REPUBLIC OF ZIMBABWE

CHAPTER ... : ...

Computer Crime and Cybercrime Bill

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY PROVISIONS

Section Title

PART II
Offences

PART III
JURISDICTION

PART IV
ELECTRONIC EVIDENCE

PART V
PROCEDURAL LAW

PART VI
LIABILITY

PART VII
GENERAL PROVISIONS

PART VIII
CONSEQUENTIAL AMENDMENTS AND SAVINGS

POSTAL AND TELECOMMUNICATIONS ACT, NO. 4 OF 2012 CHAPTER 12:05

CRIMINAL LAW (CODIFICATION AND REFORM) ACT CHAPTER 9:23

SCHEDULE

Correspondence of References to Crimes in Code or other Enactments to Provisions of Computer Crime and Cybercrime Act Defining such Crimes

Computer Crime and Cybercrime Bill

A Bill to criminalize offences against computers and communications infrastructure networks related crimes; to consolidate the criminal law on computer crime and network crime; to provide for investigation and collection of evidence for computer and network related crime; to provide for the admission of electronic evidence for such offences, and to provide for matters connected with or incidental to the foregoing.

Enacted by the President and Parliament of Zimbabwe

PRELIMINARY PROVISIONS

Short Title

1 This Act may be cited as the Computer Crime and Cybercrime Act, Chapter ... : ... .

Application

2. This Act shall apply to the Republic of Zimbabwe.

Interpretation

3. (1) In this Act, unless the context otherwise requires –

"Access" in relation to Section 5 includes, without limitation, to make use of, gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network, a critical information infrastructure, whether in whole or in part including their logical, arithmetical, memory, transmission, data storage, processor, or memory function, whether physical, virtual, direct or indirect means or by electronic, magnetic, audio, optical or any other means.

.

"Access provider" means any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network;

"Article" includes but is not limited to:

(a) a computer system or part of a computer system;

(b) another computer system, if:

(i) computer data from that computer system is available to the first computer system being searched; and

(ii) there are reasonable grounds for believing that the computer data sought is stored in the other computer system;

(c) a computer data storage medium.

"Authority" means the Authority established under the ....Act Chapter...:...

"Caching provider" means any natural or legal person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request;

"Child" shall mean any person under the age of eighteen (18) years;

"Child pornography" means any visual depiction, including any photograph, film, video, image, whether made or produced by electronic, mechanical or other means of sexual explicit conduct, where:

a) The production of visual depiction involves a child;

b) Such visual depiction is a digital image, computer image, or computer generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge;

c) Such visual depiction has been created, adapted or modified to appear that a child is engaging in sexually explicit conduct.

"Computer data" means any representation of facts, concepts, information (being either texts, audio, video or images) machine-readable code or instructions, 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 device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the article or device is physically attached to or connected with the computer device;

"Critical infrastructure" means computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or to essential services as defined in Section 19 of the Criminal Law (Codification and Reform) Act or any combination of those matters;

"Device" means any electronic programmable device used, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or a national critical information infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions and includes all:- input devices, output devices, processing devices, computer data storage mediums, programmes and other equipment and devices, that are related to, connected with or used with such a device or any part thereof..

"Electronic Communication" 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.

"Hinder" in relation to a computer system or information system includes but is not limited to:

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

(b) causing electromagnetic interference to a computer system; or

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

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

"Hosting provider" 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 characteristic or property of an element such as symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.

Hyperlink provider means any natural or legal person providing one or more hyperlinks.

"Information system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, automatically processes computer data as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.;

"Interception" means the acquisition, viewing, capturing, or copying of data through the use of a hardware or software tool or any other means, so as to make some or all of the data available to a person other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data and includes the-

a) Examination or inspection of the contents of the data; and
b) Diversion of the data or any part thereof from its intended destination to any other destination.

"Racist and xenophobic material" means any data message which advocates, promotes or incites hate, discrimination or violence means any data message representing ideas or theories which advocate, promote or incite hatred, discrimination or violence against a person or group of persons based on national or social origin, race, colour, ethnicity, religious beliefs, gender, gender identity, or mental or physical disability.

"Remote 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;

"Seize" includes:

(a) activating any onsite computer system and computer data storage media;

(b) making and retaining a copy of computer data, including by using onsite equipment;

(c) maintaining the integrity of the relevant stored computer data;

(d) rendering inaccessible, or removing, computer data in the accessed computer system;

(e) taking a printout of output of computer data; or

(f) seize or similarly secure a computer system or part of it or a computer-data storage medium.

"Traffic data" means data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service.

"Computer related terrorist activities" means a premeditated criminal act perpetrated by the use of computers or computer networks or information

infrastructure networks or a premeditated criminal act against computer systems, information infrastructure networks, computer programmes and data resulting in violence, destruction, and/or disruption of services with the intention to cause harm or intimidate or coerce a government or people in furtherance of political, religious, social and ideological objectives.

"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.

(2) A reference in this Act or any other enactment to any of the offences mentioned in the first column of the Schedule shall be construed as referring to those offences as defined in the provisions of this Act mentioned opposite thereto in the second column.

PART II

COMPUTER AND CYBERCRIME MANAGEMENT CENTRE

4

1) The Minister responsible for State Security shall in consultation with the Minister responsible for Finance establish the Computer and Cybercrime Management Centre.

2) The Centre shall be headed by the Deputy Director General within the State Security Department who reports to the Computer and Cybercrime Committee.

3) The Computer and Cybercrime Committee shall consist of nine Members drawn from the:

a) Ministry of Defence

b) Ministry of Science and Technology

c) Ministry of Justice, Legal and Parliamentary Affairs;

d) Zimbabwe Republic Police;

e) Zimbabwe Prison Services;

f) National Prosecution Authority

g) Director General of the Postal and Telecommunications Regulatory Authority

h) Two representatives from Organizations representing Information Technologies and Computers professionals

The functions of the Computer and Cybercrime Management Centre shall be to:

a) Implement Government policy relating to computer crime, cybercrime and cyber security;

b) Identify areas for intervention;

c) Coordinate cyber security and establish the national 24/7 contact point on all matter relating to cybercrime and cyber security;

d) Promote and coordinate activities focused on improving cyber security by all stakeholders in the public and private sectors;

e) Provide guidelines to public and private sector stakeholders on matters relating to awareness, training, enhancing, investigating, prosecuting combating cybercrime and managing cyber security threats.

f) Provide technical and policy advice to the Minister

g) Provide advice to the Minister on the establishment and development of a comprehensive legal framework governing cyber related matters.

PART III

OFFENCES

5

Illegal Access

(1) Any person who unlawfully and intentionally accesses the whole or any part of a computer system shall be guilty of an offence

(2) Any person who contravenes the provisions of subsection (1) shall be liable, on conviction to: a fine not exceeding Level 14 or to imprisonment not exceeding ....years or both such fine and imprisonment.

(3) Any person who contravenes the provisions of subsection (1) by infringing security measures or with the intention of obtaining computer data, shall be liable on conviction to a fine not exceeding level ten or to imprisonment for a term not exceeding five years or both.

(4) Any person who contravenes the provisions of subsection (1) with any of the aggravating circumstances described in section 24, shall be liable on conviction to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

Illegal Remaining

6. (1) Any person who unlawfully and exceeds his or her lawful authority to access a computer or information system by remaining logged in a computer or information system or part of a computer or information system or continues to use a computer information system beyond the authorised period or purpose shall be guilty of an offence and liable, on conviction, to a fine not exceeding level ten or imprisonment not exceeding five years or both.

Illegal Interception

7. (1) Any person who, unlawfully and intentionally, intercepts by technical means:

(a) any non-public transmission of computer data to, from or within a computer network, computer device, database or information system; or

(b) electromagnetic emissions from a computer or information system carrying such computer data

shall be guilty of an offence.

2) Any person who contravenes the provisions of subsection (1) shall be liable, on conviction to a fine not exceeding level 10 or to imprisonment not exceeding five years or both.

(3)Any person who contravenes the provisions of subsection (1) with aggravating circumstances described in section 24, shall be liable, on conviction to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

Illegal Data. Interference

8. (1) Any person who unlawfully and intentionally interferes with data by: :

(a) damaging, , corrupting, impairing or deteriorating computer data; or

(b) deleting computer data ; or

(c) altering computer data; or

(d) rendering computer data meaningless, useless or ineffective; or

(e) obstructing, interrupting or interfering with the lawful use of computer data; or

(f) obstructing, interrupting or interfering with any person in the lawful use of computer data; or

(g) denying, hindering, blocking access to computer data to any person authorized to access it; or

(h) fraudulently or mischievously creating, altering or manipulating any data, programme or system in whole or in part which is intended for installation in a computer;

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding level 10 or imprisonment not exceeding five years or to both.

2) Any person who contraventions the provisions of subsection (1) with aggravating circumstances described in section 24 shall be liable on conviction to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

Illegal System Interference

9. 1) Any person who unlawfully and intentionally interferes with the use of a computer or information network, computer device, electronic communications network or critical information infrastructure by blocking, hindering, impeding, interrupting, altering or impairing the functioning of, access to or the integrity of a computer device, computer or information network, electronic communications network or critical information infrastructure shall be guilty of an offence and liable on conviction to a fine not exceeding level fourteen or imprisonment not exceeding 10 years or both. .

Illegal Disclosure of Access Codes

10. (1) Any person who unlawfully and intentionally -

a) communicates, discloses or transmits any computer data, program, access code or command or any other means of gaining access to any programme or data held in a computer or information system to any person not authorized to access the computer data, program, code or command for the purpose of committing an offence or for an unlawful purpose shall be guilty of an offence and liable on conviction to a fine not exceeding level ten or imprisonment for a period not exceeding 5 years or both.

(b) activates or installs or downloads a program that is designed to create, destroy, mutilate, remove or modify data, program or any other form of information existing within or outside a computer or computer network; or

(c) creates, alters, or destroys a password, personal identification number, code or method used to access a computer or computer network,

shall be guilty of an offence and liable on conviction to a fine of not exceeding level twelve or to imprisonment for a period not exceeding ten years or both.

(2) A person shall not be liable under this section where –

(a) he is acting pursuant to measures that can be taken under Part V of this Act; or

(b) he is acting in reliance of any other statutory power.

(3) Where an offence under this section is committed in relation to data that forms part of a database or that is concerned with national security or the provision of an essential service, such person shall be liable upon conviction, to imprisonment for a term not exceeding 10 years.

(6) For the purposes of this section, it is immaterial whether an illegal interference or any intended effect of it is permanent or merely temporary.

Data Espionage

11. (1) Any person who, unlawfully and intentionally performs or authorises, procures, allows another person, possesses, communicates, delivers or makes available or receives computer data or intercepts computer data which is in the possession of the State and which is classified or specially protected against unauthorized access with the intention of directly or indirectly benefitting a Foreign State shall be guilty of an offence and liable on conviction to imprisonment not exceeding 20 years.

Illegal Use of Data or Devices

12. (1) Any person who unlawfully and intentionally acquires, possesses produces, sales, procures for use, imports, distributes, provides to another, uses or makes available an access code, password, a computer programme designed or adapted for the purpose of committing a offence or similar data or device by which the whole or any part of a computer or information system is capable of being accessed, for purposes of the commission or attempted commission of a crime under this Act, shall be guilty of an offence and liable on conviction to a fine not exceeding level 12 or imprisonment not exceeding 10 years or both.

Provided that section 12 (1) shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, importation, distribution or otherwise making available or possession referred to is for lawful purposes such as for the authorized testing or protection of a computer or information system.

2) any person who unlawfully and intentionally assembles, obtains, sells, purchases, possess, makes available, advertises or uses malicious software or programmes or devices for purposes of causing damage to data, computer or information systems, computer networks, electronic

communications networks, critical information infrastructure or computer devices shall be guilty of an offence and liable on conviction to a fine not exceeding level ten or imprisonment not exceeding five years or both.

3) Any person who contraventions the provisions of section 12 with aggravating circumstances described in section 24 shall be liable on conviction to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

Computer-related Forgery and Uttering

13. (1) Any person who unlawfully and intentionally 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 to the actual or potential prejudice of another person shall be guilty of an offence and liable on conviction to a fine not exceeding level ten or imprisonment not exceeding five years or both.

(2) Any person who unlawfully and intentionally 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 by sending out multiple electronic mail messages from or through a computer or information systems to the actual or potential prejudice of the intended recipients of such message shall be guilty of an offence and liable on conviction to a fine not exceeding level twelve or imprisonment not exceeding ten years or both.

Computer-related Fraud

14. 1) Any person who unlawfully and intentionally, makes a misrepresentation causes actual or potential 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, an economic benefit for himself or herself or for another person shall be guilty of an offence and liable on conviction to a fine not exceeding level 14 or imprisonment not exceeding 5years or both such fine and imprisonment.

Computer related financial Offences

15. 1) Any person who unlawfully and intentionally acquires by any means, possess, uses or provides to another person the financial information of another for the purpose of committing an offence under this Act shall be guilty of an offence and liable on conviction to a fine not exceeding level 14 or imprisonment not exceeding 5 years or both.

2) Any person who unlawfully and intentionally is found in possession of the financial information of another person in regard of which there is a reasonable suspicion that such financial information was acquired, is possessed or is provided to another for purposes of committing an offence or was used

or may be used to commit an offence under this Act shall be guilty of an offence and liable on conviction to not exceeding level 14 or imprisonment not exceeding 5 years.

Computer Related Terrorism activities

16. Any person, entity or organisation who unlawfully and intentionally;

a) provides, receives or participates in training, or instructions or recruits a person, entity or organisation to receive training or instruction for effecting or furtherance of computer related terrorist activities;

b) possesses, receives or makes available data, any software or hardware tool, malware, a password, access code or similar data and device, or computer data, computer device, computer network or information infrastructure network for effecting or furtherance of computer related terrorist activities;

c) provide financial assistance, information, publications and disseminate propaganda materials or communications for the furtherance of computer related terrorist activities

d) engages in any computer related terrorist activity in contravention of the Suppression of Foreign and International Terrorism Act (Chapter 11:21).

shall be guilty of an offence and liable on conviction to imprisonment for a period not exceeding 20 years.

Child Pornography

17. (1) Any person who unlawfully and intentionally~~:~~

(a) produces child pornography for the purpose of 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 obtains child pornography through a computer or information system for oneself or for another person;

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

(f) knowingly obtains, access or procures through information and communication technologies, child pornography,

shall be guilty of an offence and liable on conviction to a fine not exceeding level 14 or to imprisonment not exceeding ten years, or both such fine and imprisonment.

(2) Any person who unlawfully and makes pornography available to one or more children through a computer or information system or facilitates the access of children to pornography through a computer or information system shall be guilty of an offence and liable on conviction to a fine not exceeding

level 14 or imprisonment not exceeding 5 years years or both such fine and imprisonment.

.

Pornography

18. (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 level 14 or to imprisonment for a term not exceeding ten years or both.

(3) For the purpose of this Section, "Publish" includes

(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; or

(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(c) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in subsection (a)

Identity-related crimes

19. Any person who unlawfully and intentionally by using a computer system, acquires, transfers, possesses, or uses, any means of identification of another person with the intent to commit, or to aid or abet, or in connection with the commission of a crime shall be guilty of an offence and liable on conviction to a fine not exceeding level eight or imprisonment not exceeding three years or both.

Racist and/or Xenophobic Material and Insults	20.	Any person who unlawfully and intentionally through a computer system produces or causes to be produced racist and/or xenophobic material for the purpose of its distribution; ~~(a)~~ offers, makes available or broadcasts or causes to be offered, made available or broadcast racist and/or xenophobic material; (b) distributes or transmits or causes to be distributed or transmitted racist and/or xenophobic material; d)uses language that tends to lower the reputation or feelings of 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; e) uses language that tends to lower the reputation or feelings of a group of persons which is distinguished by any of these characteristics; shall be guilty of an offence and liable on conviction to a fine not exceeding level 14 or imprisonment not exceeding 5 years years or both.
SPAM	21.	(1) A person who, intentionally 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 punishable, on conviction, by imprisonment for a period not exceeding one year, or a fine not exceeding level five, or both. (2) Provided that it shall not be an offence under this Act where the transmission of multiple electronic mail messages from or through such computer system is done within customer or business relationships
Harassment utilizing means of electronic communication	22.	(1)Any person who, unlawfully and intentionally generates, possesses, and distributes an electronic communication, with the intent to coerce, intimidate, harass, threaten bully or cause emotional distress, degrade humiliate or demean the person of another person, using a computer system or information system shall be guilty of an offence and liable on conviction to a fine not exceeding level 10 or imprisonment not exceeding five years or both.
Violation of intellectual	23.	Any person who unlawfully and intentionally appropriates in any manner rights in property which rights are vested in another person or where copyrights exists in respect of any work without the authority of the owner of the rights by means of a computer network of electronic communications

property rights

network which the person knows is subject to intellectual property protection or copyright shall be guilty of an offence and liable on conviction to in addition to any penalty or relief provided under the intellectual property law in question, a fine not exceeding level 14 or imprisonment not exceeding 5 years or both such fine and imprisonment.

Attempt Abetment and Conspiracy

24. (1) Any person who:

(a) attempts to commit any offence under this Act; or

(b) aids, abets or does any act preparatory to or in furtherance of the commission of an offence under this Act; or

(c) conspires with another to commit any offence under this Act, shall be guilty of an offence and liable on conviction to the punishment provided for such an offence under this Act.

Aggravating circumstances Sections 5, 7, 8 and 12

25 In this Part the crime of illegal access to or use of a computer, illegal interception, illegal data interference, illegal system interference, and illegal use of data or devices is committed in aggravating circumstances if—

(*a*) committed in connection with or in furtherance of the commission or attempted commission of the crime of insurgency, banditry, sabotage or terrorism, theft, unauthorised borrowing or use of property, extortion, fraud, forgery and uttering, malicious damage to property, damaging, destroying or prejudicing the safe operation of an aircraft, concealing, disguising or enjoying the proceeds of the unlawful dealing in dangerous drugs, corruptly using false data or defeating or obstructing the course of justice; or

(*b*) the computer, computer network, information communications network data, programme or system is owned by the State, a law enforcement agency, the Defence Forces, the Prison Service, a statutory corporation or a local authority; or

(*c*) the crime occasions considerable material prejudice to the owner of the computer, computer network, data, programme or system; or

(d) the crime disrupts or interferes with an essential service.

(e) the crime was committed in furtherance of organised crime or the perpetrator was part of organised criminal gang.

PART III
JURISDICTION

26. (1) A Court in Zimbabwe shall have jurisdiction to try any offence under this Act or any regulations made under it where the offence has been committed wholly or in part –

2

(a) within the territory of Zimbabwe;
or

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

(c) by a national or permanent resident of the Republic of Zimbabwe or a person carrying on business in Zimbabwe and the offence is committed outside the jurisdiction of the Republic of Zimbabwe;
or

(d) by a national or permanent resident of the Republic of Zimbabwe or a person carrying on business in Zimbabwe and the offence is committed outside the territory of Zimbabwe, if the person's conduct would also constitute an offence under the law of the country where the offence was committed.

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

(1) when the offense is committed within the territory of Zimbabwe; or

(2) using a computer system or information system or device , software, or data located within Zimbabwe, regardless of the location of the person; or

(3) directed against a computer system or information system or device , software, or data located in Zimbabwe regardless of the location of the person.

Extradition

27. 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 Chapter 9:08.

PART IV
ELECTRONIC EVIDENCE

Admissibility of Electronic Evidence

28. (1) In any criminal proceedings under this Act, the rules of evidence shall apply in so far as the admissibility of evidence generated from a computer system or information system is permissible under the laws of Zimbabwe. .

2) Evidence in electronic form shall subject to subsection (3) be given evidential weight.

3) In assessing the admissibility or evidential weight of data or data message regard shall be had to:

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

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

c) the manner in which the originator or recipient of the data or data message was identified, and

d) any other relevant factors

PART V

PROCEDURAL LAW

Search and Seizure

29 (1)A magistrate may issue a warrant authorising the search and seizure of an article , on written application by a police officer that there are reasonable grounds for suspecting or believing that that there may be at a given place an article or computer 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;

2) The warrant issued under subsection (1) may authorize the police officer to obtain such assistance as may be necessary, to enter the place to search and seize the article or computer data including searching or accessing:

i) a computer or information system in whole or in part computer data stored therein; or

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

(2) A police officer undertaking a search in terms of a warrant issued under subsection (1) who has grounds to believe that the data sought is stored in another computer system or part of it within the Republic of Zimbabwe, and such data is accessible from or available to the initial system, he shall to expeditiously extend the search or access to the other system.

(3) A police officer undertaking a search in terms of subsection (1) shall seize or secure the computer data so accessed..

Assistance 30. (1) Any person, other than the person suspected of having committed an offence under this Act 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 28 shall, if required or requested, provide assistance to the person authorized to make the search by:

(a) providing information that enables the undertaking of measures referred to in section 28;

(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 devices 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.

(f) (f) Any person who, without lawful excuse fails to comply with the provisions of subsection (1) shall be guilty of an offence and liable to a fine not exceeding level four or to imprisonment for a period not exceeding three months or to both such fine and such imprisonment

Production Order 31. 1) A Magistrate may order, on application by a police officer in the prescribed form that specified computer data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, that:

(a) a person in the territory of Zimbabwe 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 provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.

2) The application referred to in subsection (1) shall be supported by an affidavit.

Expedited preservation

32. A police officer issued with a warrant in terms of section 28, if there are reasonable grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is vulnerable to loss, alteration, deletion, impairment or modification, he may, 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, on an application to a Magistrate for an extension for a further period..

Partial Disclosure of traffic data

33. A police officer issued with a warrant granted in terms of section 28 , if he reasonably believes that computer data is required for the purposes of a criminal investigation, may, by written notice to a person in control of the computer system or information system, require the person to disclose relevant traffic data about a specified communications in order to identify:

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

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

Collection of traffic data

34. (1) A Magistrate may, on the basis of an application in the prescribed form, by a police officer, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is required for the purposes of a criminal investigation, 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 police officer to collect or record that data.

(2) A Magistrate may, on the basis of an application in the prescribed form, by a police officer, that there are reasonable grounds to suspect or believe that traffic data is required for the purposes of a criminal investigation, authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through the use of technical means. The application referred to in subsections (1) and (2) shall be supported by an affidavit.

Interception of content data

35. (1) A Magistrate may, on the basis of an application by a police officer in the prescribed form that he has reasonable grounds to suspect or believe that the content of electronic communications is required for the purposes of a criminal investigation,:

(a) order an electronic communications service provider whose service is available in Zimbabwe 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 information system; or

(b) authorize a police officer to collect or record that data through the use of technical means.

2. The application referred to in subsection (1) shall be supported by an affidavit.

36. Forensic Tool

(1) A Magistrate may, on the basis of an application by a police officer in the prescribed form, that in an investigation relating to or concerning an offence listed in subsection 10 or regulations made under Section 44 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, authorize the police officer to utilize remote forensic tools. The application shall specify the following information:

(a) the name and address of the suspect of the offence,

(b) description of the targeted computer system,

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

(d) reasons for the utilization of remote forensic tools..

(2) The application referred to in subsection (1) shall be supported by an affidavit.

3). 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. .

4) During the conduct of the investigation the police officer shall record:

(a) the technical means used, time and date ; and

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

(c) any information obtained;

5) Information or data obtained by the use of such tool shall be protected against any modification, unauthorized deletion and unauthorized access.

(6) The duration of authorization in section 33(1) shall be 3 months. .

(7) The authorization to install the tool shall include remotely accessing the suspect's computer system.

8) A police officer may pursuant to the authorization grated in subsection (1) above request that the authorization direct an electronic communications service provider support the installation process.

10) The offences referred to in subsection (1) include:
i. Murder or treason.
ii. Kidnapping or abduction.
iii. Money laundering as provided for in the Money Laundering and Proceeds of Crime Act (Chapter 9:24) and Suppression of Money laundering Act (Chapter 24:24) .
iv. Producing, manufacturing, supplying or otherwise dealing in

any dangerous drug in contravention of the Dangerous Drugs Act (Chapter 15:02).
v. Importing or exporting a dangerous drug in contravention of the Dangerous Drugs Act (Chapter 15:02).
vi. Importation, exportation or trans-shipment of any firearm or ammunition in contravention of the Firearms Act (Chapter 10:09).
vii. Manufacture of, or dealing, in firearms or ammunition in contravention of the Firearms Act (Chapter 10:09).
viii. Illegal possession of a prohibited weapon or any other firearm or ammunition contrary to the Firearms Act (Chapter 10:09)
ix. An offence contrary to the Prevention of Corruption Act (Chapter 9:16).
x. Arson.
xi. International Convention on hijacking, terrorist offences .
xii. Suppression of Foreign and International Terrorism Act (Chapter 11:21.
xiii. Attempting or conspiring to commit, or aiding, abetting, concealing or procuring the commission of an offence. .

PART VI

LIABILITY

General Obligations

37. (1) The Minister shall , subject to the provisions of any other law, prescribe procedures for electronic communications service providers to

(a) inform the Cybercrime and Cyber Security Management Centre or any other competent public authorities of suspected illegal activities conducted through their electronic communications infrastructure or computer systems or information provided by recipients of their service; and

(b) to provide the Cybercrime and Cyber Security Management Centre or any other competent authorities, at their request, information enabling the identification of specific recipients of their service.

Access Provider

38. (1) An electronic communications network or access or service provider shall not be criminally liable for providing access or transmitting information through its system provided the provider:

(a) has not initiated the transmission;

(b) has not selected the receiver of the transmission; or

(c) has not selected or modified the information contained in the transmission.

(2) The acts of transmission and/or provision of access referred to in subsection (1) shall 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 the information is not stored for any period longer than is reasonably necessary for the transmission.

(3) An electronic communications network or access or service provider who contravenes these provisions shall be guilty of an offence and liable on conviction to a fine not exceeding level eight

Hosting Provider

39. (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 Cybercrime and Cyber Security Management Centre to enable it to evaluate the nature of the information and if necessary issue an order to remove the content.

(2) Subsection (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.

(2) A hosting provider who fails to remove or disable access to the information in terms of subsection 1 (a) and 1 (b) commits an offence and shall be liable to a fine not exceeding level eight or imprisonment for a period of two years or both such fine and imprisonment.

Caching Provider

40. 1) 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.

2) A catching provider who violates any of the conditions stated in subsection (1) (a) to (e) commits an offence and shall be liable to a fine not exceeding level eight or imprisonment for a period of two years or both such fine and imprisonment.

Hyperlinks Provider

41. 1) 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.

2) An Internet Service Provider who fails to expeditiously remove or disable access to information in terms of subsection (1) (a) and (b) commits an offence and shall be liable to a fine not exceeding level eight or imprisonment for a period of two years or both such fine and imprisonment.

Search Engine Provider

42. (1) An Internet service provider who makes and/or operates a search engine that either automatically or based on entries by others creates an index of Internet-related content or makes available electronic tools to search for information provided by a third party is not liable for search results 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) An Internet Service Provider who contravenes subsection (1) (a) to (c) commits an offence and shall be liable to a fine not exceeding level eight or imprisonment for a period of two years or both such fine and imprisonment.

PART VII

GENERAL PROVISIONS

43.

General Provision on Cybercrimes

(1) A Court convicting any person of a offence under this Act, may order the forfeiture to the State of –

(a) any asset, money or property constituting or traceable to gross proceeds of such offence; and

(b) any computer system or information system, software or other devices used or intended to be used to commit or to facilitate the commission of such offence.

Except as provided for in this Act, any offence under any Act which is committed in whole or in part by use of a computer, electronic device or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply.

44. Regulations

(1)The Minister may, in consultation with the Computer and Cybercrime Management Centre make regulations regarding any matter which by this Act is required or permitted to be prescribed or which is necessary or expedient to be prescribed for carrying out or giving effect to the provisions of this Act and may include regulations on-

(a) interception of computer data communication including but not limited to the security, functional and technical requirements for interception;

(b) the declaration of critical information infrastructure, including but not limited to the identification, securing the integrity and authenticity of, registration, and other procedures relating to critical information infrastructure

(c) the liability of access providers including the security, functional and technical requirements for the purposes of Part VI of this Act.

(2) The Authority may, with the approval of the Minister, issue such guidelines as may be required for the carrying out of the provisions of this Act as it relates to its functions under this Act.

45. Offence by body corporate or un-incorporate

1) An information communications service provider whether a corporate or un-incorporated body who fails to comply with the provisions of this Act shall be guilty of an offence and liable on conviction to a fine of not exceeding level 14.

PART IX

AMENDMENT OF CRIMINAL LAW(CODIFICATION AND REFORM) ACT CHAPTER 9:23

This Part shall be read as one with the Criminal Law (Codification And Reform) Act Criminal Procedure Code hereinafter referred to as the "principal Act"

Construction Criminal Code

46. The principal Act is amended in Section 163 to Section 168 by deleting the said Sections.

Amendment Section 163, 164, 165, 166, 167, and 168 Criminal Code

---