following the ccTLD;

" service provider " means a public or private entity authorised to—

(a) provide or offer electronic communications by means of a computer system;

(b) process or store computer data on behalf of a communication service or users of such service; or

(c) own an electronic communications system to provide or offer an electronic communication service;

" sign language " means a language that uses manual communication, body language, facial expressions, lip patterns, hand shapes, orientation and movement of the hands, arms or other parts of the body, other than sound, to communicate or express a person's thoughts;

" spamming " means an illegal attempt or act to deliver a message, over the internet, to someone who has not solicited it;

" stored communication " means communication that has been submitted using a delayed access message service, is stored on equipment, and can be accessed;

" stored recovery information " means information that can be used to decrypt data or electronic communications;

" sub-domain " means any subdivision of the zm domain name space which begins at the second level domain;

" system interference " means the illegal interception, hindering or data interference of an electronic communications system or computer system, or the inputting, transmission, damage, deletion, deterioration, alteration or suppression of computer data, an electronic communication or its contents through, or by means of, an illegal access;

" TCP/IP " means the Transmission Control Protocol

Internet Protocol used by an information system to connect to the internet;

"third party " in relation to a service provider, means a subscriber to the service provider's services, any other user of the service provider's services or a user of information systems;

" TLD " means a top level domain of the domain name system;

" traffic data " means any computer data indicating the electronic communication's origin, destination, route, time, date, size, duration or type of underlying service and any content thereof;

" transaction " means a transaction of either a commercial or non-commercial nature or the provision of information or e-government services, but does not include any banking transaction or electronic funds transferred by a financial institution;

" trespasser " in relation to a computer or electronic communication system, means a person who accesses a computer or electronic communication system without authorisation, but does not include a person authorised by the owner or operator of the computer or electronic communication system to access all or part of the computer or electronic communication system;

" universal access " means access by all citizens of Zambia to internet connectivity and electronic transactions;

" user " means a person or entity who is authorised by a service provider to use its services;

" WAP " means the Wireless Application Protocol, an open international standard developed by the Wireless Application Protocol Forum Limited, a company incorporated under the laws of the United Kingdom, for applications that use wireless communication, and includes internet access from a mobile phone;

" wire communication " means an aural transfer made in whole or in part for the transmission and storage of communications by the aid of wire, cable or other like connection;

" web page " means a data message on the World Wide Web;

" website " means any location on the internet containing a home page or web page;

" World Wide Web " means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer;

" Zambia Development Agency " means the Zambia Development Agency established under section *four* of the Zambia Development Agency Act, 2006;

Act No. 11 of 2006

" Zambia Postal Services Corporation " means the Zambia Postal Services Corporation established under the Postal Services Act; and

Cap. 470

" zm domain name space " means the .zm ccTLD assigned to the Republic of Zambia according to the two-letter codes in the International Standard ISO.

Application

3. (1) Subject to the other provisions of this section, this Act applies in respect of any electronic transaction or data message.

(2) This Act shall not be construed as—

(a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by, or in, electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

Cap. 184

(3) Sections *five* and *six* of this Act do not apply to the Lands Act.

Cap. 60

(4) Part II of this Act does not apply to the Wills and Administration of Testate Estates Act.

(5) This Act shall not be construed as giving validity to any of the following transactions:

(a) an agreement for the alienation of immovable property under the Lands Act; Cap. 184

(b) the execution, retention and presentation of a will or codicil under the Wills and Administration of Testate Estates Act; Cap. 60

(c) the execution of a bill of exchange; or

(d) any guarantee.

(6) This Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages, including any requirement by, or under, any law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method.

PART II

LEGAL REQUIREMENTS FOR DATA MESSAGES

Legal requirements for data messages

4. (1) Information shall not be without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

(2) Information shall not be without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in the data message.

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

Writing

5. (1) A requirement in law that a document or information shall be in writing shall be met if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.

Use of advanced electronic signature

6. (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 shall be met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature shall not be without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement shall be met in relation to a data message if—

(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

(4) Where an advanced electronic signature has been used, such signature shall be treated as a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement shall not be 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 is evidenced by other means from which such person's intent or other statement can be inferred.

Determination of originality of data message

7. (1) Where a law requires information to be presented or retained in its original form, that requirement shall be met by a data message if—

(a) 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 the assessment specified under subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of paragraph (a) of subsection (1), the integrity of any information shall be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Admissibility and evidential weight of data messages

8. (1) In any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message in evidence—

(a) on the mere grounds that it is constituted by a data message; or

(b) 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 shall be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard shall be had to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of, or an extract from, the data message certified to be correct by an officer in the service of such person, shall on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law, be admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Retention of information in data message

9. (1) Where a law requires information to be retained, that requirement shall be met by retaining the information in the form of a data message if—

(a) the information contained in the data message is accessible so as to be usable for subsequent reference;

(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of that data message, and the date and time it was sent or received, can be determined.

(2) The obligation to retain information referred to in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Production of document or information

10. (1) Subject to section *twenty-one*, where a law requires a person to produce a document or information, that requirement shall be met if the person produces, by means of a data message, an electronic form of that document or information and if—

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document shall be maintained if the information has remained complete and unaltered, except for—

(a) the addition of any endorsement; or

(b) any immaterial change, which arises in the normal course of communication, storage or display.

Notarisation, acknowledgment and certification

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

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement shall be met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement shall be met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

Other requirements

12. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time shall be satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the words "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, shall be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(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 shall be 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 shall be met if an electronic copy of the document or information is sent to the post office, is registered by the post office and sent by that post office to the electronic address provided by the sender.

Automated transactions

13. (1) In an automated transaction—

(a) an agreement may be formed where an electronic agent performs an action required by law for agreement formation;

(b) an agreement may be formed where all parties to a transaction or either one of them uses an electronic agent;

(c) a party using an electronic agent to form an agreement shall, subject to paragraph (d), 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;

(d) a party interacting with an electronic agent to form an agreement shall not be bound by the terms of the agreement unless those terms were capable of being reviewed by a natural person representing that party prior to agreement formation;

(e) no agreement shall be formed where a natural person interacted directly with the electronic agent of another person and made a material error during the creation of a data message and—

(i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;

(ii) that person notified the other person of the error as soon as practicable after that person learnt of it;

(iii) that person takes reasonable steps, including steps that conform to the other person's instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(iv) that person has not used or received any material benefit or value from any performance received from the other person.

PART III

COMMUNICATION OF DATA MESSAGES

Variation by agreement between parties

14. This Part only applies if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for in the data messages.

Formation and validity of agreements

15. (1) An agreement shall not be 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 shall be concluded at the time when, and place where, the acceptance of the offer was received by the offeree.

Time and place of communication, dispatch and receipt

16. A data message—

(a) used in the conclusion or performance of an agreement shall be treated 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 it is capable of being retrieved by the addressee;

(b) shall be treated as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee; and

(c) shall be treated as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

Expression of intent or other statement

17. As between the originator and the addressee of a data message an expression of intent or other statement shall not be 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.

Attribution of data messages to originator

18. 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 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.

Acknowledgment of receipt of data message

19. (1) An acknowledgment of receipt of a data message shall not be necessary to give legal effect to that message.

(2) An acknowledgment of receipt may be given by—

(a) any communication by the addressee, whether automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

Acceptance of electronic filing and issuing of documents

20. A public body that, pursuant to any law—

(a) accepts the filing of documents, or requires that documents be created or retained;

(b) issues any permit, licence or approval; or

(c) provides for a manner of payment; may, notwithstanding anything to the contrary in such law—

(i) accept the filing of the documents, or the creation or retention of such documents in the form of data messages;

(ii) issue the permit, licence orapproval in the form of a data message; or

(iii) make or receive payment in electronic form or by electronic means.

Requirements may be specified

21. (1) Where a public body performs any of the functions referred to in section *twenty*, such body may specify, in a daily newspaper of general circulation in Zambia—

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

(b) in cases where a data message has to be signed, the type of electronic signature required;

(c) the manner and format in which electronic signature shall be attached to, incorporated in or otherwise associated with, a data message;

(d) the identity of, or criteria that shall be met by, any authentication service provider used by the person filing a data message or that the authentication service provider shall be a preferred authentication service provider;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for data messages or payments.

(2) For the purposes of paragraph (d) of subsection (1), the Zambia Postal Services Corporation is an authentication service provider.

(3) 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.

PART IV

CRYPTOGRAPHY PROVIDERS

Registration to provide cryptograph services or products

22. (1) A person shall not provide cryptograph services or products in Zambia without registration under this Part.

(2) A cryptograph service or product shall be treated as being provided in Zambia if it is provided—

(a) from any premises in Zambia;

(b) to a person who is present in Zambia where that person makes use of the service or product; or

(c) to a person who uses the service or product for the purposes of a business carried on in Zambia or from premises in Zambia.

(3) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding seven hundred thousand penalty units or to imprisonment for a period not exceeding seven years, or to both.

(4) A person who intends to provide a cryptograph service or product shall apply to the Authority for registration in the prescribed manner and form upon payment of the prescribed fee.

(5) The Minister may, on the recommendation of the Authority, by statutory instrument, make regulations to provide for -

(a) the procedure for the registration of cryptography providers;

(b) the forms to be used for registration purposes under this Part and the fees to be paid;

(c) the information and other details to be supplied by applicants for registration; and

(d) any other matter necessary to give effect to the provisions of this Part.

Register of cryptography providers

23. (1) The Authority shall establish and maintain a Register of cryptography providers.

(2) The Authority shall record the following particulars in respect of a cryptography provider in the Register referred to under subsection (1):

(a) the name and address of the cryptography provider;

(b) a description of the type of cryptograph service or cryptograph product being provided; and

(c) such other particulars as may be prescribed to identify and locate the cryptography provider or the products or services adequately.

(3) Except as otherwise provided by law, a cryptography provider shall not be required to disclose confidential information or trade secrets in respect of the cryptograph products or services.

Restrictions on disclosure of information in Register

24. (1) Information contained in the Register shall not be disclosed to any person other than to employees of the Authority who are responsible for the keeping of the Register.

(2) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

(3) Subsection (1) does not apply in respect of information which is disclosed—

(a) to any relevant authority for purposes of investigating a criminal offence or for the purposes of any criminal proceedings;

(b) to Government agencies responsible for safety and security in Zambia, pursuant to an official request;

(c) to a cyber inspector; or

(d) for the purposes of any civil proceedings which relate to the provision of cryptograph services or products and to which a cryptography provider is a party.

PART V

ACCREDITATION AND RECOGNITION OF AUTHENTICATION SERVICE PROVIDERS

Definition

25. In this Part, "accreditation" means recognition of an authentication product or service by the Accreditation Authority.

Appointment of Accreditation Authority and other officers

26. (1) For the purposes of this Part, the Authority shall act as the Accreditation Authority.

(2) The Accreditation Authority, after consultation with the Minister, may appoint employees of any Government department as Accreditation officers.

Selling of authentication products or service

27. Subject to section *twenty-two*, a person may, without the prior authority of any other person, sell or provide authentication products or services in Zambia.

Powers and duties of Accreditation Authority

28. (1) The Accreditation Authority—

(a) shall monitor the conduct, systems and operations of an authentication service provider to ensure compliance with section *thirty* and the other obligations of authentication service providers stipulated under this Act;

(b) may suspend or revoke the accreditation of an authentication product or service; and

(c) may appoint an independent auditing firm to conduct periodic audits of an authentication service provider to ensure compliance with section *thirty* and the other obligations of authentication service providers provided for under this Act.

(2) The Accreditation Authority shall maintain a publicly accessible database in respect of—

(a) authentication products or services accredited under section *twenty-nine;*

(b) authentication products and services recognised under section *thirty-two;*

(c) revoked accreditations or recognitions; and

(d) such other information as may be prescribed.

Accreditation of authentication products and services

29. (1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.

(2) An application for accreditation shall be made to the Accreditation Authority in the prescribed manner and form upon payment of the prescribed fee.

(3) A person who falsely holds out any products or services as accredited by the Accreditation Authority under this Act, commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

Criteria for accreditation

30. (1) The Accreditation Authority shall not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which the authentication products or services relate—

(a) is uniquely linked to the user;

(b) is capable of identifying the user;

(c) is created using means that can be maintained under the sole control of the user;

(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable; and

(e) is based on the face-to-face identification of the user.

(2) For purposes of subsection (1), the Accreditation Authority shall have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services:

(a) the authentication service provider's financial and human resources, including the assets;

(b) the quality of the hardware and software systems;

(c) the procedures for the processing of products or services;

(d) the availability of information to third parties relying on the authentication product or service;

(e) the regularity and extent of audits by an independent body;

(f) the factors referred to in subsection (4), where the products and services are rendered by a certification service provider; and

(g) any other relevant factor as may be prescribed.

(3) For the purposes of paragraphs (b) and (c) of subsection (2), the hardware and software systems and procedures shall—

(a) be reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability and correct operation;

(c) be reasonably suited to performing their intended functions; and

(d) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Accreditation Authority may determine, prior to accrediting authentication products or services—

(a) the technical and other requirements to be met;

(b) the requirements for issuing certificates;

(c) the requirements for certification practice statements;

(d) the responsibilities and liability of the certification service provider;

(e) the records to be kept and the manner in which, and length of time for which they must be kept; and

(f) the suspension and revocation procedures.

(5) The Accreditation Authority may impose any conditions or restrictions necessary for purposes of accrediting an authentication product or service.

Revocation or suspension of accreditation

31. (1) The Accreditation Authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has contravened the provisions of this Act or failed or ceased to meet any of the requirements, conditions or restrictions subject to which the accreditation was granted or recognition given.

(2) Subject to subsection (3), the Accreditation Authority shall not suspend or revoke the accreditation or recognition of an authentication service provider unless it has—

(a) notified the authentication service provider, in writing, of its intention to do so;

(b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which the accreditation was granted or recognition was given; and

(c) afforded the authentication service provider the opportunity to—

(i) respond to the allegations in writing; and

(ii) remedy the alleged breach within a specified period.

(3) The Accreditation Authority may suspend the accreditation or recognition of an authentication service provider with immediate effect for a period not exceeding ninety days, pending the implementation of the procedures required under subsection (2), if the continued accreditation or recognition of the authentication service provider is likely to result in irreparable harm to consumers or any person involved in an electronic transaction in Zambia.

(4) An authentication service provider whose products or services have been accredited under this Part may terminate the accreditation at any time, subject to such conditions as the Authority may determine at the time of accreditation or thereafter.

Recognition of accredited foreign products and services

32. (1) The Minister may, on the recommendation of the Authority, by statutory notice, and subject to such conditions as the Minister may determine, recognise the accreditation or recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.

(2) An authentication service provider who falsely holds out any products or services as recognised by the Minister under subsection (1), commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

Accreditation regulations

33. The Minister may, by statutory instrument, make regulations to provide for—

(a) the rights and obligations of persons relating to the provision of accredited products and services;

(b) the manner in which the Accreditation Authority shall administer and monitor compliance with accreditation obligations;

(c) the procedure for the granting, suspension and revocation of accreditation;

(d) the fees to be paid for accreditation;

(e) information security requirements or guidelines; and

(f) any other matter necessary for the implementation of this Part.

PART VI

CONSUMER PROTECTION

34. (1) This Part applies only to electronic transactions.

(2) Section *thirty-six* does not apply to an electronic transaction—

(a) for financial services, including but not limited to, investment services, insurance and re-insurance operations, banking services and operations relating to dealings in securities;

(b) by way of an auction;

(c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;

(d) for services which began with the consumer's consent before the end of the seven-day period referred to in subsection (1) of section *thirty-six*;

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) where the goods—

(i) are made to the consumer's specifications;

(ii) are clearly personalised;

(iii) by reason of their nature cannot be returned; or

(iv) are likely to deteriorate or expire rapidly;

(g) where audio or video recordings or computer software were unsealed by the consumer;

(h) for the sale of newspapers, periodicals, magazines and books;

(i) for the provision of gaming and lottery services; or

(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

(3) This Part does not apply to a regulatory authority established under any other law if that law prescribes consumer protection provisions in respect of electronic transactions.

Information to be provided by supplier

35. (1) A supplier offering goods or services for sale, hire or exchange by way of an electronic transaction shall make the following information available to consumers on the website where the goods or services are offered:

(a) its full name and legal status;

(b) its physical address and telephone number;

(c) its website address and e-mail address;

(d) membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;

(e) any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;

(f) in the case of a legal person, its registration number, the names of its office bearers and its place of registration;

(g) the physical address where that supplier will receive legal service of documents;

(h) a description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;

(i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(j) the manner of payment for the goods or services;

(k) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;

(l) the time within which the goods will be dispatched or delivered or within which the services will be rendered;

(m) the manner and period within which consumers can access and maintain a full record of the transaction;

(n) the return, exchange and refund policy of that supplier;

(o) any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;

(p) the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;

(q) where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently; and

(r) the rights of consumers in terms of section *thirty-six* where applicable.

(2) A supplier shall provide a consumer with an opportunity to—

(a) review the entire electronic transaction;

(b) correct any mistakes; and

(c) withdraw from the transaction, before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within fourteen days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled under subsection (3)—

(a) the consumer shall return the goods of the supplier or, where applicable, cease using the services performed; and

(b) the supplier shall refund all payments made by the consumer minus the direct cost of returning the goods.

(5) A supplier shall utilise a payment system that is sufficiently secure in accordance with accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) A supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

Cooling-off period

36. (1) A consumer may cancel, without giving any reason and without incurring any penalty, a transaction and a related credit agreement for the supply—

(a) of goods, within seven days after the date of the receipt of the goods; or

(b) of services, within seven days after the date of the conclusion of the agreement.

(2) Where a consumer cancels a transaction under subsection (1), the only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising the right referred to in subsection (1), the supplier shall give the consumer a full refund of the payment, which refund shall be made within thirty days of the date of cancellation.

(4) This section shall not be construed as prejudicing the rights of a consumer provided for in any other law.

Performance

37. (1) A supplier shall execute an order within thirty days from the date on which the supplier received the order, unless the parties have agreed otherwise.

(2) Where a supplier has failed to execute an order within thirty days or within the agreed period, the consumer may cancel the agreement upon giving seven days' written notice.

(3) Where a supplier is unable to perform under the agreement on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payments forthwith.

Applicability of foreign law

38. The protection provided to consumers in this Part applies irrespective of the legal system applicable to the agreement in question.

Non-exclusion

39. Any provision in an agreement which excludes any rights provided for in this Part is null and void.

Complaints to Authority

40. A consumer may lodge a complaint with the Authority in respect of any non-compliance with the provisions of this Part by a supplier.

PART VII

PROTECTION OF PERSONAL INFORMATION

Scope of protection of personal information

41. (1) This Part only applies to personal information that has been obtained through electronic transactions.

(2) A data controller shall subscribe to the principles outlined in section *forty-two* by recording such fact in any agreement with a data subject.

(3) A data controller shall subscribe to all the principles outlined in section *forty-eight* and not merely to parts thereof.

(4) The rights and obligations of the parties in respect of the breach of the principles outlined in section *forty-eight* shall be governed by the terms of any agreement between them.

Principles for electronically collecting personal information

42. (1) A data controller shall have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless the data controller is permitted or required to do so by law.

(2) A data controller shall not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) A data controller shall disclose, in writing, to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) A data controller shall not use any personal information for any other purpose than the disclosed purpose, without the express written permission of the data subject, unless the data controller is permitted or required to do so by law.

(5) A data controller shall, for as long as any personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller shall not disclose any personal information held by the data controller to a third party unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) A data controller shall, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which, and the purpose for which, it was disclosed.

(8) Except as otherwise provided under this Act or any other law, a data controller shall delete or destroy all personal information under the section.

(9) A data controller may use any personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

PART VIII

PROTECTION OF CRITICAL DATA BASES

Scope of critical database protection

43. The provisions of this Part apply to a critical database administrator and critical databases or parts thereof.

Identification of critical data and critical databases

44. The Minister may, by statutory instrument—

(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 Part; and

(b) establish procedures to be followed in the identification of critical databases for the purposes of this Part.

Registration of critical databases

45. (1) The Minister may, by statutory instrument, determine—

(a) the requirements for the registration of critical databases with the Authority or such other body as the Minister may specify;

(b) the procedure to be followed for the registration of critical databases; and

(c) any other matter relating to the registration of critical databases.

(2) The following information shall be recorded in a register maintained for purposes of this Part:

(a) the full name, address and contact details of the critical database administrator;

(b) the location of the critical database, including the locations of component parts thereof, where a critical database is not stored at a single location; and

(c) a general description of the categories or types of information stored in the critical database, excluding the contents of such critical database.

(3) The information referred to in subsection (2) shall not be recorded in a critical database if that information is likely to prejudice—

(a) the security of the critical database; or

(b) the physical safety of a person in control of the critical database.

Management of critical databases

46. (1) The Minister may prescribe minimum standards in respect of—

(a) the general management of critical databases;

(b) access to, transfer and control of critical databases;

(c) the infrastructural or procedural requirements for securing the integrity and authenticity of critical data;

(d) the procedures and technological methods to be used in the storage or archiving of critical databases;

(e) the disaster recovery plans in the event of loss of critical databases or parts thereof; and

(f) any other matter necessary for the adequate protection, management and control of critical databases.

(2) The regulations referred to in subsection (1) shall, in respect of critical databases administered by public bodies, be made in consultation with the Public Service Commission.

Restrictions on disclosure of information

47. (1) Information contained in a register provided for in section *forty-five* shall not be disclosed to any person other than to officers of a Government department, or other body specified by the Minister, who are responsible for the keeping of the register.

(2) Subsection (1) does not apply in respect of information which is disclosed—

(a) to an authority which is investigating a criminal offence, or for the purposes of any criminal proceedings;

(b) to Government agencies responsible for safety and security in the Republic, pursuant to an official request;

(c) to a cyber inspector for purposes of section *forty-eight*; or

(d) for the purposes of any civil proceedings which relate to the critical data or parts thereof.

Audit of critical database

48. (1) The Authority may cause audits to be performed of a critical database administrator to evaluate compliance with the provisions of this Part.

(2) The audit referred to in subsection (1) may be performed by cyber inspectors or an independent auditor.

Non-compliance with Part

49. (1) The Authority shall, where an audit reveals that a critical database administrator has contravened any provision of this Part, notify the critical database administrator in writing, stating—

(a) the finding of the audit report;

(b) the action required to remedy the non-compliance; and

(c) the period within which the critical database administrator shall take the remedial action.

(2) A critical database administrator that fails to take any remedial action within the period stipulated under subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding one year, or to both.

PART IX

Domain Name Regulation

50. (1) The Authority shall—

(a) administer and manage the .zm domain name space;

(b) comply with international best practice in the administration of the .zm domain name space;

(c) license and regulate registries and the registers for the registries; and

(d) publish guidelines on—

(i) the general administration and management of the .zm domain name space;

(ii) the requirements and procedures for domain name registration; and

(iii) the maintenance of and public access to a repository.

(2) The Authority shall enhance public awareness on the economic and commercial benefits of domain name registration.

(3) The Authority, in relation to domain name regulation—

(a) may conduct such investigations as it may consider necessary;

(b) shall conduct research into, and keep abreast of, developments in Zambia and elsewhere on the domain name system;

(c) shall continually survey and evaluate the extent to which the .zm domain name space meets the needs of the citizens of Zambia; and

(d) may issue information on the registration of domain names in Zambia.

(4) The Authority may, and shall when so requested by the Minister, make recommendations to the Minister in relation to policy on any matter relating to the .zm domain name space.

(5) The Authority shall continually evaluate the effectiveness of this Act and the management of the .zm domain name space.

(6) The Authority may—

(a) liaise, consult and co-operate with any person or other authority; and

(b) appoint experts and other consultants on such conditions as the Authority may determine.

(7) The Authority may delegate any of its functions under this Part to such person or institution as the Authority may determine.

(8) The Authority shall, in relation to the .zm domain name space existing prior to the commencement of this Act, uphold the vested rights and interests of parties involved in the management and administration of the .zm domain name space at the date of its establishment:

Provided that—

(a) the parties shall be granted a period of six months during which they may continue to operate in respect of their existing delegated sub-domains; and

(b) after the expiry of the six-month period, the parties shall apply to be licensed registrars and registries as provided for in this Part.

Licensing of registrars and registries

51. (1) A person shall not update a repository or administer a second level domain unless the person is licensed to do so by the Authority.

(2) An application to be licensed as a registrar or registry shall be made in the prescribed manner upon payment of the prescribed fee.

(3) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Regulations regarding registries, etc.

52. The Minister may, in consultation with the Authority, by statutory instrument, make regulations to provide for—

(a) the requirements which registries and registrars shall meet in order to be licensed, including standards relating to operational accuracy, stability, robustness and efficiency;

(b) the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries;

(c) the pricing policy;

(d) the provisions for the restoration of a domain name registration and penalties for late payments;

(e) the terms of the domain name registration agreement which registries and registrars shall adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution;

(f) the processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of actual or prospective registrants, registries or registrars, protocols or products;

(g) the requirements to ensure that each domain name contains an administrative and technical contact;

(h) the creation of new sub-domains;

(i) the procedures for ensuring the monitoring of compliance with the provisions of this Act, including regular .zm domain name space technical audits; and

(j) any other matter relating to the .zm domain name space as may be necessary to achieve the objectives of this Part.

Dispute resolution Act No. 19 of 2001

53. Any dispute under this Part shall be determined in accordance with the Arbitration Act.

PART X

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

Definition

54. In this Part, "service provider" means any person providing information system services.

Recognition of representative body for service provider

55. (1) The Minister may, on application by a representative body for service providers, by notice in the *Gazette*, recognise such body for purposes of section *fifty-six*.

(2) The Minister shall recognise a representative body referred to in subsection (1) if—

(a) its members are subject to a code of conduct;

(b) its membership is subject to adequate criteria;

(c) the code of conduct requires continued adherence to adequate standards of conduct; and

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

Conditions for eligibility of service provider

56. The limitations on liability established by this Part apply to a service provider if—

(a) the service provider is a member of the representative body referred to in section *fifty-five*; and

(b) the service provider has adopted and implemented the code of conduct of that representative body.

No liability for mere conduit

57. (1) A service provider is not liable for providing access to, or for operating facilities for, information systems or transmitting, routing or storage of data messages through an information system under the service provider's control, as long as the service provider—

(a) does not initiate the transmission;

(b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection of the data; and

(d) does not modify the data contained in the transmission.

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

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and

(c) for a period no longer than is reasonably necessary for the transmission.

(3) Notwithstanding this section, a court may order a service provider to terminate or prevent any unlawful activities under this Act or any other law.

Caching

58. (1) A service provider that transmits data provided by a recipient of the service through an information system under the service provider's control shall not be liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—

(a) does not modify the data;

(b) complies with conditions on access to the data;

(c) complies with guidelines regarding the updating of the data, specified in a manner widely recognised and used by the industry;

(d) does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain information on the use of the data; and

(e) removes or disables access to the data stored upon receiving a take-down notice referred to in section *sixty-one*.

(2) Notwithstanding this section, a court may order a service provider to terminate or prevent any unlawful activities under this Act or any other law.

Hosting

59. (1) A service provider that provides a service consisting of the storage of data provided by a recipient of the service, shall not be liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider—

(a) does not have actual knowledge that the data message, or an activity relating to the data message, is infringing the rights of a third party;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(c) upon receipt of a take-down notification referred to in section *sixty-one*, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless the service provider has designated an agent to receive notifications of infringement and has provided through the service provider's services, including the websites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.

(3) Subsection (1) shall not apply where the recipient of the service is acting under the authority or the control of the service provider.

(4) Notwithstanding this section, a court may order a service provider to terminate or prevent any unlawful activities under this Act or any other law.

Use of information location tools by service provider

60. (1) A service provider shall not be liable for any damage incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, and where the service provider—

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to that data message, infringes the rights of a person.

Take-down notification

61. (1) A recipient of service may, through a take-down notification, notify the service provider of—

(a) any data or activity infringing the rights of the recipient or of a third party;

(b) any unlawful material or activity; or

(c) any other matter conducted or provided contrary to the provisions of this Act.

(2) For the purposes of this Part, a take-down notification to a service provider shall be in writing, addressed by the complainant to the service provider or its designated agent, and shall include—

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) the telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith; and

(h) a statement by the complainant that the information in the take-down notification is to the complainant's knowledge true and correct.

(3) Any person who lodges a false take-down notification with a service provider commits an offence and is liable, upon conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

No general obligation on service provider to monitor unlawful activities

62. (1) Subject to the other provisions of this Part, a service provider shall not be under any obligation to—

(a) monitor the data which the service provider transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

(2) Minister may, on the advice of the Authority, by statutory instrument, prescribe procedures for service providers to—

(a) inform the competent public authorities of alleged illegal activities undertaken, or information provided, by recipients of their service; and

(b) communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Savings

63. This Part does not affect—

(a) the obligation of a service provider acting as such under a licensing or other regulatory system established by, or under, any law;

(b) any obligation imposed by law or by a court, to remove, block or deny access to any data message; or

Cap. 1

(c) any right to limitation of liability based on the Constitution.

PART XI

INTERCEPTION OF COMMUNICATION

Prohibition of interception of communication

64. (1) Except as otherwise provided under this Act, a person shall not—

(a) intercept, attempt to intercept or procure another person to intercept or attempt to intercept, any communication; or

(b) use, attempt to use or procure another person to use or attempt to use any electronic, mechanical or other device to intercept any communication.

(2) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to imprisonment for a period of twenty-five years.

Central Monitoring and Coordination Centre

65. (1) There shall be established a Centre to be known as the Central Monitoring and Coordination Centre.

(2) The Monitoring Centre shall be the sole facility through which authorised interceptions in terms of this Act shall be effected and all the intercepted communication and call-related information of any particular interception target forwarded.

(3) The Monitoring Centre shall be managed, controlled and operated by the department responsible for Government communications.

Power to intercept communication and admissibility of intercepted communication

66. (1) Subject to subsection (2), a law enforcement officer may, where the law enforcement officer has reasonable grounds to believe that an offence has been committed, is likely to be committed or is being committed and for the purpose of obtaining evidence of the commission of an offence under this Act, apply, *ex parte*, to a judge of the High Court, for an interception of communications order.

(2) A law enforcement officer shall, before making an application under subsection (1), obtain the prior written consent of the Attorney-General.

(3) A judge to whom an application is made under subsection (1) may make an order—

(a) requiring a service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that service provider;

(b) authorising the law enforcement officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device;

(c) requiring any person to furnish the law enforcement officer with such information, facilities and assistance as the judge considers necessary for the purpose of the installation of the interception device; or

(d) imposing the terms and conditions for the protection of the interests of the persons specified in the order or any third parties or to facilitate any investigation;

if the judge is satisfied that the written consent of the Attorney-General has been obtained as required by subsection (2) and that there are reasonable grounds to believe that material information relating to—

(i) the commission of an offence under this Act or any other law; or

(ii) the whereabouts of the person suspected by the law enforcement officer to have committed the offence;

is contained in that communication or communications of that description.

(4) Any information contained in a communication—

(a) intercepted and retained pursuant to an order under subsection (3); or

(b) intercepted and retained in a foreign State in accordance with the law of that foreign State and certified by a judge of that foreign State to have been so intercepted and retained;

shall be admissible in proceedings for an offence under this Act, as evidence of the truth of its contents notwithstanding the fact that it contains hearsay.

(5) An interception of communications order referred to in this section shall be valid for a period of three months and may, upon application by a law enforcement officer, be renewed for such period as the judge may determine.

(6) An action shall not lie in any court against a service provider, any officer, employee or agent of the service provider or other specified person, for providing information, facilities or assistance in accordance with the terms of a court order under this Act or any other law.

Interception of communication to prevent bodily harm, loss of life or damage to property

67. (1) A law enforcement officer may, where the law enforcement officer has reasonable grounds to believe that—

(a) a person who is a party to any communication—

(i) has caused, or may cause, the infliction of bodily harm to another person;

(ii) threatens, or has threatened, to cause the infliction of bodily harm to another person;

(iii) threatens, or has threatened, to kill oneself or another person, or to perform an act which would or may endanger that party's own life or that of another person, would or may cause the infliction of bodily harm to that party or another person; or

(iv) has caused or may cause damage to property;

(b) it is not reasonable or practical to make an application under section *sixty-six* for an interception of communications order because the delay to intercept a specified communication or communications would result in the actual infliction of bodily harm, the death of another person or damage to property; and

(c) the sole purpose of the interception is to prevent bodily harm to, or loss of life of, any person or damage to property;

intercept any communication and orally request a service provider to route duplicate signals of indirect communications specified in that request to the Monitoring Centre.

(2) A service provider shall, upon receipt of a request made under subsection (1) by a law enforcement officer, route the duplicate signals of the indirect communications to the Monitoring Centre.

(3) A law enforcement officer who makes a request to a service provider under subsection (1) shall, immediately after making that request, furnish the service provider with a written confirmation of the request setting out the information given by that law enforcement officer to that service provider in connection with the request.

(4) A law enforcement officer who intercepts any communication pursuant to subsection (1) or (2) shall, immediately after the interception of the communication, submit to a judge—

(a) a copy of the written confirmation referred to in subsection (3);

(b) an affidavit setting out the results and information obtained from that interception; and

(c) any recording of the communication that has been obtained by means of that interception, a full or partial transcript of the recording of the communication and any notes made by the law enforcement officer, if nothing in the communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has been caused or is likely to be caused.

(5) A service provider who, in accordance with subsection (2), routes duplicate signals of indirect communications to the Monitoring Centre shall, as soon as practicable thereafter, submit an affidavit to a judge setting out the steps taken by that service provider in giving effect to the request and the results obtained from such steps.

(6) A judge shall keep all written confirmations and affidavits and any recording, transcripts or notes submitted under subsections (4) and (5), or cause it to be kept, for a period of at least five years.

(7) Where a judge, upon receipt of any written confirmation and affidavits under this section, determines that the interception was effected or used for purposes contrary to, or in contravention of the provisions of this Act or any other law, the judge may make such order as the judge considers appropriate in relation to the service provider or the law enforcement officer.

Interception of communication for purposes of determining location in case of emergency

68. (1) Where a person is a party to a communication and that person, as a result of information received from another party to the communication, in this section referred to as the "sender", has reasonable grounds to believe that an emergency exists by reason of the fact that—

(a) the life of another person, whether or not the sender, is being endangered;

(b) a person is dying, or is being or has been injured;

(c) a person's life is likely to be endangered;

(d) a person is likely to die or to be injured; or

(e) property is likely to be damaged, is being damaged or has been damaged; and

the location of the sender is unknown to the person, that person may, if that person is—

(a) a law enforcement officer, and has reasonable grounds to believe that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, a service provider to—

(i) intercept any communication to or from the sender, for purposes of determining the sender's location; or

(ii) determine the location of the sender in any other manner which the service provider considers appropriate; or

(b) not a law enforcement officer, inform, or cause another person to inform, any law enforcement officer of the matter referred to in paragraphs (a), (b), (c), (d) and (e).

(2) A law enforcement officer who receives information under subsection (1) may, if the law enforcement officer has reasonable grounds to believe that determining the location of the sender is likely to be of assistance in dealing with an emergency, orally request, or cause another law enforcement officer to orally request, a service provider to determine the location of the sender.

(3) A service provider shall, upon receipt of a request made under subsection (1) or (2)—

(a) intercept any communication to, or from, the sender for purposes of determining the sender's location; or

(b) determine the location of the sender in any other manner which the service provider considers appropriate;

and if the location of the sender has been so determined, the service provider shall, immediately after determining that location, provide the law enforcement officer who made the request with the location of the sender and any other information obtained from that interception which the service provider determines, is likely to be of assistance in dealing with the emergency.

(4) A law enforcement officer who makes a request to a service provider under subsection (1) or (2) shall—

(a) immediately after making that request, furnish the service provider with a written confirmation of the request setting out the information given by that law enforcement officer to that service provider in connection with the request;

(b) immediately after making that request, furnish a judge with a copy of the written confirmation; and

(c) if the location of the sender and any other information has been provided to the law enforcement officer under subsection (3), immediately after receipt thereof, submit to a judge an affidavit setting out the results and information obtained from that interception.

(5) A service provider who has taken any of the steps referred to in subsection (3), shall, immediately thereafter, submit to a judge—

(a) an affidavit setting out the steps taken by the service provider in giving effect to the request of a law enforcement officer and the results and information obtained from such steps; and

(b) if the steps included the interception of an indirect communication, any recording of that indirect communication obtained by means of the interception, a full or partial transcript of the recording and any notes made by that service provider of the indirect communication.

(6) A judge shall keep all written confirmation and affidavits and any recordings, transcripts or notes submitted under subsections (4) and (5) or cause it to be kept, for a period of at least five years.

(7) Where a judge, upon receipt of any written confirmation and affidavits under this section, determines that the interception was effected or used for purposes contrary to, or in contravention of the provisions of this Act or any other law, the judge may make such order as the judge considers appropriate in relation to the service provider or the law enforcement officer.

Prohibition of disclosure of intercepted communication

69. (1) A law enforcement officer who intercepts any communication pursuant to an interception of communications order shall not disclose the communication or use the communication in any manner other than in accordance with the provisions of this Act.

(2) Except as otherwise provided in this Act, a person who—

(a) without authorisation, accesses, discloses or attempts to disclose to another person, the contents of any intercepted communication; or

(b) without authorisation, uses or attempts to use, the contents of any intercepted communication;

commits an offence and is liable, upon conviction, to imprisonment for a period of twenty-five years.

Disclosure, etc. of intercepted communication by law enforcement officer

70. (1) A law enforcement officer who intercepts any communication pursuant to an interception of communications order may disclose the information to another law enforcement officer where the disclosure is necessary for the determination of the commission of an offence or the whereabouts of a person suspected to have committed an offence.

(2) Where a law enforcement officer, in the performance of any functions under this Act, intercepts any communication relating to the commission of an offence under any other law, the law enforcement officer shall disclose or use the communication in accordance with the provisions of this Act or that other law.

Privileged communication to retain privileged character

71. A privileged wire, oral or electronic communication intercepted in accordance with the provisions of this Act does not lose its privileged character.

Prohibition of random monitoring

72. (1) A service provider shall not utilise the service for observing or random monitoring except for mechanical or service quality control checks.

(2) A service provider who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units, or to imprisonment for a period not exceeding five years, or to both.

(3) In this section—

" monitoring " includes listening to or recording communication by means of a monitoring device; and

" monitoring device " means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.

Protection of user, etc. from fraudulent or other unlawful use of service

73. (1) A service provider shall record that a wire or electronic communication was initiated or completed in order to protect the service provider, another service provider giving a service for the completion of a wire or electronic communication or a user of the service, from fraudulent, unlawful or abusive use of the service.

(2) A service provider who records any electronic communication under subsection (1) shall immediately inform a law enforcement officer.

Disclosure of communication inadvertently obtained by service provider

74. (1) Subject to subsection (2), a service provider shall not disclose the contents of a communication inadvertently obtained through the provision of service to another person other than the addressee, the intended recipient, or an agent of the addressee or intended recipient.

(2) A service provider may disclose the contents of a communication referred to under subsection (1)—

(a) with the consent of the originator, to the addressee or intended recipient of the communication;

(b) to a person employed or authorised, or whose facilities are used, to forward the communication to its destination; or

(c) to a law enforcement officer, where the information relates to the commission of an offence.

(3) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Interception of satellite transmission

75. (1) An interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of transmission to the public or as an audio sub-carrier intended for re-distribution to facilities open to the public is not an offence under this section unless the interception is for the purpose of a direct or indirect commercial advantage or private financial gain.

(2) Subsection (1) does not apply to any data transmission or a telephone call.

Prohibition of use of interception device

76. (1) Subject to subsection (3), a person shall not use an interception device.

(2) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to imprisonment for a period of twenty-five years.

(3) Subsection (1) does not apply to the use of an interception device by a service provider or law enforcement officer—

(a) for the operation, maintenance and testing of a communication service;

(b) to protect the rights or property of the service provider or the users of the service from abuse of service or any other unlawful use of the service;

(c) to record that the communication was initiated or completed in order to protect the service provider or another service provider in the completion of the communication, or a user of the service, from fraudulent, unlawful or abusive use of the service; or

(d) where the consent of the user of the service has been obtained.

Assistance by service providers

77. (1) A service provider shall ensure that the service provider—

(a) uses electronic communications systems that are technically capable of supporting lawful interceptions in accordance with this Act;

(b) installs hardware and software facilities and devices to enable the interception of communications when so required by a law enforcement officer or under a court order;

(c) provides services that are capable of rendering real-time and full-time monitoring facilities for the interception of communications;

(d) provides all call-related information in real-time or as soon as possible upon call termination;

(e) provides one or more interfaces from which any intercepted communication shall be transmitted to the Monitoring Centre;

(f) transmits intercepted communications to the Monitoring Centre through fixed or switched connections, as the case may be; and

(g) provides access to all intercepted subjects operating temporarily or permanently within the service provider's communications systems, and where the interception subject is using features to divert calls to other service providers or terminal equipment, access to such otherproviders or equipment.

(2) A service provider who fails to comply with the requirements of subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Duties of service provider in relation to customers

78. (1) A service provider shall, before entering into a contract with any person for the provision of any service, obtain—

(a) the person's full name, residential address and identity number contained in the person's identity document;

(b) in the case of a corporate body, its business name and address and the manner in which it is incorporated or registered; and

(c) any other information which the service provider considers necessary for the purpose of enabling it to comply with the requirements of this Act.

(2) A service provider shall ensure that proper records are kept of the information referred to in subsection (1) and any change in that information.

Interception capability of service provider

79. (1) Notwithstanding any other law, a service provider shall—

(a) provide a service which has the capability to be intercepted; and

(b) store call-related information in accordance with the provisions of this Act.

(2) The Minister may, after consultation with the Authority, by statutory instrument, make regulations to provide for—

(a) the manner in which effect is to be given to subsection (1) by every service provider;

(b) the security, technical and functional features of the facilities and devices to be acquired by every service provider to enable—

(i) the interception of communication under this Act; and

(ii) the storing of call-related information; and

(c) the period within which the requirements shall be complied with.

(3) The regulations made under subsection (2) shall specify—

(a) the capacity and technical features of the devices or systems to be used for interception purposes;

(b) the connectivity of the devices or systems to be used for interception purposes with the Monitoring Centre;

(c) the manner of routing intercepted information to the Monitoring Centre; and

(d) any other matter which is necessary to give effect to the provisions of this Part.

(4) A service provider shall, at the provider's own expense, acquire the facilities and devices specified in the regulations made under subsection (2).

(5) Subject to this Act, any cost incurred by a service provider for the purpose of—

(a) enabling—

(i) any electronic communication to be intercepted; and

(ii) call-related information to be stored; and

(b) complying with this Part;

shall be borne by the service provider.

PART XII

ACCESS TO STORED COMMUNICATION

Prohibition of disclosure of stored communication

80. (1) Except as otherwise provided under this Act, a service provider shall not disclose to any other person any communication which is electronically stored by the service provider.

(2) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

(3) A provider of remote computing services shall not disclose to any other person the contents of any communication which is carried or maintained on the remote computing service on behalf of a subscriber or solely for the purpose of providing storage or computer processing services to a subscriber, if the provider is not authorised to access the contents of the communication for purposes of providing any service other than storage or computer processing.

(4) A provider of a remote computing service or electronic communication service shall not disclose to any person a record or other information relating to a subscriber or customer of the service.

(5) A service provider may disclose the contents of a communication—

(a) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;

(b) with the consent of the originator, to the addressee or intended recipient of the communication or the subscriber, in the case of a remote computing service;

(c) to an authorised person or employee whose facilities are used to forward the communication to the addressee;

(d) where it is necessary or incidental to the provision or to the protection of the rights or property of the service provider;

(e) to a law enforcement officer where the contents—

(i) are inadvertently obtained by the service provider; and

(ii) relate to the commission of an offence;

(f) where required by any written law; or

(h) where the provider has reasonable grounds to believe that the non-disclosure of the communication is likely to cause death or bodily harm to a person or damage to property.

Disclosure of customer records

81. (1) A service provider may disclose a record or other information relating to a subscriber or customer of a service—

(a) to another person—

(i) with the consent of the customer or subscriber; or

(ii) where it is necessary to service provision or for the protection of the rights or property of theservice provider; or

(b) to a law enforcement officer—

(i) where the service provider has reasonable grounds to believe that the non-disclosure of the record or information is likely to cause death or serious harm to a person; or

(ii) where the service provider has reasonable grounds to believe that the record or information reveals the commission of an offence.

Access to communication in electronic storage

82. (1) A law enforcement officer may, with warrant, access a wire or electronic communication that is in electronic storage in an electronic communications system where the law enforcement officer has reasonable grounds to believe that an offence, is being committed, has been committed or is likely to be committed under this Act or any other law.

(2) The provisions of the Criminal procedure Code relating to warrants shall apply to this Part. Cap. 88

Access to communication in remote computing service

83. (1) A law enforcement officer may, with warrant, access a wire or electronic communication in a remote computing service without notice to the subscriber or customer of the service.

(2) Subsection (1) applies to a wire or electronic communication that is held or maintained by a service provider—

(a) on behalf of a subscriber or customer of the service and received by means of an electronic transmission from, or created by means of a computer processing of communication received by means of electronic transmission from a subscriber or customer of a remote computing service; and

(b) solely for the purpose of providing storage or computer processing services to a subscriber or customer, where the provider is not authorised to access the contents of a communication for purposes of providing any service other than storage or computer processing.

Access to record of electronic communication service or remote computing service

84. (1) A law enforcement officer may, with warrant, access a record or other information relating to a subscriber or customer of an electronic communication or remote computing service.

(2) A provider of electronic communication service or remote computing service shall provide the following information pursuant to a warrant issued under subsection (1):

(a) the name and address of the subscriber;

(b) the subscriber's telephone number or other subscriber number or identity;

(c) the subscriber's local and long distance telephone toll billing records;

(d) the subscriber's local and long distance telephone connection records, or records of session times and durations;

(e) the length of service and types of service utilised by the subscriber;

(f) any temporarily assigned network address of the subscriber; and

(g) the means and source of payment for the service of a subscriber or customer of the service.

(3) An action shall not lie in any court against a service provider, the officers, employees or agents of the service provider or other authorised persons for providing information, facilities or assistance in compliance with a court order, warrant or subpoena under this Act.

PART XIII

ENCRYPTING COMMUNICATION

Use of encrypted communication

85. A person shall use an encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used, in the manner provided for under this Act.

General construction

86. Nothing in this Act shall be construed as requiring the use by a person of any form of encryption that—

(a) limits or affects the ability of the person to use encryption without a key escrow function; or

(b) limits or affects the ability of the person who uses encryption with a key escrow function not to use a key holder.

Prohibition of unauthorised decryption or release of decryption key

87. (1) Unless otherwise provided in this Act, a key holder shall not release a decryption key or decrypt any data without authorisation.

(2) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to imprisonment for a period not exceeding twenty-five years.

(3) A key holder may release a decryption key or decrypt any data or communication—

(a) with the approval of the person whose key is held or managed by the key holder or the owner of the data or communication;

(b) where the release of the decryption key or decryption of the data or communication is necessary or incidental to the provision of encryption services or to the holding or management of the key by the key holder; or

(c) to assist a law enforcement officer pursuant to an interception of communications order to access stored wire or electronic communication or transactional records.

(4) A law enforcement officer to whom a key is released under subsection (3) shall use the key in the manner and for the purpose and duration provided for under a court order authorising the release and use and shall not exceed the duration of the electronic surveillance for which the key is released.

(5) A law enforcement officer to whom an encryption key is released shall, on or before the completion of the authorised release period, destroy the encryption key.

Prohibition of disclosure of record or other information by key holder

88. (1) A key holder shall not disclose a record or any other personal information relating to an owner of a key held or managed by the key holder except—

(a) with the consent of the owner; or

(b) to a law enforcement officer pursuant to a court order.

(2) A recovery agent shall not disclose to any person the use of any stored recovery information, any decrypted data or communication or other assistance provided to a law enforcement officer in the performance of functions under this Act.

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable, upon conviction, to imprisonment for a period not exceeding twenty-five years but not less than fifteen years.

(4) Nothing in this Act shall be construed as prohibiting a recovery agent from—

(a) using or disclosing plaintext in the recovery agent's possession, custody or control;

(b) using or disclosing recovery information that is not stored recovery information held by the recovery agent under the circumstances described in this Act; or

(c) using stored recovery information in the recovery agent's possession, custody or control;

to decrypt any data or communication in the recovery agent's possession, custody or control, where the applicable law otherwise requires the recovery agent to provide the data or communication to a law enforcement officer in plaintext or other form readily understood by the law enforcement officer.

Obstruction of law enforcement officer

89. A person who uses an encryption to obstruct or impede a law enforcement officer or in any manner interferes with the performance by the law enforcement officer of any functions under this Act commits an offence and is liable, upon conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

Sale and acquisition of encryption products

90. (1) A person may sell or acquire—

(a) an encryption product despite the encryption algorithm selected, encryption key length chosen or implementation technique or medium used;

(b) any software, including software with encryption capabilities, that is—

(i) generally available, as is, and designed for installation by the purchaser;

(ii) in the public domain or is publicly available or accessible to the public in any form; or

(iii) a computing device because it incorporates or employs in any form software exempted from any requirement for a validated licence.

(2) In this section—

" generally available " in relation to software, means software that is widely offered for sale, license or transfer including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution or sale on approval;

" as is " in relation to software, means a software program that is not designed, developed or tailored by a software company for specific purchasers;

" is designed for installation by the purchaser " in relation to software, means—

(a) that a software company intends the purchaser who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so; and

(b) that the software program is designed for installation by the purchaser without further substantial support from the supplier;

" computing device " means a device which incorporates one or more micro-processor-based central processing units that can accept, store, process or provide output of data; and

" computer hardware " in relation to information security, includes, but is not limited to, a computer system equipment, application-specific assemblies, modules and integrated circuits.

(3) A purchaser may supply an installation parameter necessary for a software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program.

(4) A company may provide telephone help-line services for software installation, electronic transmission or basic operations.

Prohibition of disclosure or use of stored recovery information

91. (1) A recovery agent shall not—

(a) disclose stored recovery information;

(b) use stored recovery information to decrypt any data or communication; or

(c) disclose any other information or record that identifies a person or entity for whom the recovery agent holds or has held stored recovery information.

(2) A person shall not access any stored recovery information from a recovery agent without authorisation.

(3) A recovery agent may disclose stored recovery information or use stored recovery information to decrypt any data or communication with the consent of the person who stored the recovery information or the agent of that person or pursuant to a court order.

(4) A recovery agent may disclose information or a record, other than stored recovery information, that identifies a person for whom the recovery agent holds or has held stored recovery information pursuant to a court order.

Immunity of recovery agents

92. No cause of action shall lie in any court against a recovery agent for providing information, facilities or assistance to a law enforcement officer in accordance with the terms of a court order.

PART XIV

Cyber Inspectors

Appointment of cyber inspectors

93. (1) The Authority may appoint any person as a cyber inspector to perform the functions provided for in this Part.

(2) The Authority shall provide any person appointed as a cyber inspector with a certificate of appointment.

(3) The certificate of appointment referred to in subsection (2) may be in the form of an advanced electronic signature.

(4) A cyber inspector shall, in performing any function under this Act—

(a) be in possession of a certificate of appointment referred to in subsection (2); and

(b) show the certificate of appointment to any person who requests to see the certificate, is subject to an investigation, or an employee of that person.

(5) A person who—

(a) hinders or obstructs a cyber inspector in the performance of functions under this Part; or

(b) falsely holds oneself out as a cyber inspector;

commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Power to inspect, search and seize

94. (1) A cyber inspector may—

(a) monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity to the appropriate authority;

(b) in respect of a cryptography provider—

(i) investigate the activities of the cryptography service provider in relation to compliance or non-compliance with the provisions of this Act; and

(ii) issue an order in writing to the cryptography provider to comply with the provisions of this Act;

(c) in respect of an authentication service provider—

(i) investigate the activities of an authentication service provider in relation to compliance or non-compliance with the provisions of this Act;

(ii) investigate the activities of an authentication service provider who is falsely holding out the products or services as having been accredited by the Authority or recognised by the Minister; and

(iii) issue an order, in writing, to an authentication service provider to comply with the provisions of this Act; and

(d) in respect of a critical database administrator, perform an audit as provided for in section fifty-four.

(2) In performing any functions under this Act, a cyber inspector may work with a law enforcement officer.

Powers of cyber inspectors

95. (1) A cyber inspector may, in the performance of functions, at any reasonable time, without prior notice, and on the authority of a warrant, enter any premises or access an information system and—

(a) search the premises or that information system;

(b) search any person on the premises if there are reasonable grounds to believe that the person has possession of an article, document or record that has a bearing on an investigation:

Provided that a person shall only be searched by a person of the same sex;

(c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on an investigation;

(d) demand the production of, and inspect, relevant licences and registration certificates;

(e) inspect any facilities on the premises which are linked or associated with the information system;

(f) access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is, or has been used in, connection with any offence;

(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;

(h) require the person by whom, or on whose behalf, the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide the cyber inspector with such reasonable technical and other assistance as the cyber inspector may require for the purposes of this Part; or

(i) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based, have been complied with.

(2) A person who refuses to co-operate with or hinders a cyber inspector from conducting a lawful search or seizure under this section commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

Cap. 88

(3) For purposes of this Act, any reference in the Criminal Procedure Code , to "premises" and "article" includes an information system as well as data messages.

Warrant to enter, etc.

96. (1) A court may, on application by a cyber inspector, issue a warrant.

(2) For the purposes of subsection (1), a court may issue a warrant where—

(a) an offence has been committed within Zambia;

(b) the subject of an investigation is—

(i) a Zambian or ordinarily resident in Zambia; or

(ii) present in Zambia at the time when the warrant is applied for; or

(c) information pertinent to an investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and shall—

(a) identify the premises or information system that may be entered and searched; and

(b) specify which acts may be performed thereunder by the cyber inspector to whom it is issued.

(4) A warrant to enter and search is valid until—

(a) the warrant has been executed;

(b) the warrant is cancelled by the person who issued it or in that person's absence, by a person with similar authority;

(c) the purpose for issuing it has lapsed; or

(d) the expiry of one month from the date on which it was issued.

(5) A warrant to enter and search premises may be executed only during the day, unless the judge who issued it authorises that it may be executed at any other time.

Prohibition of disclosure of information to unauthorised persons

97. (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 Part, obtained access to any information shall not disclose such information to any other person.

(2) Any person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

PART XV

CYBER CRIME

Definition

98. In this Part, "access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that the person is not authorised to access that data and still continues to access that data.

Unauthorised access to, interception of or interference with, data

99. (1) A person who intentionally accesses or intercepts any data without authority or permission to do so or who exceeds the authorised access, commits an offence and is liable, upon conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, commits an offence and is liable, upon conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of these acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item, commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

(4) A person who utilises any device or computer program referred to in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

(5) 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 commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

(6) A person who—

(a) communicates, discloses or transmits any data, information, program, access code or command to any person not entitled or authorised to access the data, information, program, code or command;

(b) introduces or spreads a software code that damages a computer, computer system or network;

(c) accesses or destroys any files, information, computer system or device without authorisation, or for purposes of concealing information necessary for an investigation into the commission, or otherwise, of an offence; or

(d) damages, deletes, alters or suppresses any communication or data without authorisation;

commits an offence and is liable, upon conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

(7) A person who knowingly receives data and is not authorised to receive that data, commits an offence and is liable, upon conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(8) Where an offence under this section is committed in relation to data that is in a critical database or that is concerned with national security or the provision of an essential service, the person shall be liable, upon conviction, to imprisonment for a term of not less than fifteen years but not exceeding twenty-five years.

Computer-related extortion, fraud and forgery

100. (1) A person who performs or threatens to perform any of the acts described in section *eighty-seven*, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

(2) A person who performs any of the acts described in section *eighty-seven* for the purpose of obtaining any unlawful advantage by causing false data to be produced with the intent that it be considered or acted upon as if it were authentic, commits an offence and is liable, upon conviction, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a period not exceeding one year, or to both.

Attempt, aiding and abetting

101. (1) A person who attempts to commit an offence under any provisions of this Act commits an offence and is liable, upon conviction, to the penalties set out in those provisions.

(2) A person who aids or abets someone to commit any of the offences under this Act, commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Prohibition of pornography

102. A person who—

(a) produces pornography for the purpose of its distribution through a computer system;

(b) offers or makes available any pornography through a computer system;

(c) distributes or transmits any pornography through a computer system;

(d) procures any pornography through a computer system for oneself or for another person; or

(e) possesses any pornography in a computer system or on a computer data storage medium;

commits an offence and is liable, upon conviction, to a fine not exceeding nine hundred thousand penalty units or to imprisonment for a period not exceeding ten years, or to both.

Hacking, cracking and introduction of viruses, etc. into computer system

103. A person who hacks into any computer system, or introduces or spreads a virus or malicious software into a computer system or network, commits an offence and is liable, upon conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Denial of service attacks

104. A person who renders a computer system incapable of providing normal services to its legitimate users commits an offence and is liable, upon conviction, to a fine not exceeding nine hundred thousand penalty units or to imprisonment for a period not exceeding ten years, or to both.

Spamming

105. A person who transmits any unsolicited electronic information to another person for purposes of illegal trade or commerce or other illegal activity, commits an offence and is liable, upon conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

Prohibition of illegal trade and commerce

106. (1) A person shall not use the internet as a medium for any illegal activity or trade, fraudulent transaction or to procure any internet-related fraud.

(2) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to imprisonment for a period not exceeding ten years.

Application of offences under this Act

107. (1) Subject to subsection (2), this Act shall have effect in relation to any person, whatever the person's nationality or citizenship, outside as well as within Zambia, and where an offence under this Act is committed by a person in any place outside Zambia, the person shall be dealt with as if the offence had been committed within Zambia.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question—

(a) the accused was in Zambia at the material time;

(b) the computer, program or data was in Zambia at the material time; or

(c) the damage occurred within Zambia whether or not paragraph (a) or (b) applies.

Offence committed by body corporate or un-incorporate

108. If a body corporate or un-incorporate body is convicted of an offence under this Act, every person who—

(a) is a director of, or is otherwise concerned with the management of, the body corporate or un-incorporate body; and

(b) knowingly authorised or permitted the act or omission constituting the offence;

shall be deemed to have committed the same offence and may be proceeded against and punished accordingly.

Cognizable offences Cap.88

109. An offence under this Act shall be deemed to be a cognizable offence for the purposes of the Criminal Procedure Code.

PART XV

General Provisions

General penalty

110. A person who commits an offence under this Act for which no penalty is provided is liable, upon conviction—

(a) in the case of an individual, to a penalty not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both; or

(b) in the case of a body corporate or un incorporate body to a penalty not exceeding one million penalty units.

Evidence obtained by unlawful interception not admissible in criminal proceedings

111. Notwithstanding any other law, evidence which is obtained by means of any interception effected in contravention of this Act, shall not be admissible in any criminal proceedings except with the leave of the court, and in granting or refusing such leave, the court shall have regard, among other things, to the circumstances in which it was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused person that may be occasioned by its admission or exclusion.

Data protection by Investigator-General Cap. 1

112. (1) The Investigator-General appointed under the Constitution, shall supervise the compliance with the provisions of this Act concerning personal data.

(2) When performing the duties under subsection (1), the Investigator-General shall have the right to obtain information and to perform inspections under this Act.

(3) The provisions regarding the lodging and processing of complaints to and by the Investigator-General shall be governed by the Commission for Investigations Act.

Cap. 39

Regulations

113. The Minister may, by statutory instrument, make regulations regarding any matter that may be prescribed in terms of this Act or any matter which it is necessary or expedient to prescribe for the proper implementation or administration of this Act.

Repeal of Act No. 13 of 2004

114. (1) The Computer Misuse and Crimes Act, 2004, is hereby repealed.

(2) Notwithstanding subsection (1), any legal proceedings commenced or pending under the repealed Act shall continue as if instituted under this Act.