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

50. Construction
51. Amendment of Section 88

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

52. Construction
53. Amendment of Section 163 - 168

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 for An Act to criminalize offences against computers and network related crime; 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.

[Date of Commencement: .....]

Enacted by the Parliament of Zimbabwe

PART I.

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 means entering a computer system.

"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;

.

"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 pornographic material that depicts presents or represents:

(a) a child engaged in sexually explicit conduct;

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

"Computer system" or "information system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

"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 material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or 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 defined in Section 19 of the Criminal Law (Codification and Reform) Act or any combination of those matters;

"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.

"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 includes but is not limited to:

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

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

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

(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.

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

"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.

"Internet service provider" means a natural or legal person that provides to users services mentioned in sections 37 - 42 hereof;

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

"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.

"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 computer data that:

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

(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.

"Thing" 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.

"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

OFFENCES

Aggravating circumstances Sections 5, 7, 8, 10 and 11

4 In this Part the crime of illegal access to or use of a computer, illegal interception. illegal data interference, illegal system interference, and illegal 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, 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, 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 or like 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.

Illegal Access

5. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) Where the unauthorised access under subsection (1) is gained by infringing security measures or with the intent of obtaining computer data, a person convicted of the offence under subsection (1) shall be liable to imprisonment for a term not exceeding [period] or to a fine not exceeding [amount] or both.

(3) Where the unauthorised access under subsection (1) was committed in any of the aggravating circumstances described in section 4 the person shall be liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years
or both.

Illegal Remaining

6. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, by infringing security measures or with the intent of obtaining computer data or other dishonest intent remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding

[amount], or both.

Illegal Interception

7. (1) A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means:

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) Where the illegal interception under subsection (1) was committed in any of the aggravating circumstances described in section 4 the person shall be liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years
or both.

Illegal Data Interference

8. (1) Subject to subsection 2 and 5, a person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts:

(a) damages or deteriorates computer data; or

(b) deletes computer data ; or

(c) alters computer data; or

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

(e) obstructs, interrupts or interferes with the lawful use of computer data; or

(f) obstructs, interrupts or interferes with any person in the lawful use of computer data; or

(g) denies access to computer data to any person authorized to access it; or

(h) fraudulently or mischievously creates, alters or manipulates any data, programme or system (or any part or portion thereof) which is intended for installation in a computer;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period] or a fine not exceeding [amount], or both.

PROVIDED that where the offence under subsection (1) was committed in any of the aggravating circumstances described in section 4 the person shall be liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

(2) A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification commits any act described in this section in order to deny access, including a partial denial of service to any

person authorised to access it commits an offence and is liable, upon conviction, to a fine not less than [period] but not exceeding [period] or to imprisonment for a period not exceeding [period], or to both.

(3) A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification —

a) communicates, discloses or transmits any computer data, program, access code or command to any person not authorized to access the computer data, program, code or command;

(b) accesses or destroys any computer data, for purposes of concealing information necessary for an investigation into the commission, or otherwise of an offence;

(c) receives computer data and is not authorized to receive that computer data,

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

(4) A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification destroys —or alters computer data where such data is required to be kept or maintained by law for the time being in force or any evidence in relation to any proceeding under this Act by

(a) creating, destroying- mutilating, removing or modifying data or program or any other form of information existing within or outside a computer or computer network; or

(b) activating or installing or downloading 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) creating, altering, or destroying a password, personal " identification number, code or method used to access a computer or computer network,

commits an offence and shall be liable on conviction to a fine of not less than [period] or to imprisonment for a term but not exceeding [period] or to both such fine and imprisonment.

(6) 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.

(5) Where an offence under this section is committed in relation to data that is in a critical database or that is concerned with national security or the provision of an essential service, the person shall be liable, upon conviction, to imprisonment for a term not exceeding [period].

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

Data Espionage

9. (1) A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification obtains, for himself or for another, computer data which are not meant for him and which are specially protected against unauthorized access, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Illegal System Interference

10. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification:

(a) hinders or interferes with the functioning of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding three years, and a fine not exceeding level eight, or both.

(2) A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification seizes or destroys any computer storage medium commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], and a fine not exceeding [amount], or both.

(3) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding ten years, or a fine not exceeding level twelve, or both.

(4) Where the offence in subsection (1) (a) was committed in any of the

aggravating circumstances described in Section 4 the person shall be liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

Illegal Devices

11. (1) A person commits an offence if the person:

(a) intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, 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) 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 on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or 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.

Where the offence in subsection (1) was committed in any of the aggravating circumstances described in Section 4, to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

Computer-related Forgery

12. (1) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification 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 punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not

exceeding[amount] or both.

Computer-related Fraud

13. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification 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 the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount] or both.

Child Pornography

14. (1) A person who intentionally, without lawful excuse or justification:

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

commits an offence punishable, on conviction, by imprisonment for a period not exceeding ten years, or a fine not exceeding level twelve or 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.

(3) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification makes pornography available to one or more children through a computer system or facilitates the access of children to pornography through a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount] or both.

.

Pornography

15. (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 twelve 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

16. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification 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 punishable, on conviction, by imprisonment for a period not exceeding three years or to a fine not exceeding level eight or both.

Racist and Xenophobic Material

17. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification

(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 punishable, on conviction, by imprisonment for a period not exceeding [period] , or a fine not [amount] , or both.

Racist and Xenophobic Motivated

18. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification 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

Insult

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 punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Denial of Genocide and Crimes Against Humanity

19. A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification 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 punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

SPAM

20. (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

Disclosure of details of an investigation

21. An Internet service provider 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 intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses:

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

(b) anything done under the order; or

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

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding[amount], or both.

Failure to permit assistance

22. (1) A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 30 to 32 commits an offence punishable, on conviction, by imprisonment for a period not exceeding[period], or a fine not exceeding [amount], or both.

Harassment utilizing means of electronic communication

23. (1)A person, who intentionally without lawful excuse or justification or in excess of a lawful excuse or justification 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 punishable, on conviction, by imprisonment for a period not exceeding five year, or a fine not exceeding level ten, or both.

Violation of intellectual property rights

24. Any person who uses any computer system or to violate any intellectual property rights protected under any law or treaty applicable to intellectual property rights in Zimbabwe, commits an offence under this Act and shall be liable and upon conviction, in addition to any penalty or relief provided under the intellectual property law in question, to a fine of not less than [amount] or imprisonment for a term of not more than [period] or to both such fine and imprisonment.

Attempt Abetment and Conspiracy

25. (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,

commits an offence and shall be liable on conviction to the punishment provided for such an offence under this Act.

(2) For the purposes of this section, "attempt" shall have the meaning ascribed to it under the [penal code].

PART III
JURISDICTION

Jurisdiction

26. (1) The courts in Zimbabwe shall have jurisdiction to try any offence under this Act or any regulations made under it where an act or omission constituting an offence under this Act has been committed wholly or in part –

(a) within the territory of Zimbabwe; or

(b) on a ship or aircraft registered in Zimbabwe

(c) ; or

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

(d) by a national of Zimbabwe outside the territory of Zimbabwe, 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,

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

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

(3) directed against equipment, 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 proceedings for an offence against a law of Zimbabwe, 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 the [Electronic Transactions and Communication Act Chapter … : …] shall apply to this Part.

PART V

PROCEDURAL LAW

Search and Seizure

29. (1) If a magistrate is satisfied on the basis of an application by a police officer supported by affidavit that there are reasonable grounds or to suspect or to believe that there may be in a place a thing 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;

the magistrate may issue a warrant authorizing a [law enforcement or police officer, with such assistance as may be necessary, to 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 Zimbabwe.

(2) If a police officer that is undertaking a search based on Section 28(1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system.

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

Assistance

30. (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 28 must permit, and assist if reasonably required and requested by 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 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.

(f) (f) A person who, without lawful excuse or justification, refuses or fails to assist when called upon to do so 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. If magistrate is satisfied on the basis of an application by a law enforcement officer or police 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 magistrate may order 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 Internet service provider in Zimbabwe to produce information about persons who subscribe to or otherwise use the service.

Expedited preservation

32. If a police officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the law enforcement or police officer 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 beyond seven (7) days if, on an application a judge or magistrate authorizes an extension for a further specified period of time.

Partial Disclosure of traffic data

33. If a police officer is satisfied computer data is reasonably required for the purposes of a criminal investigation, the law enforcement or police officer may, 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 Internet service providers; and/or

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

Collection of traffic data

34. (1) If a magistrate is satisfied on the basis of an application by a police 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, magistrate 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 police officer to collect or record that data.

(2) If magistrate is satisfied on the basis of an application by a police 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 magistrate may authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Interceptio-n of content data

35. (1) If a magistrate is satisfied on the basis of an application by a police 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 magistrate may:

(a) order an Internet 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

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

Forensic Tool

36. (1) If a magistrate is satisfied on the basis of an application by a police officer, supported by affidavit that in an investigation concerning an offence listed in paragraph 7 herein-below or regulations made under Section 45 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 magistrate may authorize a police officer to utilize a remote 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 needs 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, unauthorized deletion and unauthorized access.

(3) The duration of authorization in section 35(1) shall be limited to 3 months. Where the conditions of the authorization are no longer met, the action taken shall be stopped immediately.

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

(5) Where the installation process requires physical access to a place the requirements of section 28 shall need to be fulfilled.

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

(7) The offences referred to in subsection (1) include:
i. Murder or Manslaughter or treason.
ii. Kidnapping or abduction.
iii. Money laundering contrary to the [proceeds of crime] Act.
iv. Producing, manufacturing, supplying or otherwise dealing in any dangerous drug in contravention of the [dangerous drugs] Act.
v. Importing or exporting a dangerous drug in contravention of the [dangerous drugs] Act.
vi. Importation, exportation or trans-shipment of any firearm or ammunition in contravention of the [firearms] Act.
vii. Manufacture of, or dealing, in firearms or ammunition in contravention of the [firearms] Act.
viii. Illegal possession of a prohibited weapon or any other firearm or ammunition contrary to the [firearms] Act.
ix. An offence contrary to the [prevention of corruption] Act.
x. Arson.
xi. International Convention on hijacking, terrorist offences etc.
xii. [prevention of terrorism] Act.
xiii. Attempting or conspiring to commit, or aiding, abetting, counseling or procuring the commission of, an offence falling within any of the preceding paragraphs.

PART VI

LIABILITY

When providing the services under this Part -

No Monitoring Obligation

37. (1) An Internet service provider shall, subject to the provisions of any other written law, have no general obligation to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.

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.

Access Provider

38. (1) An access 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.

(3) An access provider who violates the conditions set out in paragraphs (1) and (2) 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.

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 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.

(2) A hosting provider who fails to remove or disable access to the information in terms of section 1 (a) and 1 (b) above 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. 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.

(f) A catching provider who violates any of the conditions stated in paragraphs (a) to (e) above 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. 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.

(c) An Internet Service Provider who fails to expeditiously remove or disable access to information in terms of paragraphs (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 paragraphs (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

Limitation of Liability

43. Neither the state nor the Minister the Authority nor any public officer or employee shall be liable in respect of the performance of any act or any omission where such act or omission was done in good faith and without gross negligence in accordance with the provisions of this Act.

Forfeiture of Assets

44. (1) The Court in imposing sentence on any person who is convicted of an offence under this Act, may also order that the convicted person forfeits to Zimbabwe –

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

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

(3) Any person convicted of an offence under this Act shall forfeit his passport or international travelling document to Zimbabwe until he has paid the fines or served the sentence imposed on him.

(3)Notwithstanding subsection (2) of this section, the court may:

(a) upon the grant of pardon by the President to the convicted person; or

(b) for the purposes of allowing the convicted person to travel abroad for treatment; or

(c) in the interest of the public; and

(d) upon application

grant an order that the passport or travelling document of the convicted person be released to him.

General Provision on Cybercrimes

45. 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 with the necessary modification to the person who commits the offence.

Regulations

46. (1)The Minister may, in consultation with the Authority and on the advice of the Attorney General 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 which regulations may include 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.

Offence by body corporate or un-incorporate

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

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

body; and

(2) 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.

Prosecutions

48. Criminal proceedings under this Act shall be instituted by or with the consent of the Director of Public Prosecutions of Zimbabwe.

Compounding of Offences

49. Without prejudice to any other law in force in Zimbabwe, the Director of Public Prosecutions may, subject to voluntary admission of the commission of the offence, compound any offence punishable under this Act by accepting such amount specified as a fine to which the offender would have been liable if he had been convicted of that offence.

PART VIII

CONSEQUENTIAL AMENDMENTS

(a) AMENDMENT OF POSTAL AND TELECOMMUNICATIONS ACT, CHAPTER 12:05

Construction Chapter 12:05

50. This Part shall be read as one with the Postal and Telecommunications Act, Number 4 of 2012 hereinafter referred to as the "principal Act"

Amendment of Section 88

51. The principal Act is amended in Section 88 by deleting the said Section

PART IX

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

Construction Criminal

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

Code "principal Act"

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

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

.

.

SCHEDULE (Section 3(2))

CORRESPONDENCE OF REFERENCES TO CRIMES IN CODE OR OTHER ENACTMENTS TO PROVISIONS OF COMPUTER CRIME AND CYBERCRIME ACT DEFINING SUCH CRIMES

Crime	*Provision in Computer Crime and Cybercrime Act defining it*
Aggravated indecent assault	Section 14
Allowing child to become a prostitute	Section 14
Interpretation in Chapter VIII	Section 3
Unauthorised access to or use of computer or computer network	Section 4
Deliberate introduction of computer virus into computer or computer network	Section 23
Offensive or false telephone messages	Section 22
Unauthorised manipulation of proposed computer programme	Section 9
Aggravating circumstances in relation to crimes under sections 163, 164 and 165	Section 4
Unauthorised use or possession of credit or debit cards	Section 16