OBJECTS AND REASONS

This Bill makes provision for the protection of computer systems and the information contained in those systems from

(a) unauthorised access by individuals;

(b) abuse by individuals with authorised access; and

(c) for related matters.

Arrangement of Sections

Section

Section

BARBADOS

A Bill entitled

An Act to make provision for the protection of computer systems and the information contained in those systems from *(a)* unauthorised access by individuals, *(b)* abuse by individuals with authorised access and *(c)* or related matters.

ENACTED by the Parliament of Barbados as follows:

PART I

Preliminary

Short title.

1. This Act may be cited as the *Computer Misuse Act, 2004*.

Interpretation.

2. (1) In this Act

"authorised person" means a person authorised in writing by the Commissioner of Police;

"computer" means

(a) an electronic, optical, electro-chemical, or a magnetic, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and

(b) any data storage facility or communications facility directly related to or operating in conjunction with that device or group of such interconnected or related devices, but excludes

(i) an automated typewriter or typesetter;

(ii) a portable hand held calculator;

(iii) a similar device which cannot be programmed or which does not contain any data storage facility; or

(iv) such other device as the Minister may, by Order, prescribe;

"computer output" or "output" means a statement or representation, whether in written, printed, pictorial, graphical acoustic or 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 services" includes computer time, data processing and the storage or retrieval of data;

"damage" includes, except for the purpose of section 15, any impairment to a computer or the integrity or availability of any data or program held in a computer, that

(a) causes aggregate loss of at least $5 000 in value, or such other amount as the Minister may, by Order, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(b) modifies or impairs, or potentially modifies or impairs, the medical examination diagnosis, treatment or care of a person; or

(c) threatens the public interest;

"data" means representation 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 capable of being used to intercept any function of a computer;

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

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

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

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing the computer to perform any function that person

(a) alters or erases the program or data**;**

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

(c) uses the program or data; or

(d) causes the program or data to be output from the computer in which that program or data is held, whether by having the program or data 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 read accordingly.

(3) For the purposes of section 2*(c)*, a person uses a program if the function he causes the computer to perform

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of section 2*(d)*, 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.

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or had without authority if

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

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

(6) A reference in this Act to any program or data held 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 or to any program or data held in any storage medium which is external to the computer but which is connected to it.

(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or of any other computer

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

(b) any program or data is added to any program or data held in the computer; or

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

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

(8) Any modification referred to in subsection (7) is unauthorised if the person whose act causes the modification

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

(b) has not obtained the consent of any person who is entitled to consent to the modification.

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

PART II

Offences

Unauthorised access to computer program or data.

3. (1) Subject to subsection (2), 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 summary conviction to a fine of $ 10 000 or to imprisonment for a term of 12 months or to both and, in the case of a second or subsequent conviction, to a fine of $20 000 or to imprisonment to a term of 2 years or to both.

(2) 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.

Access with intention to commit or facilitate commission of offence.

4. (1) A person who knowingly causes a computer to perform any function in order to secure access to any program or data held in that computer or in any other computer with the intention to commit an offence

(a) involving property, fraud, dishonesty or which causes bodily harm; and

(b) for which the sentence is fixed by law,

commits an offence and is liable on summary conviction to a fine of $20 000 or to imprisonment for a term of 2 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;

(b) the offence to which this section applies is

(i) committed at the same time when the access is secured or at any other time; and

(ii) punishable summarily or indictably.

Unauthorised modification of computer program or data.

5. (1) Subject to subsection (2), a person who, without authority, does an act which he knows will cause an unauthorised modification or copying of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of $10 000 or to imprisonment for a term of 12 months or to both and, in the case of a second or subsequent conviction, to a fine of $20 000 or to imprisonment for a term of 2 years or to both.

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

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

Unauthorised interception of computer service.

6. (1) Subject to subsection (2), 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 summary conviction to a fine of $10 000 or to imprisonment for a term of 12 months or to both and, in the case of a second or subsequent conviction, to a fine of $20 000 or to imprisonment for a term of 2 years or to both.

(2) For the purpose of this section, it is immaterial that the unauthorized 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.

7. 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,

commits an offence and is liable on summary conviction to a fine of $10 000 or to imprisonment of a term of 12 months or to both and, in the case of a second or subsequent conviction, to a fine of $20 000 or to imprisonment for a term of 2 years or to both.

Additional penalty and fine

8. If any damage is caused as a result of an offence committed under section 3(1), 5(1), 6(1) or 7(1), the person convicted of the offence is liable to an additional fine of $15 000 or to imprisonment for a term of 2 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 summary conviction to a fine of $10 000 or to imprisonment of a term of 12 months or to both and, in the case of a second or subsequent conviction, to a fine of $20 000 or to imprisonment for a term of 2years 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

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

(b) for an unlawful purpose; or

(c) knowing that it is likely to cause unlawful damage,

commits an offence and is liable on summary conviction to a fine of $10 000 or to imprisonment for a term of 12 months or to both and, in the case of a second or subsequent conviction, to a fine of $20 000 or to imprisonment for a term of 2 years or to both.

Enhanced punishment for offences involving protected computers.

10. (1) Where access to a protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of that offence is, in lieu of the penalty prescribed in those sections, liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 5 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 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 public key infrastructure; or

(d) 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 of access to computer program or data.

11. (1) A person who knowingly 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 from another person, whether or not he knows that that person has obtained that program or data through authorised or unauthorised means, commits an offence.

(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 that person has obtained that program or data through unauthorised means, commits an offence.

(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 he knows is not authorised to receive or have access to that program or data commits an offence.

(4) A person who has obtained any program or data held in a computer through unauthorised means and gives the program or data to another person whether or not he knows that that other person is authorised to receive or have access to that program or data commits an offence.

(5) A person who commits an offence under this section is liable on summary conviction to a fine of $50 000 or to imprisonment for a term of 2 years or to both.

Causing a computer to cease to function.

12. (1) A person who engages in conduct which causes a computer to cease to function permanently or temporarily and at the time of engaging in that conduct has

(a) knowledge that the conduct is unauthorised;

(b) the requisite knowledge; and

(c) the requisite intent,

commits an offence and is liable on summary conviction to a fine of $15 000 or to imprisonment for a term of 2 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.

Child pornography.

13. (1) A person who, intentionally, does any of the following acts:

(a) publishes child pornography through a computer system; or

(b) produces child pornography for the purpose of its publication through a computer system; or

(c) possesses child pornography in a computer system or on a computer data storage medium,

is guilty of an offence.

(2) A person who is convicted of an offence under subsection (1) is liable

(a) on conviction on indictment to imprisonment for a term of 5 years; or

(b) on summary conviction to a term of 2 years.

(3) For the purpose of subsection (1)

"child pornography" includes material that visually depicts

(a) a minor engaged in sexually explicit conduct; or

(b) a person who appears to be a minor engaged in sexually explicit conduct; or

(c) realistic images representing a minor engaged in sexually explicit conduct.

"publish" includes

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

(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 paragraph *(a)*.

.

PART III

Miscellaneous

Territorial scope of offences under this Act.

14. (1) Subject to subsection (2), this Act shall have effect in relation to any person, whatever his nationality or citizenship, outside as well as within Barbados, and where an offence under this Act is committed by a person in a place outside of Barbados; he may be dealt with as if the offence has been committed within Barbados.

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

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

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

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

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 him 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 that 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.

Saving for investigations by police officer.

16. Nothing in this Act shall prohibit a police officer or an "authorised person" from lawfully conducting investigations pursuant to any powers conferred under any written law other than this Act.

Power of police officer to access computer program and data.

17. (1) This section applies to a computer which a police officer or an authorised person has reasonable cause to suspect is or has been in use in connection with 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.

(2) 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.

(3) 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 28 days from the date of its issue.

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

(5) 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 had been disclosed in the course of the lawful exercise of the powers under this section;

(iv) make and take away a copy of any program 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 he 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 him with any reasonable technical and other assistance as he may require for the purpose of paragraph *(a)*, or

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

(6) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section commits an offence and is liable on summary conviction to a fine of $15 000 and to imprisonment for 2 years.

(7) For the purpose of this section

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted program or data from its unreadable 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;

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

Regulations.

18. The Minister may make Regulations generally for the purpose of giving effect to this Act.