GOVERNMENT OF ZAMBIA

ACT

No. 13 of 2004

Date of Assent: 2nd September, 2004

An Act to prohibit any unauthorised access, use or interference with a computer; to protect the integrity of computer systems and the confidentiality, integrity and availability of data; to prevent abuse of computer systems; to facilitate the gathering and use of electronic evidence; and to provide for matters connected with or incidental to the foregoing.

[8th September, 2004

ENACTED by the Parliament of Zambia. Enactment

PART I

PRELIMINARY

1. This Act may be cited as the Computer Misuse and Crimes Act, 2004, and shall come into operation on such date as the Minister may, by statutory instrument, appoint. Short title and commencement

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

"computer" means an electronic, optical, electrochemical or a magnetic, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnection or related devices, or such other equipment or device as the Minister may, by statutory instrument prescribe, taking into consideration developments in technology, but does not include —

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator; or

(c) a similar device which is non-programmable or which does not contain any data storage facility;

" computer output " or " output " means a statement or representation, whether in written, printed, pictorial, graphical or any other form, purporting to be a statement or representation of fact—

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

" computer service " includes computer time, computer output, data processing and the storage or retrieval of a program or data;

" data " means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

" electronic, acoustic, mechanical or other device " means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

" function " includes logic, control, arithmetic, deletion, storage and retrieval, and communication or telecommunication to, from or within a computer;

" intercept " includes, in relation to a function of a computer, listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof; and

" program or computer program " means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

Application of offences under this Act

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

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

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

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

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

PART II

OFFENCES

Unauthorised access to computer program or data

4. (1) A person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer commits an offence and is liable on conviction for a first offence to a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding two years or to both and, in the case of a subsequent offence, to a fine not exceeding sixty thousand penalty units or to imprisonment for a term not exceeding five years or to both.

(2) For the purposes of this section and this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if the person—

(a) is not entitled to control access of the kind in question to the program or data; and

(b) does not have consent to access the kind of program or data in question from the person who is entitled to control access.

(3) For the purpose of this section, a person secures or gains access to any program or data held in a computer if by causing the computer to perform any function the person—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner, and references to access to a program or data and to an intent to secure such access shall be construed accordingly.

(4) For the purpose of paragraph *(c)* of subsection (3), a person uses a program if the function the person causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

(5) For the purpose of paragraph *(d)* of subsection (3), the form in which any program or data is output, and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial.

(6) For the purpose of this section, it is immaterial that the act in question is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(7) A reference in this section and Act to a program or data in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(8) A reference in this Act to a program includes a reference to part of a program.

(9) For the purpose of this Act—

(a) a program or data held in a computer or in any storage medium capable of being accessed and printed into readable form through a computer is a document; and

(b) it is immaterial that access to a program or data held in a computer is achieved through the use of that or any other computer or by any other means.

Access with intent to commit or facilitate commission of offence

5. (1) A person who knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer with intent to commit or facilitate the commission of an offence involving property, fraud, dishonesty or which causes bodily harm, commits an offence and is liable on conviction to a fine not exceeding three hundred thousand penalty units or to imprisonment for a term not exceeding seven years, or to both.

(2) For the purpose of this section, it is immaterial whether—

(a) the access referred to in subsection (1) is authorised or unauthorised; or

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorised modification of computer program or data

6. (1) A person who does a direct or an indirect act without authority which the person knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on conviction for a first offence to a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding three years, or to both, and, in the case of a subsequent offence, to a fine not exceeding one hundred thousand penalty units or to imprisonment for a term not exceeding six years, or to both.

(2) For the purpose of this section —

(a) it is immaterial that the act in question is not directed at—

(i) any particular program or data;

(ii) a program or data of any kind; or

(iii) a program or data held in any particular computer;

(b) it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary;

(c) a modification of any program or data held in any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(i) any program or data held in any computer is altered or erased;

(ii) any program or data is added to or removed from any program or data held in any computer; or

(iii) any act occurs which impairs the normal operation of any computer;

and any act which contributes towards causing such a modification shall be regarded as causing it.

(3) Any modification referred to in this section is unauthorised if the person—

(a) whose act causes it is not entitled to determine whether the modification should be made; and

(b) does not have consent to the modification from the person who is so entitled.

Unauthorised use or interception of computer service

7. A person who knowingly and without authority—

(a) secures access to a computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted directly or indirectly, any function of any computer by means of an electromagnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, a computer, or any other device for the purpose of committing an offence under paragraph *(a)* or *(b)*,

commits an offence and is liable on conviction—

(i) in the case of the first offence to a fine not exceeding two thousand penalty units or to imprisonment for a term not exceeding five years, or to both; and

(ii) in the case of a subsequent offence, to a fine not exceeding three hundred thousand penalty units or to imprisonment for seven years.

(2) For the purpose of this section, it is immaterial that the unauthorised access or interception is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Unauthorised obstruction of use of computer

8. A person who knowingly and without authority—

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

(b) impedes, prevents access to, or impairs the usefulness or effectiveness of any program or data held in a computer;

(c) causes direct or indirectly, a degradation, failure, or other impairment of function of a computerised system or any part therefor.

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

Unauthorised disclosure of access code

9. (1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer commits an offence and is liable on conviction—

(a) in the case of a first offence to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both; and

(b) in the case of a second or subsequent offence, to a fine not exceeding three hundred thousand penalty units or imprisonment for a term not exceeding seven years, or to both.

(2) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in a computer commits an offence if the person didso—

(a) for any unlawful gain, whether to oneself or to another person;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause unlawful damage, and is liable on conviction—

(i) in the case of a first offence to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding five years; and

(ii) in the case of a subsequent offence to a fine not exceeding three hundred thousand penalty units or to imprisonment for a term not exceeding seven years or to both.

Enhanced punishment for offences involving protected computers

10. (1) Where access to any protected computer is obtained in the course of the commission of an offence under section *four, five, six* or *eight,* the person convicted of such an offence shall, in lieu of the penalty prescribed in those sections, be liable on conviction to imprisonment for a term of not less than fifteen years but not exceeding twenty-five years, or to both.

(2) For the purpose of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known that the computer, program or data is used directly in connection with or is necessary for—

(a) the security, defence or international relations of the State;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or key public infrastructure;

(d) the storing of classified Government information, or

(e) the protection of public safety and public health, including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purpose of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer or program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer or program or data attracts an enhanced penalty under this section.

Unauthorised receiving or giving access to computer program or data

11. (1) A person who receives or is given access to any program or data held in a computer and who is not authorised to receive or have access to that program or data whether or not the person knows that the person giving him the program or data has obtained that program or data through authorised or unauthorised means, commits an offence and is liable on conviction to a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(2) A person who is authorised to receive or have access to any program or data held in a computer and who receives that program or data from another person knowing that the other person has obtained that program or data through unauthorised means commits an offence and is liable on conviction to a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding three years, or to both.

(3) A person who has obtained any program or data held in a computer through authorised means and gives that program or data to another person who the person knows is not authorised to receive or have access to that program or data commits an offence and is liable on conviction to a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(4) A person who has obtained any program or data held in a computer through unauthorised means and gives that program or data to another person whether or not the person knows that that other person is authorised to receive or have access to that program or data commits an offence and is liable on conviction to a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

Causing a computer to cease to function

12. (1) A person who with requisite knowledge and intent engages in conduct which causes a computer to cease to function permanently or temporarily and at the time the person engages in that conduct has knowledge that the conduct is unauthorised commits an offence and is liable on conviction to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

(2) For the purpose of subsection (1)—

(a) "requisite knowledge" means knowledge that the conduct would or would be likely to cause a computer to cease to function permanently or temporarily; and

(b) "requisite intent" means intent to cause a computer to cease to function and by so doing—

(i) prevents or hinders access to the computer; or

(ii) impair the operation of the computer, but the intent need not be directed at a particular computer.

Omission to introduce, record or store data

13. A person who being under a contractual obligation or other duty to introduce, record or store a program or data into a computer, computer system or network and intentionally, or dishonestly fails to so introduce, record or store the program or data into such computer, commits an offence and is liable on conviction, or to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding five years, or to both.

Offences by corporation

14. Where a corporation is convicted of an offence, or is fined under this Act, any person who is a director of, or who is concerned in the management of that corporation shall be deemed to have committed the same offence and is liable to be fined as if the person authorised or permitted the act or omission constituting the offence:

Provided that where, at the trial of a corporation for an offence under this Act, a director or any person concerned in the management of that body corporate shows that—

(a) the act constituting the offence was done without the knowledge or consent of that director or person; or

(b) the director or person took, reasonable steps to prevent the act from being committed;

the director or person shall not be liable.

PART III

GENERAL PROVISIONS

Order for payment of compensation

15. (1) The Court before which a person is convicted of any offence under this Act may make an order against such person for the payment of a sum to be fixed by the Court by way of compensation to any person for any damage caused to that person's computer, program or data as a result of the offence for which the sentence is passed.

(2) A claim by a person for damages sustained by reason of the offence is deemed to have been satisfied to the extent of any amount which has been paid to such person under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order for compensation under this section is recoverable as a civil debt.

(4) For the purpose of this section, a program or data held in a computer is deemed to be the property of the owner of the computer.

Search and seizure warrants

16. (1) Where a Magistrate is satisfied by information on oath given by a police officer that there are reasonable grounds for believing that an offence under this Act has been or is about to be committed in any place and that evidence that such an offence has been or is about to be committed is in that place, the Magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer, using such reasonable force as is necessary.

(2) A warrant issued under this section may also direct an authorised person to accompany any police officer executing the warrant and remains in force for twenty-eight days from the date of its issue.

(3) In executing a warrant under this section, a police officer may seize any computer, data, program, information, document or thing if the police officer reasonably believes that it is evidence that an offence under this Act has been or is about to be committed.

(4) A police officer executing a warrant may be accompanied by an authorised person and is—

(a) entitled, with the assistance of that person, to—

(i) have access to and inspect and check the operation of any computer to which this section applies;

(ii) use or cause to be used any such computer to search any program or data held in or available to such computer;

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted program or data held in or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section; and

(iv) to make and take away a copy of any program or data held in the computer or data held in the computer as specified in the search warrant and any other program or data held in that or any other computer which the police officer has reasonable grounds to believe is evidence of the commission of any other offence;

(b) entitled to require—

(i) the person by whom or on whose behalf, the police officer has reasonable cause to suspect, any computer to which this section applies is or has been used; or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer, to provide the police officer or any authorised person with such reasonable technical and other assistance as the police officer or authorised person may require for the purposes of paragraph *(a)*; and

(c) entitled to require any person in possession of decryption information to grant the police officer or the authorised person access to such decryption information necessary to decrypt data required for the purpose of investigating an offence.

(5) A person who obstructs a police officer in the execution of duty under this section or who fails to comply with a request under this section commits an offence and is liable on conviction to a fine not exceeding thirty thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(6) For the purposes of this section--

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted program or data from its unreasonable and incomprehensible format to its plain text version;

"encrypted program or data" means a program or data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such program or data occur or can be found for the purpose of protecting the content of such program or data; and

"plain text version" means a program or original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

Regulations

17. The Minister may, by statutory instrument, make regulations for the better carrying out of the provisions of this Act.