CYBERCRIME AND COMPUTER RELATED CRIMES ACT, 2007

No. 22 **of 2007**

ARRANGEMENT OF SECTIONS

SECTION

PART I — *Preliminary*

1. Short title
2. Interpretation
3. Jurisdiction

PART II — *Offences*

4. Unauthorised access to a computer or computer system
5. Unauthorised access to computer service
6. Access with intent to commit an offence
7. Unauthorised interference with data
8. Unauthorised interference with a computer or computer system
9. Unlawful interception of data
10. Unlawful possession of devices or data
11. Unauthorised disclosure of password
12. Damage to a computer or computer system
13. Protected computers
14. Cyber extortion
15. Cyber fraud
16. Electronic traffic in pornographic or obscene material
17. Unlawful disclosure by service provider
18. Attempt
19. Parties to an offence

PART III — *Procedural Powers*

20. Preservation order
21. Disclosure of preserved data
22. Production order
23. Access, search and seizure
24. Real time collection of traffic data
25. Deletion order
26. Acting without an order
27. Limited use of disclosed data and information
28. Non-compliance with order or notice

PART IV — *Miscellaneous*

29. Extradition
30. Regulations

An Act to combat cybercrime and computer related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence.

Date of assent: 24.12.2007
Date of commencement: 28.12.2007

ENACTED by the Parliament of Botswana.

PART I — *Preliminary*

Short title

1. This Act may be cited as the Cybercrime and Computer Related Crimes Act, 2007.

Interpretation

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

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

"Commissioner" means the Commissioner of Police appointed by the President in terms of section 112 of the Constitution;

"computer data storage medium" means any device or material from which data is capable of being stored or reproduced, with or without the aid of any other device or material;

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

"computer or computer system" means an electronic, magnetic or optical device or a group of interconnected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function;

"data" means —

(*a*) any representation of facts, information or concepts in a form suitable for processing in a computer or computer system;

(*b*) any information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; or

(*c*) a programme suitable to cause a computer or computer system to perform a function;

"Director " means the Director of the Directorate on Corruption and Economic Crime appointed by the President in terms of section 4 of the Corruption and Economic Crime Act or any person who may be appointed by the Minister by notice published in the Gazette;

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

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

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

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

"intercepts" means the aural or other acquisition of the contents of any electronic, magnetic, optical or oral communication through the use of any device;

"national emergency organisations" include the police force, security forces, fire brigade, ambulance services, medical services, veterinarian services and environmental disaster agencies, whether or not such organisations are owned and managed on a private or public basis;

"password" means any data by which a computer service, computer or computer system is capable of being obtained, accessed or used;

"programme" means an instruction or 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 or computer system to 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 Botswana;

(*b*) information, including an electronically produced programme or data or copy thereof, whether tangible or intangible, human or computer-readable data, or data in transit; or

(*c*) any right or interest in property;

"service provider" means any public or private person who —

(*a*) provides to users of its services the ability to communicate by means of a computer or computer system;

(*b*) processes or stores computer data on its behalf or on behalf of the users of its services; or

(*c*) provides an information and communication service, including telecommunication;

"subscriber" means a person who lawfully uses the service of a service provider;

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

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

(*b*) information available on the basis of a service agreement or arrangement, including information on the site of installation of communication equipment or information on the subscriber's identity, postal or geographical address or billing or payment information;

"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 —

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

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

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

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

Jurisdiction

3. The courts of Botswana shall have jurisdiction where an act done or an omission made constituting an offence under this Act has been committed —

(*a*) in the territory of Botswana;

(*b*) by a national of Botswana outside the territory of Botswana, if the person's conduct would also constitute an offence under the law of the country where the offence was committed and if the person has not been prosecuted for the offence in that country;

(*c*) on a ship or aircraft registered in Botswana;

(*d*) in part in Botswana; or

(*e*) outside the territory of Botswana and where any result of the offence has an effect in Botswana.

PART II — *Offences*

Unauthorised access to a computer or computer system

4. (1) Subject to subsections (2) and (3), any person who —

(*a*) accesses the whole or any part of a computer or computer system, knowing that the access he or she intends to secure is unauthorised; or

(*b*) causes a computer or computer system to perform any function as a result of unauthorised access to such system,

commits an offence and shall on conviction be liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

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

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

(*b*) has the express or implied consent of a person empowered to authorise him or her to have access to the computer or computer system;

(*c*) has reasonable grounds to believe that he or she had such consent as specified in subparagraph (*b*);

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

(*e*) is acting in reliance of any statutory power arising under any enactment or a power conferred under any Act, for the purpose of —

(i) obtaining information, or

(ii) taking possession of any document or other property.

(3) A person's access to a computer or computer system is unauthorised where the person —

(*a*) is not himself or herself entitled to access of the kind in question;

(*b*) does not have consent, from any person who is so entitled, to access of the kind in question; or

(*c*) exceeds the access he or she is authorised.

(4) For the purposes of this section, it is immaterial that the unauthorised access is not directed at —

(*a*) a particular programme or data;

(*b*) a programme or data of any kind; or

(*c*) a programme or data held in any particular computer or computer system.

Unauthorised access to computer service

5. (1) Subject to subsection (5), a person commits an offence where such person, knowingly and by any means, without authorisation or exceeding the authorisation he or she is given —

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

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

(2) A person who commits an offence under subsection (1) shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(3) Where, as a result of the commission of an offence under subsection (1), the operation of a computer or computer system is impaired, or data contained in the computer or computer system is suppressed or modified, a person shall on conviction be liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

(4) For the purposes of this section, it is immaterial that the unauthorised access or interception in subsection (1) is not directed at —

(*a*) a particular programme or data;

(*b*) a programme or data of any kind; or

(*c*) a programme or data held in any particular computer or computer system.

(5) A person shall not be liable under subsection (1) where he or she —

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

(*b*) is acting in reliance of a statutory power arising under any enactment or a power conferred under any Act.

Access with intent to commit an offence

6. (1) A person who, with intent to commit an offence under any other enactment, causes a computer or computer system to perform any function for the purpose of securing access to —

(*a*) any programme or data held in a computer or computer system; or

(*b*) a computer service,

commits an offence and shall on conviction be liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

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

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

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

Unauthorised interference with data

7. (1) A person who intentionally, without lawful excuse or justification, does any of the following acts —

(*a*) destroys, deletes, suppresses, alters or modifies data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with —

(i) the lawful use of data, or

(ii) any person in the lawful use of data; or

(*d*) denies access to data to any person entitled to it,

commits an offence and shall on conviction be sentenced to a minimum fine of P10 000 but not exceeding P40 000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

(2) Where, as a result of the commission of an offence under subsection (1), the following is impaired, suppressed, altered or modified —

(*a*) the operation of the computer or computer system;

(*b*) access to any programme or data held in any computer or computer system; or

(*c*) the operation of any programme or the reliability of any data,

a person shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

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

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

(*b*) is acting in reliance of any statutory power arising under any enactment or a power conferred under any Act, for the purpose of —

(i) obtaining information, or

(ii) taking possession of any document or other property.

(4) An interference is unauthorised —

(*a*) where the person whose act causes it is not himself or herself entitled to determine whether the interference of the kind in question should be made; or

(*b*) where the person does not have consent, from any person who is so entitled, to the interference of the kind in question.

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

Unauthorised interference with a computer or computer system

8. (1) A person who intentionally, without lawful excuse or justification —

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

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

commits an offence and shall on conviction be liable to a fine not exceeding P5 000 or to imprisonment for a term not exceeding three months, or to both.

(2) For the purposes of subsection (1) "hinder", in relation to a computer or computer system, includes —

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

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

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

(*d*) inputting, deleting, altering or modifying data; and

(*e*) impairing, by any means, the connectivity, infrastructure or support of a computer or computer system.

(3) A person who intentionally, without lawful excuse or justification, commits an act which causes, directly or indirectly —

(*a*) a denial, including a partial denial, of access to a computer or computer system; or

(*b*) an impairment of any programme or data stored in a computer or computer system, commits an offence and shall on conviction be sentenced to a minimum fine of P10 000 but not exceeding P40 000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

Unlawful interception of data

9. A person who intentionally and by technical means, without lawful excuse or justification, intercepts —

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

(*b*) electromagnetic emissions that are carrying data, from a computer or computer system,

commits an offence and shall on conviction be sentenced to a minimum fine of P10 000 but not exceeding P40 000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

Unlawful possession of devices or data

10. (1) A person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act, commits an offence and shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(2) A person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1), commits an offence and shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(3) A person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act, commits an offence and shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

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

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

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

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

Unauthorised disclosure of password

11. A person who intentionally, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to the whole or part of a computer or computer system —

(*a*) for wrongful gain;

(*b*) for any unlawful purpose;

(*c*) to overcome security measures for the protection of data; or

(*d*) with the knowledge that it is likely to cause prejudice to any person,

commits an offence and shall on conviction be liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

Damage to a computer or computer system

12. (1) In this section "computer contaminant" includes any programme which —

(*a*) modifies, destroys, records or transmits any data or programme residing within a computer or computer system;

(*b*) usurps the normal operation of a computer or computer system; or

(*c*) destroys, damages, degrades or adversely affects the performance of a computer or computer system or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer or computer system.

(2) A person who intentionally introduces, or causes to be introduced, a computer contaminant into any computer or computer system which causes, or is capable of causing, damage to such computer or computer system, commits an offence and shall on conviction be sentenced to a minimum fine of P40 000 but not exceeding P100 000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

Protected computers

13. (1) In this section, a "protected computer" means a computer or computer system or programme or data used directly in connection with, or necessary for —

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

(*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 public key infrastructure; or

(*d*) the protection of the public, including systems related to national emergency organisations.

(2) Where access to a protected computer is obtained in the course of the commission of an offence under this Act, the person convicted of any such offence shall be sentenced to a minimum fine of P40 000 but not exceeding P100 000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the person referred to in subsection (2) knew that the computer was a protected computer if there was, in respect of the computer, programme or data —

(*a*) provision for a warning within the computer, programme or data; or

(*b*) a warning exhibited to the person to the effect that unauthorised access to the computer, programme or data is prohibited.

Cyber extortion

14. A person who performs or threatens to perform any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by —

(*a*) undertaking to cease or desist from such actions; or

(*b*) undertaking to restore any damage caused as a result of those actions,

commits an offence and shall on conviction be liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

Cyber fraud

15. (1) A person who performs any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(2) A person who, with intent to procure any advantage for himself or herself or another person, 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 or computer system,

commits an offence and shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

Electronic traffic in pornographic or obscene material

16. (1) In this section —

(*a*) "publish" includes —

(i) to 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,

(ii) to have in possession or custody, or under control, for the purpose of doing an act referred to in subparagraph (*a*), or

(iii) to print, photograph, copy or make in any other manner (whether of the same or of a different kind of nature) for the purpose of doing any act referred to in subparagraph (*a*);

(*b*) "child pornography" includes material that visually or otherwise depicts —

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or

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

(*c*) "child" means a person who is under the age of 14 years; and

(*d*) "sexually explicit conduct" means any conduct, whether real or simulated, which involves —

(i) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic sexual abuse; or

(v) the exhibition of the genitals or pubic area of a child.

(2) A person who —

(*a*) publishes pornographic or obscene material through a computer or computer system;

(*b*) produces pornographic or obscene material for the purpose of its publication through a computer or computer system;

(*c*) possesses pornographic or obscene material in a computer or computer system or on a computer data storage medium;

(*d*) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows pornographic or obscene material; or

(*e*) accesses pornographic or obscene material through a computer or computer system,

commits an offence and shall on conviction be liable to a fine not exceeding P5 000 or to imprisonment for a term not exceeding three months, or to both.

(3) A person who —

(*a*) publishes child pornography or obscene material relating to children through a computer or computer system;

(*b*) produces child pornography or obscene material relating to children for the purpose of its publication through a computer or computer system;

(*c*) possesses child pornography or obscene material relating to children in a computer or computer system or on a computer data storage medium;

(*d*) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children; or

(*e*) accesses child pornography or obscene material relating to children through a computer or computer system,

commits an offence and shall be sentenced to a minimum fine of P40 000 but not exceeding P100 000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

(4) A person who, by means of a computer or computer system, communicates with —

(*a*) a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code; Cap. 08:01

(*b*) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or Cap. 08:01

(*c*) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of the offence of defilement or any sexual offence of that person under the Penal Code, Cap. 08:01

commits an offence and shall be sentenced to a minimum fine of P40 000 but not exceeding P100 000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

(5) Evidence that the person in paragraph (*a*), (*b*) or (*c*) of subsection (4) was represented to the accused as being under the age of 18 years or 16 years, as the case may be, is, in absence of evidence to the contrary, proof that the accused believed that the person was under that age.

(6) It shall not be a defence to a charge under subsection (4) that the accused believed that the person he or she was communicating with was at least 18 or 16 years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.

(7) For the purposes of subsection (4), it does not matter that the person in paragraph (*a*), (*b*) or (*c*) is a fictitious person, represented to the accused as a real person.

Unlawful disclosure by service provider

17. A service provider who, without lawful authority, discloses —

(*a*) that an order under this Act has been made;

(*b*) any act done under an order; or

(*c*) any data collected or recorded under an order,

commits an offence and shall be sentenced to a minimum fine of P10 000 but not exceeding P40 000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

Attempt

18. (1) A person who attempts to commit any of the offences described under this Part, commits an offence and shall on conviction be liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

(2) For the purposes of this section, "attempt" shall have the meaning ascribed to it under section 388 of the Penal Code. Cap. 08:01

Parties to an offence

19. (1) Where an offence is committed under this Part, each of the following persons is deemed to have taken part in committing the offence and is deemed to be guilty of the offence, and may be charged with actually committing it —

(*a*) a person who actually does the act or makes the omission which constitutes the offence;

(*b*) a person who does or omits to do any act for the purpose of enabling or aiding another person to commit the offence;

(*c*) a person who aids or abets another person in committing the offence; or

(*d*) a person who counsels or procures any other person to commit the offence.

(2) A person who counsels or procures any other person to commit an offence may be charged either with committing the offence or with counselling or procuring its commission.

(3) A conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence.

PART III — *Procedural Powers*

Preservation order

20. (1) A police officer or any person authorised by the Commissioner or by the Director, in writing, may, by written notice, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, 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.

Disclosure of preserved data

21. A police officer or any person authorised by the Commissioner or by the Director, in writing, may, by written notice given to a person in control of a computer or computer system, require the person to —

(*a*) ensure that the data specified in the notice is preserved for the period specified in the notice; or

(*b*) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted.

Production order

22. (1) A police officer or any person authorised by the Commissioner or by the Director, in writing, may apply to a judicial officer for an order compelling —

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

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

(2) Where the data in subsection (1) consists of data stored in an electronic, magnetic or optical form on a 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.

Access, search and seizure

23. (1) Where a police officer, or any person authorised by the Commissioner or by the Director, in writing, has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply to a judicial officer for the issue of an order to enter any premises to access, search and seize such data or information.

(2) A police officer or any person authorised by the Commissioner or by the Director, in writing, in the execution of an order issued under subsection (1), shall —

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

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

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

(*d*) print, photograph, copy or make in any other manner for the purpose of doing an act referred to in paragraph (*a*); and

(*e*) render inaccessible or remove the stored data or information from the computer or computer system, or any information and communication technology medium.

Real time collection of traffic data

24. A police officer or any person authorised by the Commissioner or by the Director, in writing, may apply to a judicial officer, *ex parte*, for an order —

(*a*) for the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer or computer system; or

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

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

(ii) assist the Police, to effect such collection and recording.

Deletion order

25. The Director of Public Prosecutions, or any person authorised by him or her, may apply to a judicial officer for an order that data in a computer or computer system or other information communication technology medium which contains pornography, obscene material or child pornography —

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

(*b*) be deleted or destroyed.

Acting without an order

26. A police officer of the rank of sergeant or above such rank may act without applying for an order under this Act if such application would result in an undue delay in the investigation of any offence under this Act.

Limited use of disclosed data and information

27. (1) Data obtained under this Act by a police officer, or any person authorised by the Commissioner or by the Director, in writing, shall be used for the purpose for which the data was originally sought, unless such data is sought —

(*a*) in accordance with any other enactment;

(*b*) in compliance with an order of court;

(*c*) in the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or

(*d*) in the public interest.

(2) Subject to subsection (3), on request, a police officer or any person authorised by the Commissioner or by the Director, in writing, shall permit a person who had the custody or control of a computer or computer system to access and copy computer data on the computer or computer system.

(3) A police officer or any person authorised by the Commissioner or by the Director, in writing, may refuse to give access to computer data or provide copies of such computer data if he or she has reasonable grounds for believing that giving access, or providing the copies —

(*a*) would constitute a criminal offence; or

(*b*) would prejudice —

(i) the investigation in connection with which the search was carried out; or

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Non-compliance with order or notice

28. A person who fails to comply with an order or notice issued under this Part commits an offence and shall on conviction be liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

PART IV — *Miscellaneous*

Extradition

29. An offence under this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

Cap. 09:03

Regulations

30. The Minister may make Regulations for the better carrying out of the provisions and purposes of this Act.

PASSED by the National Assembly this 3rd day of December, 2007.

E.S. MPOFU,
Clerk of the National Assembly.