COMPUTER MISUSE AND CYBERCRIME ACT

Act 22 of 2003 – 9 August 2003

ARRANGEMENT OF SECTIONS

COMPUTER MISUSE AND CYBERCRIME ACT

PART I – PRELIMINARY

1. Short title

This Act may be cited as the Computer Misuse and Cybercrime Act.

2. Interpretation

In this Act—

"access", in relation to any computer system, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system;

"asymmetric cryptosystem" means a system capable of generating a secure key

pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device or combination of devices, including input and output devices, but excluding calculators which are not programmable, and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

"data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium;

"digital signature"—

(a) means an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem such that a person having the initial untransformed electronic record and the signer's public key can accurately determine—

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

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

(b) includes voice recognition relating features, digital finger-printing or such other biotechnological features or process, as may be prescribed;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;

"electronic record" means a record created, generated, sent, communicated, received or stored by electronic means;

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

"information and communication service" means any service involving the use of information and communication technologies, including telecommunication services;

"information and communication technologies" means technologies employed in collecting, storing, using or sending out information and include those involving the use of computers or any telecommunication system;

"intercept", in relation to a function of a computer, includes listen to, or record a function of a computer, or acquire the substance, its meaning or purport of such function;

"investigatory authority" means the police or any other body lawfully empowered to investigate any offence;

"key" means either a public or private key;

"modification" means a modification of the contents of any computer system by the operation of any function of that computer system or any other computer system as a result of which—

(a) any program or data held in the computer system is altered or erased;

(b) any program or data is added to its contents; or

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

"password" means any data by which a computer service or a computer system is

capable of being obtained or used;

"private key" means the key of a key pair used to create a digital signature;

"program" means a set of instructions, expressed in words, codes, schemes or any other form, which is capable, when incorporated in a machine readable medium, of causing a computer to perform or achieve a particular task or result;

"property" means property of any kind, nature or description, whether moveable or immoveable, tangible or intangible and includes—

(a) any currency, whether or not the currency is legal tender in Mauritius;

(b) information, including an electronically produced data or program, or a copy thereof, whether tangible or intangible, human or computer readable data, or data while in transit; or

(c) any right or interest in property;

"public key" means the key of a key pair used to verify a digital signature;

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form;

"service provider" means any person who provides an information and communication service, including a telecommunication service;

"subscriber" means a person using the services of a service provider;

"subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers, other than traffic or other data, by which can be established—

(a) the type of the communication service used, the technical provisions taken to use the communication service and the period of the service;

(b) the subscriber's identity, postal or geographical address, telephone and other access number, billing and payment information, available on the basis of a service agreement or arrangement; or

(c) any other information on the site of installation of a communication equipment available on the basis of a service agreement or arrangement;

"telecommunication" means a transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, optical or other electro-magnetic systems, whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of their transmission, emission or reception;

"traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

"underlying service" means the type of service that is being used within the computer system.

PART II – OFFENCES

3. Unauthorised access to computer data

(1) Subject to subsections (2) and (3), any person who causes a computer system to perform a function, knowing that the access he intends to secure is unauthorised, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50,000 rupees and to penal servitude for a term not exceeding 5 years.

(2) A person shall not be liable under subsection (1) where—

(a) he is a person with a right to control the operation or use of the computer system and exercises such right in good faith;

(b) he has the express or implied consent of the person, empowered to authorise him, to have such an access;

(c) he has reasonable grounds to believe that he had such consent as specified in paragraph (b);

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

(e) he is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

(3) An access by a person to a computer system shall be unauthorised where the person—

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

(b) does not have consent to access by him of the kind in question from any person who is so entitled.

(4) For the purposes of this section, it is immaterial that the unauthorised access 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 system.

4. Access with intent to commit offences

(1) Any person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system with intent to commit an offence under any other enactment, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.

(2) For the purposes of this section, it is immaterial that—

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

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

5. Unauthorised access to and interception of computer service

(1) Subject to subsection (5), any person who, by any means, knowingly—

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

(b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within, a computer system,

shall commit an offence.

(2) (a) A person convicted of an offence under subsection (1) shall be liable to a fine not exceeding 100,000 rupees and to penal servitude for a term not exceeding 10 years.

(b) Where, as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, a person convicted of such offence shall be liable to a fine not

exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.

(3) 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 system.

(4) A person shall not be liable under subsection (1) where he—

(a) has the express or implied consent of both the person who sent the data and the intended recipient of such data;

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

6. Unauthorised modification of computer material

(1) Subject to subsections (3) and (4), any person who knowingly does an act which causes an unauthorised modification of data held in any computer system shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to penal servitude for a term not exceeding 10 years.

(2) Where as a result of the commission of an offence under this section—

(a) the operation of the computer system;

(b) access to any program or data held in any computer; or

(c) the operation of any program or the reliability of any data,

is suppressed, modified or otherwise impaired, a person convicted of the offence shall be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.

(3) A person shall not be liable under this section where—

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

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

(4) A modification shall be unauthorised if—

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

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

(5) For the purposes of this section, it is immaterial whether an unauthorised modification or any intended effect of it be permanent or merely temporary.

7. Damaging or denying access to computer system

Any person who without lawful authority or lawful excuse, does an act which causes directly or indirectly—

(a) a degradation, failure, interruption or obstruction of the operation of a computer system; or

(b) a denial of access to, or impairment of any program or data stored in, the computer system,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to penal servitude not exceeding 20 years.

8. Unauthorised disclosure of password

Any person who, knowingly discloses any password, access code, or any other means of gaining access to any program or data held in any computer system—

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause prejudice to any person,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 5 years.

9. Unlawful possession of devices and data

(1) Any person who knowingly manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system or any other device, designed or adapted primarily for the purpose of committing any offence under sections 3 to 8, shall commit an offence.

(2) Any person who knowingly receives, or, without sufficient excuse or justification, is in possession of, one or more of the devices under subsection (1) shall commit an offence.

(3) Any person who is found in possession of any data or program with the intention that the data or program be used, by the person himself or another person, to commit or facilitate the commission of an offence under this Act, shall commit an offence.

(4) For the purposes of subsection (3), possession of any data or program includes—

(a) having possession of a computer system or data storage device that holds or contains the data or program;

(b) having possession of a document in which the data or program is recorded; or

(c) having control of data or program that is in the possession of another person.

(5) Where a person is convicted under this section, he shall be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 5 years.

10. Electronic fraud

Any person who fraudulently causes loss of property to another person by—

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

(b) any interference with the functioning of a computer system,

with intent to procure for himself or another person, an advantage, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.

PART III – INVESTIGATIONS AND PROCEDURES

11. Preservation order

(1) Any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purposes of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence;

(b) where prosecution is instituted, until the final determination of the case; or

(c) until such time as the Judge in Chambers deems fit.

12. Disclosure of preserved data

The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data;

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or

(c) electronic key enabling access to or the interpretation of data.

13. Production order

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling—

(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

14. Powers of access, search and seizure for purposes of investigation

(1) Where an investigatory authority has reasonable grounds to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize such data.

(2) In the execution of a warrant under subsection (1), the powers of the investigatory authority shall include the power to—

(a) seize or secure a computer system or any information and communication technologies medium;

(b) make and retain a copy of such data or information;

(c) maintain the integrity of the relevant stored data or information; or

(d) render inaccessible or remove the stored data or information from the computer system, or any information and communication technologies medium.

15. Real time collection of traffic data

Where the investigatory authority has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, it may apply to the Judge in Chambers for an order—

(a) allowing the collection or recording of traffic data, in real time, associated

with specified communications transmitted by means of any computer system; or

(b) compelling a service provider, within its technical capabilities, to—

(i) effect such collection and recording referred to in paragraph (a); or

(ii) assist the investigatory authority to effect such collection and recording.

16. Deletion order

A Judge in Chambers may, upon application by an investigatory authority, and being satisfied that a computer system or any other information and communication technologies medium contains an indecent photograph of a child, order that such data be—

(a) no longer stored on and made available through the computer system or any other medium; or

(b) deleted or destroyed.

17. Limited use of disclosed data and information

No data obtained under sections 11 to 15 shall be used for any purpose other than that for which the data was originally sought except—

(a) in accordance with any other enactment;

(b) in compliance with an order of a Court or Judge;

(c) where such data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable to the Government;

(d) for the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or

(e) in the public interest.

PART IV – MISCELLANEOUS

18. Prosecution

No prosecution shall be instituted under this Act except on an information filed by, or with the consent of, the Director of Public Prosecutions.

19. Jurisdiction

(1) Notwithstanding any other enactment, the Intermediate Court shall have jurisdiction to try any offence under this Act or any regulations made under it and may, on conviction, impose any penalty or forfeiture provided for under this Act.

(2) The Intermediate Court shall also have jurisdiction where the act constituting an offence under this Act has been committed outside Mauritius—

(a) on board a Mauritian ship; or

(b) on board an aircraft registered in Mauritius.

20. Extradition

Any offence under sections 3, 4, 5, 6, 7 and 10 of this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

21. Forfeiture

The Court before which a person is convicted of an offence may, in addition to any other penalty imposed, order the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence.

22. – 23. —