THE CYBERSECURITY AND CYBERCRIMES DRAFT BILL, 2017

_____

MEMORANDUM

The objectives of this Bill are to:

(a) authorize the taking of measures to ensure cyber security in Zambia;

(b) establish the Zambia National Cyber Security Agency and provide for its functions;

(c) protect victims against cybercrime;

(d) provide for Child Online Protection;

(e) provide Information and Communication Technology user education on cybersecurity and develop local skills in cyber security;

(f) facilitate identification, declaration and protection of critical information infrastructure;

(g) repeal certain provision in the Electronic and Communications Transactions Act No. 21 of 2009;

(h) provides powers to investigate and prevent cybersecurity incidents

(i) criminalize offences against computers and network related crime;

(j) provide for investigation and collection of evidence for computer and network related crime;

(k) provide for the admission of electronic evidence for such offences; and

(l) 1provide for matters connected with, or incidental to, the foregoing.

,
LIKANDO KALALUKA, S.C.
Attorney-General

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY PROVISIONS

Sections

PART II

ZAMBIA CYBERSECURITY AGENCY

PART III

PREVENTION OF CYBERSECURITY INCIDENTS

PART XIV

LIABILITY

PART XV

GENERAL PROVISIONS

BILL

ENTITLED

An ACT to authorize the taking of measures to ensure cyber security in Zambia; establish the Zambia National Cyber Security Agency and provide for its functions; protect victims against cybercrime; provide for Child Online Protection; provide Information and Communication Technology user education on cybersecurity and develop local skills in cyber security; facilitate identification, declaration and protection of critical information infrastructure; repeal certain provision in the Electronic and Communications Transactions Act No. 21 of 2009; provides powers to investigate and prevent cybersecurity incidents; criminalize offences against computers and network related crime; provide for investigation and collection of evidence for computer and network related crime; provide for the admission of electronic evidence for such offences; and 1provide for matters connected with, or incidental to, the foregoing.

Enactment

ENACTED by the Parliament of Zambia

PART I

PRELIMINARY

Short Title and Commencement

1. This Act may be cited as the Cyber Security and **Cybercrimes** Act No. XX of 201X and shall come into operation on such date as the Minister may, by statutory instrument appoint.

Application

2. This Act shall apply to matters relating to Cyber Security, Cyber Crime, and Child Online Protection.

Interpretation

3. 1In this Act, unless the context otherwise requires-

"Access" in relation to a computer system or electronic communication system, means the entry to, instruct, communicate with, store in, retrieve data from, or otherwise make use of any of the resources of the computer system.

"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 if the data is changed, the signature is invalidated;

"Article" means any data computer program, computer data storage medium or computer system which-

(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission of crime or suspected commission of crime;

(b) may afford evidence of the commission or suspected commission of crime; and

(c) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission of crime;

“Agency” means the Zambia Cyber Security Agency established under section XXX of this Act;

“caching” means the process of storing data in a cache which is a high speed memory that stores data for relatively short periods of time, under computer control, in order to speedup data transmission or processing;

“Child” has the meaning assigned to the word in the Constitution;

“Child pornography” means pornographic material that depicts or represents:

(a) a child engaged in sexually explicit conduct;

(b) a person appearing to be a child engaged in sexually explicit conduct; or

(c) images representing a child engaged in sexually explicit conduct;

this includes, but is not limited to, any audio, visual or text pornographic material;

“Child Solicitation” means soliciting or luring, or attempting to lure through the use of a computer system or device, regardless of the outcome, a child into sexual activity with an adult;

“computer” means any electronic programmable device used, whether by itself or part of a computer system or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing, processing, or storage operations in accordance with set instructions and includes input devices, output devices, processing devices, computer data storage mediums, and other equipment and

devices related to, or connected with the computer system;

"computer data" means any representation of facts, concepts, information in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device;

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

"critical Information" means information that is declared by the Minister to be important for the purposes of national security or economic and social well-being of the people of Zambia;

"critical information infrastructure" refers to a computer or a computer system that is necessary for the continuous delivery of essential services critical to the functioning of the state, whereby the loss or compromise of which will lead to a debilitating impact on national security, defense, foreign relations, economy, public health, public safety or public order;

“Cyber” means the use, simulated environment or state of connection or association with electronic communications systems or networks including the internet;

“Cyber Ecosystem” means the interconnected information infrastructure of interactions among persons, process, data, and information and communications technologies, along with the environment and the conditions that influence those interactions;

“cybersecurity” means the security of a computer or computer system against unauthorized access or attack, to preserve the availability and integrity of the computer or computer system, or confidentiality of information stored or processed therein;

“cyber security incident” refers to an act or activity on or through a computer or computer system, that jeopardizes or adversely impacts, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system;

“Cyber Inspector” refers to a person appointed under Part III, section 8;

“cybersecurity service” refers to a service provided for reward that is intended primarily for or aimed at ensuring or safeguarding the cybersecurity of a computer or computer system belonging to another person;

“Cybersecurity solution” refers to any computer, computer system, computer program or computer service designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system;

“Cybersecurity Threat” refers to an act or activity on or through a computer or computer system, which is known or suspected, that may imminently jeopardize or adversely impacts, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system;

“device” includes but is not limited to -

(a) components of computer systems such as graphic cards, memory, chips and processors;

(b) storage components such as hard drives, memory cards, compact discs, tapes;

(c) input devices such as keyboards, mouse, track pad, scanner, digital cameras;

(d) output devices such as printer, screens;

(e) an apparatus which can be used to intercept a wire, oral or electronic communications;

“Denial of Service” refers to 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;

"electronic Communications" means any transfer of signs, signals or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system;

"Electronic Communications Service provider" means a licensee under the Zambia Information and Communications Technology Authority;

"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;

"forensic tool" means an investigative tool including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address;

"hinder" in relation to a computer system includes but is not limited to:

(a) cutting the electricity supply to a computer system;

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system by any means; and

(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

(e) refusal to avail access to computer systems

“hosting” means any natural or legal person providing an electronic data transmission service by storing of information provided by a user of the service;

“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;

“interception” includes but is not limited to the acquiring, viewing and capturing of any computer data communication whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any technical device;

“Information Infrastructure” means the communication networks and associated software that support interaction among people and organisations;

“illegal activity or trade ” means any fraud-related activity done through the use of a computer system as a medium for illegal trade or any other illegal activity;

“judge” means a judge of the High Court;

“Licensable Cybersecurity Service” refers to any licensable investigative cybersecurity service or licensable non-investigative cybersecurity service;

“Malicious software” is a computer data written to illegally access a computer system , whether with or without user intervention, and thereby either affecting negatively normal computer system usage or modifying data or transmitting data to another computer system;

“multiple electronic mail messages” mean a mail message including E- Mail and instant messaging sent to more than one thousand recipients;

“Investigating Officer” refers to the Commissioner, Deputy Commissioner, any Assistant Commissioner or cybersecurity officer exercising the powers of investigation under this section or section 21, as the case may be;

“Network Traffic” refers to activities on the network relating to a communication indicating the communication’s origin, destination, route, format, time, date, size, duration or type of the underlying service;

“managed security operations centre (SOC) monitoring service” refers to a service for the monitoring, assessment and defence of an organisation’s computer or computer system for the purpose of preventing, detecting and responding to any cybersecurity threats or cybersecurity incidents occurring in the computer or computer system, including preventing unauthorised access to, modification of or copying of any information

stored in or processed by the computer or computer system;

“penetration testing service” refers to a service for assessing, testing or evaluating the cybersecurity of a computer or computer system and the integrity of any information stored in or processed by the computer or computer system], by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system with express permission of the system owner;

“pornography” means material that visually depicts images of a person(s) engaged in explicit sexual conduct;

“racist and xenophobic material” means any material, including but not limited to any image, video audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors;

“traffic data” means computer data that:

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of the chain of communication; and

(c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services;

"utilise" shall include -

(a) developing of a remote forensic tool;

(b) adopting of a remote forensic tool; and

(c) purchasing of a remote forensic tool; and

"Zambia Information and Communications Technology Authority" has the meaning assigned to in the Information and Communications Technology Act No. 21 of 2009.

Application

4. (1) This Act is applicable to the cyber security and cybercrime in Zambia.

PART III

THE ZAMBIA CYBER SECURITY AGENCY

Establishment of Zambia Cyber Security Agency

5. (1) There is established the Zambia Cyber Security Agency which is a body corporate with perpetual succession and a common seal, capable of suing and being sued in its corporate name, and with power, subject to the provisions of this Act, to do all such acts and things as a body corporate may, by law, do or perform.

(2) The seal of the Agency shall be such device as may be determined by the Agency and shall be kept by the Director General.

(3) The affixing of the seal shall be authenticated by the Chairperson or the Vice-Chairperson and the

Director General or one other person authorised in that regard by a resolution of the Board.

(4) The provisions of the First Schedule apply to the **Agency**.

Autonomy of the Agency

6. Except as otherwise provided in this Act, the Agency shall be an autonomous body.

Functions of Agency

7. (1) The Agency shall without limiting the generality of its powers perform the following functions:

(a) coordinate the Zambia Computer Incidence Response Team;

(b) coordinate and oversee all activities related to cybercrime and cybersecurity;

(c) develop and promote an all-inclusive secure cyber ecosystem;

(d) create a safer cyber space in Zambia;

(e) coordinate the protection of Zambia's critical information infrastructure;

(f) establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure;

(g) promote, develop, maintain and improve competencies, expertise and professional standards in the cybersecurity community;

(h) Promote research and development the use of new and appropriate technologies and techniques in cyber security and cyber crimes.

(i) Promote the manufacturing and production of localised relevant apparatus;

(j) promote awareness of the need for and importance of cybersecurity;

(k) set mechanisms of cooperation with cyber security agencies of other countries and strengthen international partnerships in combating cybercrime;

(l) the Agency shall issue regulations concerning its rules of procedure within six months following its operationalisation. These regulations shall be published in the Government Gazette. These regulations shall establish the proceedings for:

(i) the deliberations, instruction and presentation of the cases heard by the Agency;

(ii) the complaints, inquiries and sanctions administered by the Agency; and

(iii) all other proceedings handled by the Agency

(m) perform such other functions and discharge such other duties as may be conferred under any other written law of the land;

(n) coordinate with Law enforcement agencies to ensure safe cyber space in

Zambia and coordinating investigations of national cyber incidences.

(2) The Agency shall consult the Zambia Information and Communications Technology Authority on any matter relating to consumer protection in the cyber ecosystem.

The Board of Agency

8. There is constituted the Board of the Agency which shall consist of the following Part time members appointed by the Minister -

(a) a representative each from the following security wings:

(i) the Zambia Air force;

(ii) the Zambia Army;

(iii) the Zambia National Service;

(iv) the Zambia Police; and

(v) the Zambia Security Intelligence Services;

(b) a representative from the Ministry responsible for communications;

(c) a representative from Engineering Institute of Zambia;

(d) a representative from the Law Association of Zambia; and

(e) one other person appointed by the Minister with experience in cyber security.

Functions of the Board

9. (1) The Board shall be the governing body of the Agency and shall exercise and perform the functions of the Agency.

(2) Without prejudice to the generality of subsection (1), the functions of the Board are to—

(a) oversee the implementation and successful operation of the policy and functions of the Agency;

(b) review and approve the policy and strategic plans of the Agency;

(c) approve the annual budget and plans of the Agency;

(d) approve codes of practice and standards of performance for critical information infrastructure protection;

(e) approve the investment of the funds of the Agency in accordance with Ministerial approval and relevant regulations;

(f) monitor and evaluate the performance of the Agency against budgets and plans; and

(g) do all such things as are connected with, or incidental to, the functions of the Board under this Act.

(3) The Minister may enter into a performance contract with the Board for a specified period, which shall be consistent with the provisions of this Act.

(4) Subject to the other provisions of this Act, the Board may, by direction, in writing, and subject to any terms and conditions as it considers necessary, delegate to the Executive Director any of its functions under this Act.

(5) A delegation made under subsection (1) shall—

(a) be in writing;

(b) be subject to a condition or restriction imposed by the Board; and

(c) not prevent the exercise of that power by the Board.

(6) The Board may amend or withdraw a delegation at any time, in writing.

Director-General

10. (1) The Board shall appoint the Director-General on the terms and conditions determined by the Emoluments Commission.

(2) The Director-General shall be the chief executive officer of the Agency and shall be responsible, under the general direction of the Board, for—

(a) the management and administration of the affairs of the Agency;

(b) the implementation of the decisions of the Board; and

(c) any other function assigned or delegated to the Director-General by the Board or under this Act.

(3) The Director-General shall attend the meetings of the Board and may address those meetings but shall not vote on any matter.

(4) The Director-General may, with the approval of the Board, delegate any of the Director-General's function under this Act to any other member of staff of the Agency.

Secretary and other staff

11. (1) The Board shall appoint, on the terms and conditions that the Emoluments Commission may determine, the Secretary and other staff of the Agency that

it considers necessary for the performance of the functions of the Agency.

(2) The Secretary shall perform corporate secretarial duties for the Board and such other functions as the Board may determine, under the direction of the Board and the Director-General.

PART III
PREVENTION OF CYBERSECURITY INCIDENTS

Powers to investigate

12. (1) Where information regarding a cybersecurity threat or a cybersecurity incident has been received by the Agency, the Director General may, having regard to the impact or potential impact of the cybersecurity threat or cybersecurity incident:

(a) require, by written notice, any person to attend at such reasonable time and at such place as may be specified in the notice to answer any question or to provide a signed statement in writing concerning the cybersecurity incident or cybersecurity threat;

(b) require, by written notice, any person to produce to the investigating officer any physical or electronic record, document or copy thereof in the possession of that person, or to provide the investigating officer with any information, which the investigating officer considers to be

relevant to the investigation, and without giving any fee or reward;

(c) inspect, copy or take extracts from any physical or electronic record or document; and

(d) examine orally any person who appears to be acquainted with the facts and circumstances relating to the cybersecurity incident or cybersecurity threat, and to reduce to writing any statement made by the person so examined.

(2) The cyber inspector may specify in the notice mentioned in subsection (1)(b):

(a) the time and place at which any record or document is to be produced or any information is to be provided; and

(b) the manner and form in which it is to be produced or provided.

(3) A person examined under this section who, in good faith, discloses any information to a cyber inspector is not treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.

(4) If any person fails to attend as required by a written notice under subsection (1)(a), the cyber inspector may report such failure to a court with competent jurisdiction which may then issue a warrant to secure the attendance of that person as required by the written notice.

(5) A person who -

(a) willfully gives false information or without lawful excuse refuses to give any information or produce any record, document or copy thereof required of the person by the cyber inspector under subsection (1); or

(b) refuses to cooperate with or hinders a cyber inspector from conducting a lawful search, or seizure commits an offence and

is liable on conviction to a fine not exceeding [XX] or to imprisonment for a term not exceeding [X months] or to both.

Prevention of Cybersecurity Incidents

13. (1) Where information has been received by the Commissioner regarding a cybersecurity threat or a cybersecurity incident that satisfies the severity threshold in subsection (2) the National Cybersecurity Agency may exercise such of the following powers as may be necessary to determine the impact or potential impact of the cybersecurity threat or cybersecurity incident, to prevent further harm arising from the cybersecurity incident, or to prevent a further cybersecurity incident from arising from that cybersecurity threat or cybersecurity incident:

(a) any power mentioned in section 20(1)(a), (b) or (c);

(b) direct, by written notice, any person to carry out such remedial measures, or to cease carrying on such activities, as may be specified, in relation to a computer or computer system that the investigating

officer has reasonable cause to suspect is or was impacted by a cybersecurity incident, in order to minimize cybersecurity vulnerabilities. The remedial measures directed to be carried out may include:

(i) the cleaning up of computers that have been infected by malware;

(ii) the installation of software updates to address cybersecurity vulnerabilities;

(iii) temporarily disconnecting infected computers from a computer network subject to completion of (a) and (b);

(iv) the redirection of malicious data traffic to designated computer servers.

(c) require the owner of a computer or computer system to carryout steps to assist with the investigation, including but not limited to -

(i) preserving the state of the computer or computer system by not using it;

(ii) monitoring the computer or computer system for a specified period of time;

(iii) performing a scan of the computer or computer system to detect cybersecurity vulnerabilities; and

(iv) allowing the investigating officer to install on the computer or computer system any software program, or interconnect any equipment to the computer or computer system, for the purpose of the investigation.

(d) after producing the investigating officer's identification card on demand being made, enter with reasonable notice any premises owned or occupied by any person suspected to have within the premises a computer or computer system that the investigating officer has reasonable cause to suspect is or was impacted by a cybersecurity incident;

(e) access, inspect and check the operation of a computer that the investigating officer has reasonable cause to suspect is or was impacted by a cybersecurity incident, or use or cause to be used any such computer to search any data contained in or available to such computer;

(f) perform a scan of a computer or computer system to detect cybersecurity vulnerabilities;

(g) take a copy of, or extracts from, any electronic record or program contained in a computer that the investigating officer has reasonable cause to suspect is or

was impacted by a cybersecurity incident; and

(h) subject to subsection (4) or with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

(2) A cybersecurity incident or cybersecurity threat satisfies the severity threshold mentioned in subsection (2) if:

(a) it creates a real risk of significant harm being caused to a critical information infrastructure;

(b) it creates a real risk of disruption being caused to the delivery of an essential service;

(c) it creates a [real] threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Zambia; or

(d) the cybersecurity threat is of a severe nature, in terms of the severity of harm that may be caused or the number of computers or value of information put at risk, whether or not the computers or computer systems put at risk are of the nature of a critical information infrastructure.

(3) The cyber inspector exercising the power mentioned in subsection (1)(e) may require any assistance needed to gain such access from:

(a) any person whom the cyber inspector reasonably suspects of using or having used the computer impacted by the cybersecurity incident; or

(b) any person having charge of, or otherwise concerned with the operation of, such computer.

(4) Where the owner of the computer or other equipment does not consent to the exercise of the power mentioned in subsection (1)(h), the power may be exercised only after the Director-General has issued to the cyber inspector a written authorisation after being satisfied that:

(a) the exercise of the power is necessary for the purposes of the investigation;

(b) there is no less disruptive method of achieving the purpose of the investigation; and

(c) after consultation with the owner, and having regard to the importance of the computer or other equipment to the business or operational needs of the owner, the benefit from the exercise of the power outweighs the detriment caused to the owner.

(5) Any person who —

(a) willfully mis-states or without lawful excuse refuses to give any information or produce any record, document or copy thereof required of the person by the

investigating officer under subsection (1)(a); or

(b) fails, without reasonable excuse, to comply with a lawful demand of the investigating officer in the discharge by the investigating officer of the investigating officer's duties under this section, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding {XXXX} or to imprisonment for a term not exceeding {XX years} or to both.

Appointment of cyber inspector

14. (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

15. (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 critical information infrastructure, perform an audit.

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

……..

16. (1) A law enforcement officer or cyber inspector 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.

Internet connection record

17. (1) An Internet connection record (‘ICR’) is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is communications data which may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunications system for the purpose of obtaining access to, or running, a computer file or program. It comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of

the communication. In most cases ICRs will be held by internet access providers which are telecommunications operators which provide access to the internet and can include a home broadband connection, mobile internet or publicly available Wi-Fi.

(2) An ICR will only identify the service that a customer has been using. It is not intended to show what a customer has been doing on that service. For example many social media apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the public authority to make further enquiries of the service provider identified through an ICR. An ICR may consist of:

(a) a customer account reference – this may be an account number or an identifier of the customer's device or internet connection;

(b) the date/time of the start and end of the event or its duration;

(c) the source IP address and port;

(d) the destination IP address and port – this is the address of the service accessed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc.);

(e) the volume of data transferred in either, or both, directions;

(f) the name of the internet service or server connected to; and

(g) those elements of a URL which constitute communications data – this is the web address which is the text you type in the address bar in an internet browser. In most cases this will simply be the domain name – e.g. socialmedia.com.

(3) The core information that is likely to be included is: an account reference, a source IP and port address, a destination IP and port address and a time/date. However, there is no single set of data that constitutes an internet connection record, it will depend on the service and service provider concerned.

(4) Where a data retention notice is issued requiring a CSP to retain ICR the specific data that an internet access provider may be required to retain will be discussed with the provider before the requirement is imposed13.

(5) A CSP cannot be required to retain third party data as part of an ICR.

(6) ICRs can include connections which are made automatically by a person's browser or device.

Power of cyber inspectors

18. (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.

(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.

Cap. 88

Warrant to enter, etc

19. (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

20. (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.

Appointment of Cybersecurity Technical Expert

21. (1) The Director-General may, appoint any of the following individuals to be a cybersecurity technical expert for a specified period to assist any cyber inspector in the cyber inspector's exercise of any powers under section 12 or 13:

(a) a public officer or an employee of a statutory body with experience in cybersecurity;

(b) an individual, who is not a public officer or an employee of a statutory body, with suitable qualifications or experience to properly perform the role of a cybersecurity technical expert; or

(c) a full time law enforcement officer with relevant experience in cybersecurity.

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

(3) The Director-General may, for any reason that appears to the Director General to be sufficient, at any

time revoke an individual's appointment as a cybersecurity technical expert.

(4) The Director-General must issue to each cybersecurity technical expert an identification card, which must be carried at all times by the cybersecurity technical expert when performing the role of a cybersecurity technical expert under any provision in this Act.

(5) A cybersecurity technical expert whose appointment as such ceases must return any identification card issued to the cybersecurity technical expert under subsection (3) to the Director-General.

(6) An individual mentioned in subsection (1)(b) [or (c)] who is appointed as a cybersecurity technical expert under that subsection does not, by virtue only of that appointment, become an employee or agent of the Government.

Emergency cybersecurity measures and requirements

22. (1) Where the Minister is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the essential services or national security, defence, foreign relations, economy, public health, public safety or public order of Zambia, the Minister may, by a certificate under the Minister's hand, authorise or direct any person or organisation specified in the certificate (referred to in this section as the specified person) to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service] [system] or any class of computers or computer services] [systems].

(2) The measures and requirements referred to in subsection (1) may include, without limitation:

(a) the exercise by the specified person of the powers referred to in sections 39(1)(a) and (b) and (2)(a) and (b) and 40(2)(a),(b) and (c) of the Criminal Procedure Code (Cap. 68);

(b) requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer [service][system]; and

(ii) information relating to the security of any computer, computer program or computer [service][system];

(c) providing to the Minister or [the Director General][a public officer authorised by the Minister] any information (including real-time information) obtained from any computer controlled or operated by the specified person, or obtained by the specified person from another person pursuant to a measure or requirement under paragraph (b), that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer [service][system]; and

(ii) information relating to the security of any computer, computer program or computer [service] [system]; and

(d) providing to the Minister or [the Commissioner][a public officer authorised by the Minister] a report of a breach or an attempted breach of security of a description specified in the certificate under subsection (1), relating to any computer controlled or operated by the specified person.

(3) Any measure or requirement referred to in subsection (1), and any direction given by a specified person for the purpose of taking any such measure or complying with any such requirement —

(a) does not confer any right to the production of, or of access to, information subject to legal privilege; and

(b) subject to paragraph (a), has effect notwithstanding any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on disclosure of information imposed by law, contract or rules of professional conduct.

(4) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding XXXX or to imprisonment for a term not exceeding XX years or to both.

(5) Any person who, without reasonable excuse —

(a) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (1); or

(b) fails to comply with any direction given by a specified person for the purpose of the specified person taking any such measure or complying with any such requirement, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding XXX or to imprisonment for a term not exceeding XX years or to both.

(6) No civil or criminal liability is incurred by —

(a) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (1); or

(b) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying

with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement.

(7) The following persons are not to be treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct:

(a) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection, or who discloses any information to the Minister or {the Director General} a public officer authorised by the Minister, in compliance with any requirement under that subsection;

(b) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection.

(8) The following persons, namely:

(a) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure

under subsection (1) or complying with any requirement under that subsection;

(b) a person to whom a specified person provides information in compliance with any requirement under subsection (1), must not use or disclose the information, except —

(i) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person;

(ii) for the purpose of preventing, detecting or countering a threat to a computer, computer [service] [system] or class of computers or computer [services][systems];

(iii) to disclose to any police officer or other law enforcement authority any information which discloses the commission of an offence under this Act, the Computer Misuse and Cybersecurity Act or any other written law; or

(iv) in compliance with a requirement of a court or the provisions of this Act or any other written law.

(9) Any person who contravenes subsection (8) shall be guilty of an offence and shall be liable on

conviction to a fine not exceeding XX or to imprisonment for a term not exceeding XX months or both.

(10) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —

(a) no information for that offence may be admitted in evidence in any civil or criminal proceedings; and

(b) no witness in any civil or criminal proceedings is obliged —

(i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or

(ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(11) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contains any entry in which any informer is named or described or which may lead to the informer's discovery, the court must cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

PART V
PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

Scope of protecting critical Information Infrastructure

23. (1) The provisions of this Part apply to a critical database and/or Critical Information Infrastructure or parts thereof.

(2) The provisions of this part apply to the handlers of these critical database and information infrastructure i.e. database Administrators, network Administrators, Cloud Engineers.

(3) The provisions of this part mandates the undertaking of various security audits on all critical databases and information infrastructure.

Identification and designation of critical databases and Information infrastructure

24. (1) The Minister may in consultation with Established Institutions and after consultations with the owner or the person in control of any critical database or information infrastructure which is identified as potentially critical to national security and economic sovereignty declare as such.

(2) Establish procedures to be followed in the identification and designation of critical databases or information infrastructure for the purposes of this Part. The Minister may by written Notice, designate as critical database or information infrastructure if-

(a) the database or information infrastructure fulfils the criteria set through a consultative process; and

(b) the database or information infrastructure is located wholly or partly in Zambia.

(3) Any Notice made under subsection (1) must —

(a) identify the specific database or information infrastructure that is being designated as a critical information infrastructure;

(b) identify the owner of the database or information infrastructure that is being designated as a critical information infrastructure;

(c) inform the owner of the database or information infrastructure, regarding the owner's duties and responsibilities under the Act that arise from the designation;

(d) provide the name and contact particulars of the designated Officer from the National Cyber Security Agency to oversee the critical database or information infrastructure;

(e) inform the owner that any representations against the designation are to be made to the Director General not later than 14 days after the date of the notice; and

(f) inform the owner of the avenue to appeal to the Minister against the designation, and the applicable procedure.

(4) Any notice made under subsection (1) continues to have effect for a period of XX years unless it is withdrawn by the Director General before the expiry of the period.

(5) The owner of a Critical Database or Information Infrastructure that is designated as critical by Notice under subsection (1) must, not later than 14 days after the receipt of the notice –

(a) acknowledge receipt of the Notice in writing; and

(b) appoint a contact person for the critical database or information infrastructure.

Registration of Critical Databases and Information Infrastructure

25. (1) The Minister may, by Statutory Instrument, determine-

(a) the requirements for the registration of critical Databases or Information Infrastructure with the national cyber security Agency;

(b) the procedure to be followed for the registration of critical Databases or Information Infrastructure; and

(c) any other matter relating to the registration of critical Databases or Information Infrastructure

(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 or information infrastructure handlers;

(b) The location of the critical database or information infrastructure , including the locations of the component parts thereof, where a critical database or information

infrastructure 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.

Change in ownership of Critical Database and Information Infrastructure

26. (1) An owner of a critical information infrastructure must inform the Director General of any intended change in ownership of the critical information infrastructure, not later than 90 days before the date of the intended change in ownership.

(2) Any owner of a critical information infrastructure who fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [XXX] or to imprisonment for a term not exceeding [XX years] or to both.

Auditing of critical information infrastructure to ensure compliance

27. (1) The Cyber Security Agency may cause audits to be performed of a critical information infrastructure, database and/or application.

(2) The Agency may evaluate compliance with provision of this Act and any subsidiary laws that may be issued;

(3) The owner or person in control of a critical information infrastructure must, once every 24 months, at own cost, cause an audit to be performed on the critical information infrastructure by an independent auditor in order to evaluate compliance with the directives issued in compliance of this Act.

Duty to report cyber security incidents in respect of critical information infrastructure

28. (1) An owner of a critical information infrastructure must notify the Commissioner in such manner and form as may be prescribed, within the prescribed period after the occurrence of any 5 of the following events:

(a) a significant cybersecurity incident in respect of the critical information infrastructure;

(b) a significant cybersecurity incident in respect of any computer or computer system under the owner's control that 10 is interconnected with or communicates with the critical information infrastructure;

(c) any other type of cybersecurity incident in respect of the critical information infrastructure that the Minister may prescribe by notification or the Commissioner may specify 15 by written direction;

(d) the owner of the critical infrastructure shall submit a cyber security incident and threat report to be issued monthly to the Zambia Cyber Security Agency.

(2) An owner of a critical information infrastructure must establish mechanisms and processes as may be necessary in order to detect any cybersecurity threat in respect of its critical information infrastructure.

(3) Any owner of a critical information infrastructure who fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [$100,000] or to imprisonment for a term not exceeding [2 years] or to both.

Designation of persons administering Critical Databases and Information Infrastructure

29. (1) The processing of non-sensitive personal data is permitted, without the consent of the data subject:

(a) that may be material as evidence in proving an offence;

(b) for compliance with an obligation to which the controller is subject by or by virtue of a law;

(c) in order to protect the vital interests of the data subject;

(d) for the performance of a task carried out in the public interest, or in the exercise of the official authority vested in the controller, or in a third party to whom the data is disclosed;

(e) for the promotion of the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the

data subject claiming protection under this Act.

(2) The Authority can specify the circumstances in which the condition stipulated under (e) is considered as not having been met.

Restrictions on disclosure of information

30. (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,

(b) or for the purposes of any criminal proceedings;

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

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

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

National Cybersecurity Exercises

31. (1) The National Cyber Security Agency may conduct national cyber Security exercises for the purposes of testing the state of readiness of owners of different critical information infrastructure in responding to significant cybersecurity incidents at the national level.

(2) An owner of a critical information infrastructure must participate in any national cyber Security exercises as directed in writing by the Commissioner.

(3) Any person who fails to comply with a written direction issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [XXX] [or to imprisonment for a term not exceeding [XX years] or to both] and, in the case of a continuing offence, to a further fine not exceeding [$5,000] for every day or part thereof during which the offence continues after conviction.

Non Compliance with Part

32. (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 V
INTERCEPTION OF COMMUNICATIONS

Prohibition of Interception of Communication

33. (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 offense and is liable, upon conviction, to imprisonment for a period of twenty-five years

Central Monitoring and Coordination Centre

34. (1) There is established the Central Monitoring and Coordination Centre.

(2) The Central Monitoring and Coordination Centre is 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 Central Monitoring and Coordination Centre shall be managed, controlled and operated by the department responsible for Government communications in liaison with the Agency.

Power to intercept Communication and Admissibility of Intercepted Communications

35. (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);

(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; or

(c) 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

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

(a) a person who is a part 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) to 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

37. (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;

(2) the location of the sender is unknown to the person, that person may, if that 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).

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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

38. (1) A law enforcement officer who intercepts any communication pursuant to an interception of communications order shall not disclose the communications or use the communications 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 of Intercepted communication by Law Enforcement Officer

39. (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

40. 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

41. (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 from fraudulent or other unlawful use of service

42. (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

43. (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

44. (1) An interception of 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

45. (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

46. (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 other providers 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

47. (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

48. (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 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 VI
ZAMBIA NATIONAL STRUCTURE TO DEAL WITH CYBER SECURITY

The Zambia Computer Incidence Response Team

49. (1) The Agency shall constitute the Zambia Computer Incidence Response Team.

(2) The Agency may, by statutory instrument, make regulations to provide for the composition, tenure, and procedure of the Zambia Computer Incidence Response Team.

(3) The Zambia Computer Incidence Response Team constituted under sub-section (1) shall –

(a) be the first point of contact with reference to the handling of cyber incidents and communication between local, regional and international cyber security emergency response teams or cyber security incident response teams to address cyber incidents or incidents of a similar nature as it affects national critical information infrastructure;

(b) provide incident response and management services, in a coordinated manner, via established industry standard policies and procedures to manage threats associated with cyber incidents;

(c) provide alerts and warnings on the latest cyber threats and vulnerabilities which can impact the national community;

(d) assess and analyse the impact of incidents such as, but not limited to network security breaches, website hackings, virus and network attacks, in order to develop

strategies and measures to counteract these incidents;

(e) assess the work of incident response teams within the public and private sector;

(f) participate in trusted information sharing and disseminate information with international cyber security incident response teams and computer emergency response teams on the emerging threats to critical information infrastructure and Internet resources;

(g) participate in and be a member of regional and international computer emergency response team groups, for collaborative efforts to fight cyber incidents; and

(f) perform any other functions conferred on the Zambia Computer Incidence Response Team by the Agency for purposes of this Act.

(4) The Zambia Computer Incidence Response Team will create a national image by cooperating with international CIRTs for cyber security and Cybercrime.

Established Government Structures Supporting Cyber Security

50. (1) The National Joint Standing Committee on Defense and Security shall provide and formulate key policy decisions in the sphere of Cyber Security in Zambia.

(2) The Committee shall coordinate with the Presidency to sanction emergency cybersecurity measures

with recommendation from the National Cyber Security Agency.

(3) The Institution responsible for State Security shall continue to provide strategic intelligence operations with the National Cyber Security Agency by maintaining sufficient human and operational capacity to give effect to cyber security measures under the Anti-Terrorism Act of 2007, the State Securities Act and the Zambia Intelligence Security Act.

(4) The Ministry responsible for defense and the Defense wings created under the Act No XX of 19XX and ZAF Act No. of 19XX will continue to work with the National Cyber Security Agency by maintaining a cyber offensive and defensive capacity as part of the defense mandate and obligations.

(5) The Ministry responsible for home affairs and the law enforcement agencies shall jointly conduct investigations with the National Cyber Security Agency into potential cybersecurity threats and incidents by-

(a) maintaining sufficient human and operational capacity to detect, prevent and investigate cybercrimes; and

(b) ensure that law enforcement officers are trained in aspects relating to the detection, prevention and investigation of cybercrimes.

(6) The Ministry responsible for communications will work closely with the Zambia Cyber Security Agency to establish and maintain a Cyber Security Hub that will promote the interface with the private businesses and the ordinary consumers.

Recognised Private Sector Structure supporting Cyber

51. The Minister responsible for communications shall recognise and declare certain private sector players which provide an electronic communication service as a duly recognised private sector contact to liaise on the vulnerabilities affecting that sector with the Zambia Cyber Security Agency. (appropriate text to be provided)

Promotion of Information Sharing on Cybersecurity related matters

52. The Minister in consultation with the Minister responsible for justice will make regulations to regulate information sharing, for the purposes of this part, regarding-

(a) Cyber Security Incidents;

(b) the detection, prevention, investigation or mitigation of cybercrime. (to recast)

PART VII

CYBERSECURITY SERVICE PROVIDERS

Conducting Licensable Investigative Cyber Security Services without a License

53. (1) A person shall not —

(a) [carry out][perform], for reward (whether in the course of business or of employment), any licensable investigative cybersecurity service; or

(b) advertise, or in any way hold out, that the person [carries out][performs] or is willing to [carry out][perform] for reward any licensable investigative cybersecurity service, except under and in accordance with an investigative cybersecurity service practitioner’s licence granted under this Act.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding XXXX or to imprisonment for a term not exceeding XX years or to both.

(3) This section does not apply to a person employed under a contract of service by another person to carry out an investigative cybersecurity service for a computer or computer system belonging to that other person.

Condition to supply licensable investigative Cyber Security Practitioners without license

54. (1) No person may -

(a) engage in the business of supplying to other persons, for reward, the services of investigative cybersecurity practitioners for the [carrying out][performance] of a licensable investigative cybersecurity service; or

(b) advertise, or in any way hold out, that the person supplies for reward, or is willing to supply for reward, the services of investigative cybersecurity practitioners for the [carrying out][performance] of a licensable investigative cybersecurity service,

except under and in accordance with [a licensable][an] investigative cybersecurity service provider's licence granted under this Act.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding XXXX or to

imprisonment for a term not exceeding XX years or to both.

Conditions for employees who are investigative Cyber Security Service Practitioners

55. (1) No person may employ another person as an investigative cybersecurity service practitioner for the [carrying out][performance] of a licensable investigative cybersecurity service unless the other person is a licensed investigative cybersecurity service practitioner.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 2 years or to both.

Conditions for providing licensable non-investigative cyber security service without license

56. (1) No person may -

(a) engage in the business of providing, for reward, any licensable non-investigative cybersecurity service to other persons; or

(b) advertise, or in any way hold out, that the person (who is in the business of providing a licensable non-investigative cybersecurity service) provides for reward, or is willing to provide for reward, the licensable non-investigative cybersecurity service, except under and in accordance with a [licensable] non-investigative cybersecurity service provider’s licence granted under this Act.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [XXXX] or to

imprisonment for a term not exceeding XX years or to both.

Cyber Security Licensing Officers

57. (1) For the purposes of this Part, the National Cyber Security Agency is the licensing entity and the Director General will be responsible for the administration of this Part.

(2) The Director General may appoint such number of public officers to be assistant licensing officers as are necessary to assist in carrying out the functions and duties under this Part.

(3) The functions and duties conferred on the Director General by this Part may be performed by any assistant licensing officer appointed by the Commissioner under subsection (2) and subject to the direction and control of the Director General.

(4) The Minister may from time to time give to the Director General such directions, not inconsistent with the provisions of this Part, as the Minister may consider necessary for carrying out the provisions of this Part, and the Commissioner must comply with any direction so given.

Grant and renewal of License

58. (1) An application for the grant or renewal of a licence must be -

(a) made to the licensing officer in such form or manner as maybe prescribed;

(b) accompanied by the prescribed fees, if any; and

(c) in the case of an application for the renewal of a licence, made not later than

one month or such other period before the expiry of the licence (called in this section as the late renewal period) as may be prescribed.

(2) An applicant for a licence must, at the request of the licensing officer, provide any further information or evidence that the licensing officer may require to decide the application.

(3) Upon receipt of an application under subsection (1), the licensing officer may -

(a) grant or renew the licence applied for, with or without conditions; or

(b) refuse the application.

(4) Subject to the provisions of this Act, a person who applies to be licensed, or to renew the person's licence, is eligible to be granted a licence or a renewal of the licence if, and only if -

(a) the applicant has paid the prescribed fees for such licence or its renewal;

(b) where the applicant is an individual, the applicant satisfies the licensing officer that the applicant has the qualifications and the practical experience (whether in Zambia or elsewhere) prescribed for that licence; and

(c) the applicant satisfies such other requirements as may be prescribed for such licence or its renewal.

(5) Without prejudice to subsection (4), the licensing officer may refuse to grant a licence, or to renew

a licence of a person if, in the opinion of the licensing officer -

(a) where the person who applies to be licensed, or to renew the person's licence is an individual, the person is not a fit or proper person to hold or to continue to hold the licence;

(b) where the person who applies to be licensed, or to renew the person's licence is a business entity, an officer of the business entity is not a fit or proper person; or

(c) it is not in the public interest to grant or renew the licence, or the grant or renewal of the licence may pose a threat to national security.

(6) Where a person submits an application for the renewal of the person's licence before the late renewal period, the licence continues in force until the date on which the licence is renewed or the application for its renewal is refused, as the case may be.

(7) Any person who, in making an application for a licence-

(a) makes any statement or furnishes any particulars, information or document which the person knows to be false or does not believe to be true; or

(b) by the intentional suppression of any material fact, furnishes any information which is misleading in a material particular, shall be guilty of an offence

and shall be liable on conviction to a fine not exceeding [XXXX] or to imprisonment for a term not exceeding [XX year] or to both.

(8) In deciding for the purposes of this section whether a person or an officer of a business entity is a fit and proper person, the licensing officer may consider any of the following matters as indicating that the person or officer may not be a fit and proper person:

(a) that the person or officer associates with a criminal in a way that indicates involvement in an unlawful activity;

(b) that in dealings in which the person or officer has been involved, the person or officer has shown dishonesty or lack of integrity;

(c) that the person or officer is or was suffering from a mental disorder;

(d) that the person or officer is an undischarged bankrupt or has entered into a composition with the debtors of the person or officer

(e) that the person or officer has had a license revoked by the licensing officer previously

(9) Subsection (8) does not limit the circumstances in which a person or an officer of a business entity may be considered by the licensing officer not to be a fit and proper person.

Conditions of Cyber Security License

59. (1) The licensing officer may grant a licence to an applicant, or renew the applicant's licence, subject to such conditions as the licensing officer thinks fit to impose.

(2) The licensing officer may at any time add to, vary or revoke any condition of a licence imposed under subsection (1).

(3) Before making any modification to the conditions of a licence under this section, the licensing officer must give notice to the licensee concerned -

(a) stating that the licensing officer proposes to make the modification in the manner specified in the notice; and

(b) specifying the time (being not less than 14 days from the date of service of notice on the licensee concerned) within which written representations with respect to the proposed modification may be made.

(4) Upon receipt of any written representation mentioned in subsection (3)(b), the licensing officer must consider the representation and may -

(a) reject the representation; or

(b) withdraw or amend the proposed modification in accordance with the representation, or otherwise, and, in either case, must thereupon issue a direction in writing to the licensee concerned requiring that effect be given to the proposed modification specified in the notice or to such modification as

subsequently amended by the licensing officer within a reasonable time.

(5) A licensee who fails to comply with any licence condition of the licence shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [XXXX] or to imprisonment for a term not exceeding [XX year] or to both.

Form and validity of License

60. (1) A licence must -

(a) be in such form as the licensing officer may determine; and

(b) contain the conditions subject to which it is granted.

(2) A licence is in force for such period (not exceeding XX years) as may be specified therein, from the date of its issue under this Act.

(3) A licence that has been renewed in accordance with the provisions of this Part continues in force for such period not exceeding XX years as the licensing officer may specify in writing to the licensee, from the date immediately following that on which, but for its renewal, the licence would have expired.

Revocation or suspension of License

61. (1) Subject to subsection (3), the licensing officer may by order revoke any license if the licensing officer is satisfied that -

(a) the licensee has failed to comply with any condition imposed by the licensing officer on the license;

(b) the license had been obtained by fraud or misrepresentation;

(c) a circumstance which the licensing officer becomes aware of would have required or permitted the licensing officer to refuse to grant or renew the licensee's license, had the licensing officer been aware of the circumstance immediately before the license was granted or renewed;

(d) the licensee holding a license has ceased to carry on in Zambia the business or activity for which the licensee is licensed;

(e) the licensee has been declared bankrupt or has gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction;

(f) the licensee has been convicted of an offence under this Act, or an offence involving dishonesty;

(g) where the licensee is an individual — the licensee is no longer a fit and proper person to continue to hold the license;

(h) where the licensee is a business entity — an officer of the business entity is no longer a fit and proper person; or

(i) it is in the public interest to do so.

(2) Subject to subsection (3), the licensing officer may, in any case in which the licensing officer considers that no cause of sufficient gravity for revoking any license exists, by order -

(a) suspend the license for a period not exceeding 6 months;

(b) censure the licensee concerned; or

(c) impose such other directions or restrictions as the licensing officer considers appropriate on -

(i) the holder of an investigative cybersecurity service practitioner's licence mentioned in section 26; or

(ii) on the licensee's business or functions as a licensed cybersecurity service provider.

(3) The licensing officer must not exercise the licensing officer's powers under subsection (1) or (2) unless an opportunity of being heard (whether in person or by a representative and whether in writing or otherwise) had been given to the licensee against whom the licensing officer intends to exercise the licensing officer's powers, being a period of not more than 14 days after the licensing officer informs the licensee of such intention.

(4) Where the licensing officer has by order revoked a licence under subsection (1) or made any order under subsection (2) in respect of a licensee, the licensing officer must serve on the licensee concerned a notice of the order made under those subsections.

(5) Despite subsection (3), where a licensee has been charged with or convicted of a prescribed offence, being an offence which would make it undesirable in the public interest for the licensee to continue to carry out the functions of a licensee -

(a) the licensing officer may serve on the licensee a notice of immediate suspension of the licence, which takes

immediate effect and remains in force until the licensing officer makes an order under subsection (7) and any appeal to the Minister under section 37 against such an order is determined; and

(b) the licensee must, upon a notice being served under paragraph (a) but subject to subsection (7), immediately cease to carry out any function of a licensee to which the licence refers.

(6) A licensee whose licence has been suspended with immediate effect under subsection (5) may, within 14 days after the licensing officer has served the notice of immediate suspension under paragraph (a) of that subsection, apply to the licensing officer to review the licensing officer's decision under subsection (7).

(7) The licensing officer may, on reviewing the licensing officer's decision, by order -

(a) revoke the licence in question;

(b) suspend that licence for a period not exceeding 6 months starting from the date of immediate suspension of that licence; or

(c) rescind the immediate suspension of that licence.

(8) Where the licensing officer has by order revoked or suspended a licence under subsection (7) in respect of a licensee, the licensing officer must serve on the licensee concerned a notice of the order made under that subsection.

(9) Subject to section 37, an order under subsection (1), (2) or (7)(a) or (b) by the licensing officer revoking or suspending a licence does not take effect until the expiration of 14 days after notice has been served on the licensee under subsection (4) or (8).

(10) In any proceedings under this section in relation to the conviction of a licensee for a criminal offence, the licensing officer is to accept the licensee's conviction as final and conclusive.

(11) In deciding for the purposes of this section whether a person or an officer of a business entity is a fit and proper person, the licensing officer may consider any of the following matters as indicating that the person or officer may not be a fit and proper person:

(a) that the person or officer associates with a criminal in a way that indicates involvement in an unlawful activity; or

(b) that in dealings in which the person or officer has been involved, the person or officer has shown dishonesty or lack of integrity.

(12) Subsection (11) does not limit the circumstances in which a person or an officer of a business entity may be considered by the licensing officer not to be a fit and proper person.

PART VIII
REQUIREMENTS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND FINANCIAL INSTITUTIONS

Obligation of electronic communications service providers and financial institutions

62. (1) An electronic communications service provider or financial institution that is aware or becomes

aware that its computer system is involved in the commission of any category or class of offences must-

(a) without undue delay and, where feasible, not later than seventy-two hours after having become aware of the offence, report the offence in the prescribed form and manner to the Zambia Police Service; and

(b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.

(2) The Minister responsible for police service, in consultation with the Minister responsible for the administration of justice, must, by notice in the Gazette, prescribe-

(a) the category or class of offences which must be reported to the Zambia Police Service in terms of subsection (1); and

(b) the form and manner in which an electronic communications service provider or financial institution must report offences to the Zambia Police Service.

(3) An electronic communications service provider or financial institution that fails to comply with subsection (1) is guilty of an offence and is liable on conviction to a fine of XXXXX.

(4) Subject to any other law or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic service provider or financial institution to-

(a) monitor the data which the electronic communications service provider or financial institution transmits or stores; or

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

(5) This Part does not apply to a financial sector regulator or a function performed by the Bank of Zambia.

PART IX
COOPERATION WITH OTHER COUNTRIES IN MAINTAINING CYBER SECURITY

Identifying Areas of Cooperation

63. (1)

Entering into Agreement

64. The Government of the Republic of Zambia may enter into any agreement with any foreign State regarding-

(a) the provision of mutual assistance and cooperation relating to the investigation and prosecution of-

(i) an offence committed under the Cyber Crime Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means or facilitated by the use of an article; or

(iii) an offence similar to those contemplated the Cyber Crime Act committed in a foreign State; or

(iv) any other offence substantially similar to an offence recognised in the Zambia which is or was committed by means of, or facilitated by the use of an article, in that foreign State;

PART X
CYBER CRIME

Unauthorised access to, interception of or interference with data

65. (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, on conviction or to a fine not below one million penalty units but not exceeding two million penalty units or to imprisonment for a period not below two years but not exceeding five years, or to both.

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

(3) A person who intentionally or negligently uses a subscriber identity module for terminating an international call on any electronic communications network in Zambia as a local call commits an offence and is liable upon conviction to a fine not exceeding five hundred penalty units in respect of each subscriber identity module used to terminate the international call as

a local call or to imprisonment for a period not less than fifteen years but not exceeding twenty-five years or to both.

(4) Where an offence under this section is committed in relation to data that is in a critical information infrastructure 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**.**

(5) 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, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

(6) A person who knowingly possesses data and is not authorized to possess that data, commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(7) Where an offence under this section is committed in relation to data that is in a critical information infrastructure 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.

Illegal devices

66. (1) A person commits an offence if that person:

(a) knowingly, without lawful excuse, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under this Part; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

(iii) introduces or spreads a software code that damages a computer or computer system with the intent

that it be used by any person for the purpose of committing an offence defined by other provisions under this Part; or

(b) knowingly has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing any offence under this Part ; and is liable, upon conviction, to imprisonment for a period not exceeding [period] or a fine not exceeding [amount], or to both.

(2) This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of this Part, such as for the authorized testing or protection of a computer system.

Computer related forgery

67. (1) Any person who knowingly, without lawful excuse, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence and is liable, upon, conviction, to imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or to both.

(2) Where the offence in subsection (1) is committed by sending out multiple electronic mail messages from or through computer systems, the person shall be liable, upon conviction, to imprisonment for a period not exceeding [period], or a fine not exceeding [amount] or to both.

Computer related fraud

68. Any person who knowingly, without lawful excuse causes a loss of property to another person by:

(a) any input, alteration, deletion or suppression of computer data;

(b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person commits an offence and is liable, upon conviction, to imprisonment for a period not exceeding [period], or a fine not exceeding [amount]or to both.

Identity-related crimes

69. Any person who, knowingly without lawful excuse by using a computer system in any stage of the offence, transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence and is liable upon conviction, to a fine not exceeding one million penalty units, or to imprisonment for a period not exceeding five years, or to both.

Attempt, aiding and abetting

70. (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.

(3) For the purposes of this section, “attempt” has the meaning of the word assigned in the Penal Code.

Prohibition of pornography

71. (1) 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.

(2) A person who knowingly -

(a) sells or makes available any pornography to a child through a computer system;

(b) compels, invites or allows a child to or view pornography through a computer system intended to corrupt a child's morals;

commits an offence and is liable, upon, conviction, to imprisonment for a period not exceeding fifteen years.

Child pornography

72. (1) Any person who knowingly:

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

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

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

(d) procures and/or obtain child pornography through a computer system for oneself or for another person;

(e) possesses child pornography in a computer system or on a computer-data storage medium; and

(f) obtains access, through information and communication technologies, to child pornography,

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

(2) It is a defence to a charge of an offence under paragraph (1)(b) to (1)(f) if the person establishes that the child pornography was for a bona fide law enforcement purpose.

Child Solicitation

73. A person who

(a) uses computer system to meet a child for the purpose of committing a sexual related crime;

(b) communicates with a child through a computer system for the purpose of making it easier to procure the child to engage in sexual activity with him/herself;

(c) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with him/herself;

(d) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with another person;

(e) recruits a child to participate in pornographic performances that is intended to be produced/recorded with or without the intent to distribute such material through a computer system or computer network;

Commits an offence and is liable upon conviction to a fine nor exceeding to imprisonment for a period of or to both.

(3) To provide text on impersonation/grooming

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

74. A person who without lawful authority hacks or cracks 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

75. 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

76. (1) Any person who, knowingly without lawful excuse or justification:

(a) initiates the transmission of multiple electronic mail messages from or through a computer system; or

(b) uses a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages, or

(c) materially falsifies header information in multiple electronic mail messages and intentionally initiates the transmission of such messages;

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

(2) Provided that it shall not be an offence under this Act where -

(a) the transmission of multiple electronic mail messages from or through such computer system is done within customer or business relationships; and

(b) the recipient of such electronic mail messages has not opted out of the business or customer relationship.

Prohibition of illegal trade and commerce

77. (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 illegal trade and commerce

78. (1) Subject to subsection (2), this Act shall have effect in of offences relation to any person, whatever the person’s nationality or under this Act 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.

Illegal remaining

79. Any person who knowingly, without lawful excuse, by infringing security measures remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence and is liable, upon conviction, to imprisonment for a period not exceeding one year, or a fine not exceeding one hundred thousand penalty units, or to both.

Offences committed by body corporate or unincorporated body

80. 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.

General penalty

81. 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.

Cognizable offences Cap.88

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

Racist and xenophobic material

83. Any person who, knowingly without lawful excuse-

(a) produces racist and xenophobic material for the purpose of its distribution through a computer system;

(b) offers or makes available racist and xenophobic material through a computer system;

(c) distributes or transmits racist and xenophobic material through a computer system;

commits an offence and is liable, upon, conviction, to imprisonment for a period not exceeding [period], or a fine not [amount], or to both.

Racist and xenophobic motivated insult

84. Any person who, knowingly without lawful excuse, publicly, through a computer system, uses language that tends to lower the reputation or feelings of -

(a) persons for the reason that they belong to a group distinguished by race, colour,

descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

(b) a group of persons which is distinguished by any of these characteristics;

commits an offence and is liable, upon, upon conviction, to imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or to both.

Genocide and crimes against humanity

85. Any person who, knowingly without lawful excuse distributes or otherwise makes available, through a computer system to the public or another person, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity that aids, induces or incites others to commit such acts, or incites, instigates, commands, or procures any other person to commit genocide or crimes against humanity, commits an offence and is liable, upon conviction, to a fine not exceeding two million penalty units, or to imprisonment for a period not exceeding fifteen years, or to both.

Disclosure of details of an investigation

86. A person who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and knowingly without lawful excuse discloses:

(a) the fact that an order has been made;

(b) anything done under the order; or

(c) any data collected or recorded under the order;

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 one year, or to both.

Failure to permit assistance

87. A person who obstructs or hinders law enforcement officers or cyber inspectors in the exercise of any powers under this act or who neglects or fails to comply with an order 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.

Harassment utilizing means of electronic communication

88. A person, who intentionally initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behaviour, 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 one year, or to both.

PART XI
JURISDICTION

Jurisdiction under this Act

89. The Courts in the Republic of Zambia shall have jurisdiction to try any offence under this act or any regulations where an act or omission constituting an offence under this act has been committed wholly or in part –

(a) within the territory of Zambia; or

(b) on a ship or aircraft registered in Zambia; or

(c) by a national of Zambia outside the jurisdiction of any country; or

(d) by a national of Zambia outside the territory of Zambia, if the person's conduct would also constitute an offence under a law of the country where the offence was committed;

(e) by a person, irrespective of the nationality or citizenship of the person:

(i) using equipment, software, or data located within Zambia, regardless of the location of the person; or

(ii) directed against equipment, software, or data located in Zambia regardless of the location of the person.

Extradition

90. Any offence under the provisions of this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

PART XII
ELECTRONIC EVIDENCE

Admissibility of electronic evidence

91. (1) In proceedings for an offence under this Act, the fact that evidence has been generated from a computer system shall not by itself prevent that evidence from being admissible.

(2) The provisions of Part …. of the [e-transactions] Act Number …of 2018 shall apply to this Part.

PART XIII
PROCEDURAL LAW

Search and seizure

92. (1) The provisions of the Criminal Procedure Code relating to warrants shall apply to this Part.

(2) A law enforcement officer may with warrant, where he has reasonable grounds to believe that there may be stored or hidden in a device or computer system data:

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence;

enter the place to search and seize the thing or computer data including search or similarly access

(i) a computer system or part of it and computer data stored therein; and

(ii) a computer-data storage medium in which computer data may be stored in the territory of Zambia.

(2) A law enforcement officer that is undertaking a search based on Section 29(1) may, where he has reasonable grounds to believe that the data sought is stored in another device or computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial device or system, extend the search or similar accessing to the other device or system.

(3) A law enforcement officer that is undertaking a search is empowered to seize or similarly secure computer data accessed according to sub-sections (1) or (2).

Assistance

93. (1) Any person, who is not a suspect of a crime or otherwise excluded from an obligation to follow such order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 29 shall permit, and assist if reasonably required and requested by the person authorised to make the search by:

(a) providing information that enables the undertaking of measures referred to in section 29;

(b) accessing and using a computer system or computer data storage medium to search any computer data available to or in the system;

(c) obtaining and copying such computer data;

(d) using equipment to make copies; and

(e) obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings.

Production order

94. If a judge is satisfied on the basis of an ex-parte application by a law enforcement officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal

investigation or criminal proceedings, the Judge may order that:

(a) a person in the territory of Zambia in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or

(b) an electronic communications service providers in Zambia to produce information about persons who subscribe to or otherwise use the service.

Expedited preservation

95. A law enforcement officer may, where the law enforcement officer has grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days only if, on an application a judge authorises an extension for a further specified period of time.

Partial disclosure of traffic data

96. A law enforcement officer may, where the law enforcement officer is satisfied computer data is reasonably required for the purposes of a criminal investigation, by written notice given to a person in control of the computer system, require the person to disclose relevant traffic data about a specified communications to identify:

(a) the electronic communications service providers; and/or

(b) the path through which a communication was transmitted.

Collection of traffic data

97. (1) If a judge is satisfied on the basis of an ex-parte application by a law enforcement officer, supported by affidavit that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the Judge may order a person in control of such data to:

(a) collect or record traffic data associated with a specified communication during a specified period; or

(b) permit and assist a specified law enforcement officer to collect or record that data.

(2) If the Judge is satisfied on the basis of an application by a law enforcement officer, supported by affidavit that there are reasonable grounds to suspect or believe that traffic data is reasonably required for the purposes of a criminal investigation, the Judge may authorize a law enforcement officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interception of content data

98. (1) If a judge is satisfied on the basis of an ex-parte application by a law enforcement officer, supported by affidavit that there are reasonable grounds to

suspect or believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judge may:

(a) order an electronic communications service provider whose service is available in Zambia through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorise a law enforcement officer to collect or record that data through application of technical means.

Forensic tool

99. (1) If a judge is satisfied on the basis of an ex-parte application by a law enforcement officer, supported by affidavit that in an investigation concerning an offence listed in paragraph 7 herein-below or regulations made under Section 46 there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in this Part but is reasonably required for the purposes of a criminal investigation, the judge may authorise a law enforcement officer to utilise a forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application shall to contain the following information:

(a) suspect of the offence, if available with name and address if available, and

(b) description of the targeted computer system, and

(c) description of the intended measure, extent and duration of the utilization, and

(d) reasons for the necessity of the utilization.

(2) It shall be a condition of the authorisation that such investigation shall ensure that modifications to the computer system of the suspect are limited to those modifications essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it shall be necessary to log -

(a) the technical means used and time and date of the application; and

(b) the identification of the computer system and details of the modifications undertaken within the investigation;

(c) any information obtained; and that

(d) information obtained by the use of such tool shall be protected against any modification, unauthorised deletion and unauthorized access.

(3) The duration of authorisation in section 36(1) shall be limited to 3 months. Where the conditions of the authorisation are no longer met, the action taken shall be stopped immediately.

(4) The authorization to install the tool shall include accessing the suspects computer system.

(5) Where the installation process requires physical access to a place the requirements of section 29 shall need to be fulfilled.

(6) A law enforcement officer may pursuant to the order of court granted in (1) above request that the court order an electronic communications service provider to support the installation process.

(7) The offences referred to in subsection (1) include but not limited to:

(a) murder or Manslaughter or treason;

(b) kidnapping or abduction;

(c) money laundering contrary to the [proceeds of crime] Act;

(d) producing, manufacturing, supplying or otherwise dealing in any dangerous drug in contravention of the [dangerous drugs] Act;

(e) importing or exporting a dangerous drug in contravention of the [dangerous drugs] Act;

(f) importation, exportation or trans-shipment of any firearm or ammunition in contravention of the [firearms] Ac;

(g) manufacture of, or dealing, in firearms or ammunition in contravention of the [firearms] Act;

(h) illegal possession of a prohibited weapon or any other firearm or ammunition contrary to the [firearms] Act;

(i) an offence contrary to the [prevention of corruption] Act;

(j) arson;

(k) international Convention on hijacking, terrorist offences etc;

(m) [prevention of terrorism] Act;

(n) attempting or conspiring to commit, or aiding, abetting, counseling or procuring the commission of, an offence falling within any of the preceding paragraphs.

PART XIV
LIABILITY

No monitoring obligation

100. (1) An electronic communications service provider shall have no general obligation to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to the provisions of any other law, 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) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

(3) The Minister may, on application by a representative body for service providers, by notice in the Gazette, recognise such body for purposes of section 37(1).

(4) The Minister shall recognise a representative body referred to in subsection (3) 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.

(5) The limitations on liability established by this Part apply to an electronic communications service provider if

(a) the electronic communications service provider is a member of the representative body referred to in section 37(3); and

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

Access

101. (1) An electronic communications service provider shall not be criminally liable for providing access and transmitting information on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

(2) The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Hosting

102. (1) A hosting provider shall not be criminally liable for the information stored at the request of a user of the service, on condition that:

(a) the hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court of law to remove specific illegal information stored; or

(b) the hosting provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs the Authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

(2) Paragraph 1 shall not apply when the user of the service is acting under the authority or the control of the hosting provider.

(3) Where the hosting provider removes the content after receiving an order pursuant to sub-section (1) no liability shall arise from contractual obligations with its customer to ensure the availability of the service.

Caching

103. A caching provider shall not be criminally liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, on condition that:

(a) the caching provider does not modify the information;

(b) the caching provider complies with conditions of access to the information;

(c) the caching provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

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

(e) the caching provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been

disabled, or that a court or the relevant authority has ordered such removal or disablement.

Hyperlink provider

104. An Internet service provider who enables the access to information provided by a third person by providing an electronic hyperlink shall not be liable for the information where -

(a) the Internet service provider expeditiously removes or disables access to the information after receiving an order from any public authority or court to remove the link; or

(b) the Internet service provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority, expeditiously informs the relevant authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

PART XV
GENERAL PROVISIONS

Evidence obtained by Lawful Interception not admissible in Criminal Proceedings

105. 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.

Regulations

106. 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 the ECT Act No. 21 of 2009

107. (1) Part VIII, IX, XI, and Parts of XIV herewith contained in the ECT Act No. 21 of 2009 are hereby repealed.

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

General penalty

108. 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.