THE COMPUTER MISUSE BILL, 2003

ARRANGEMENT OF CLAUSES

PART I
PRELIMINARY

PART II
OFFENCES

PART III

MISCELLANEOUS AND GENERAL

Session: 2002
Bill No. 25

Hon. Perry G. Christie
or a member of government
23 January, 2003

A BILL

for

AN ACT TO MAKE PROVISIONS SECURING COMPUTER MATERIAL AGAINST UNAUTHORISED ACCESS OR MODIFICATION AND FOR CONNECTED PURPOSES

Enacted by the Parliament of the Bahamas

PART I

PRELIMINARY

Short title and commencement.

1. (1) This Act may be cited as the Computer Misuse Act, 2003.

(2) This Act shall come into operation on such day as the Minister may, by notice published in the Gazette, appoint.

Interpretation.

2. (1) In this Act -

"computer" means an electronic, magnetic, optical, electrochemical, 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 interconnected or related devices, but does not include -

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

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

(d) such other device as the Minister may, by notice published in the Gazette, prescribe;

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

"damage" means, except for the purposes of section 12, any impairment to a computer or the integrity or availability of data, a program or system, or information, that -

(a) causes economic loss aggregating ten thousand dollars in value, or such other amount as the Minister may, by notice published in the Gazette, prescribe except that any such 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 one or more persons;

(c) causes or threatens physical injury or death to any person;

(d) threatens public health or public safety; or

(e) threatens physical damage to a computer;

"data" means representations of information or of concepts 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" , in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function; and a reference in this Act to a program includes a reference to part of a program.

(2) For the purposes of this Act, a person "secures access" to any program or data held in a computer if he causes a computer to perform any function in relation to such program or data, that -

(a) alters or erases it;

(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 in this Act to securing access or to an intent to secure such access shall be construed accordingly.

(3) For the purposes of subsection (2) (c), a person “uses” a program if the function he causes the computer to perform causes the program to be executed or is itself a function of the program.

(4) For the purposes of subsection (2) (d), the form in which any program or data is output is immaterial (including 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).

(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” if -

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

(b) he does not have consent to such access 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 such 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.

(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 any

other computer -

(a) any program or data held in the computer concerned 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 any computer;

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

(8) Any modification referred to in subsection (7) is 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.

PART II
OFFENCES

Unauthorised access to computer material.

3. (1) Subject to subsection (2), any person who, without authority, knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in any computer shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding six months or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding ten thousand or to imprisonment for a term not exceeding one year or to both such

fine and imprisonment.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(3) For the purposes 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 intent to commit or facilitate commission of offence.

4. (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence (whether by himself or by any other person) to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years.

(3) Any person guilty of an offence under this section shall be liable on summary conviction, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) For the purposes 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 committed at the same time when the access is secured or at any other time.

Unauthorised modification of computer material.

5. (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(3) For the purposes 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.

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

Unauthorised use or inter-ception of computer service.

6. (1) Subject to subsection (2), any person who knowingly –

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

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

shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.

(3) For the purposes 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.

7. (1) Any person who, knowingly and without authority or lawful excuse -

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

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

shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.

Unauthorised disclosure of access code.

8. (1) Any 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 any computer shall be guilty of an offence if he did so -

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.

Enhanced punishment

9. (1) Where access to any protected computer is obtained in the course of the commission of an offence under

for offences involving protected computers.

section 3, 5, 6 or 7, the person shall be tried on information and shall be liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding twenty years or to both such fine and imprisonment.

(2) For the purposes 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 or program or data is used directly in connection with or necessary for -

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

(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 including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes 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, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

Incitement, abetments and attempts punishable as full offences.

10. (1) Any person who incites, solicits or abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on summary conviction to the punishment provided for the full offence.

(2) For an offence to be committed under this section, it is immaterial where the full offence in question took place.

PART III
MISCELLANEOUS AND GENERAL

Territorial scope of offences under this Act.
Ch.77.

11. (1) This section has effect to supplement the provisions of the Penal Code in relation to the jurisdiction of the courts of The Bahamas to try offences which do not take place wholly in The Bahamas.

(2) Subject to subsection (3) the provisions of the Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within The Bahamas.

(3) Where an offence under this Act is committed by any person in any place outside The Bahamas, he may be dealt with as if the offence had been committed within The Bahamas.

(4) For the purposes of this section, this Act shall apply if, for the offence in question.

(a) the accused was in The Bahamas at the material time; or

(b) the computer, program or data was in The Bahamas at the material time.

Commencement

12. (1) Notwithstanding any Act to the contrary

of proceedings.

prescribing the time limit within which summary proceedings may be commenced and subject to subsection (2), proceedings for an offence under this Act may be brought within a period of twelve months from the date on which evidence sufficient in the opinion of the Attorney-General to warrant prosecutions came to his knowledge.

(2) No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence.

(3) For the purposes of this section, a certificate signed by or on behalf of the Attorney General and stating the date on which evidence sufficient in his opinion to warrant the commencement of proceedings came to his knowledge shall be conclusive evidence of that fact.

Order for payment of compensation.

13. (1) The court before which a person is convicted of any offence under this Act may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his computer, program or data by the offence for which the sentence is passed.

(2) Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him 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 of compensation under this section shall be recoverable as a civil debt.

Saving for investigations.

14. Nothing in this Act shall prohibit a police officer, a person authorised in writing by the Commissioner of Police under section 16(1) or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to his powers conferred under any

written law.

Police powers.

15. (1) A police officer may arrest without warrant any person who has committed or is committing, or whom the police officer with reasonable cause suspects to have committed, or to be committing, an offence under this Act.

(2) Any power of seizure conferred on a police officer who has entered premises by virtue of a warrant issued under section 66 of the Criminal Procedure Code in relation to an offence under this Act, or any related inchoate offence, shall be construed as including a power to require any information relating to the warrant which is held in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is legible (whether or not with the use of a computer).

(3) Where the items seized by a police officer under section 66 of the Criminal Procedure Code include computers, disks or other computer equipment, the magistrate before whom those items are brought in accordance with section 68 of the Criminal Procedure Code may, on the application of the person to whom those items belong or from under whose control they were taken, and subject to subsection (4), make an order -

(a) permitting a police officer to make copies of such programs or data held in the computer, disks or other equipment as may be required for the investigation or prosecution of the offence;

(b) requiring copies of those copies to be given to any person charged in relation to the offence ("the accused person"); and

(c) requiring the items to be returned within a period of seventy-two hours,

and when seizing any such items the police officer shall inform the person to whom those items belong or from under whose control they are taken of his right to make an application under this subsection.

(4) Subsection (3) (b) shall not apply -

(a) in relation to copies of any items returned to the accused person; or

(b) where the court is satisfied that -

(i) the provision of copies would substantially prejudice the investigation or prosecution, or

(ii) owing to the confidential nature of the information obtained from the computers, disks or other equipment, the harm which may be caused to the business or other interests of the applicant or any third party by giving copies of that information to the accused person outweighs any prejudice which may be caused by not so doing.

(5) Any copies made pursuant to subsection (2) or (3) shall, for the purposes of admissibility in any proceedings, be treated as if they were themselves the items seized.

Power of police officer to access computer

16. (1) A police officer or a person authorised in writing by the Commissioner of Police, pursuant to a warrant under section 66 of the Criminal Procedure Code, shall -

(a) be entitled at any time to -

(i) have access to and inspect and

and data.

check the operation of any computer to which this section applies,

(ii) use or cause to be used any such computer to search any data contained in or available to such computer, or

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained 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;

(b) be entitled to require -

(i) the person by whom or on whose behalf, the police officer or investigation 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 such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or

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

(2) This section shall apply to a computer which a police officer or a person authorised in writing by the Commissioner of Police 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.

(3) The powers referred to in paragraphs (a) (ii) and (iii) and (c) of subsection (1) shall not be exercised except with the consent of the Attorney-General.

(4) Any person who obstructs the lawful exercise of the powers under subsection (1) (a) or who fails to comply with a request under subsection (1) (b) or (c) shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.

(5) For the purposes of this section -

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

"encrypted data" means 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 data occurs or can be found for the purposes of protecting the content of such data;

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

Forfeiture.

17. (1) Where a person is convicted of an offence under this Act, or any related inchoate offence, and the court is satisfied that any property which was in his possession or under his control at the time he was apprehended for the offence or when a summons in respect of it was issued -

(a) has been used for the purpose of committing, or facilitating the commission of, the offence in question or any other such offence; or

(b) was intended by him to be used for that purpose,

the court may order that property to be forfeited to the Crown, and may do so whether or not it deals with the offender in respect of the offence in any other way.

(2) In considering whether to make an order in respect of any property the court shall have regard -

(a) to the value of the property; and

(b) to the likely financial and other effects on the offender of the making of the order (taken together with any other order the court contemplates making).

OBJECTS AND REASONS

This Bill seeks to make provision for securing computers and computer material against unauthorised access, modification and interference. The aim is to enforce observance of computer security by imposing stringent penalties for specified computer related offences. The Bill also provides for enhanced penalties where the offence results in damage, which includes financial loss, injury, or harm.

Clause 1 provides for the short title and commencement provisions of the Act.

Clause 2 provides the interpretation provision.

Clause 3 makes it an offence for a person to cause a computer to perform any function with intent to secure unauthorised access to any program or data held in a computer. The offence is punishable with a fine and/or imprisonment. An increased penalty would be imposed where that unauthorised access results in sustained damage above the prescribed limit.

Clause 4 makes it an offence for a person to access a computer with the intention of committing an offence. The offence is punishable with a fine and/or imprisonment.

Clause 5 makes it an offence for a person to do any act which causes an unauthorised modification of the contents of any computer. The offence is punishable with a fine and/or imprisonment. There is an enhanced penalty where damage above the prescribed limit results from the modification.

Clause 6 makes it an offence to secure unauthorised access to any computer for the purpose of obtaining computer services, or to intercept without authority

any function of a computer, or uses any device for the purpose of an unauthorised access to obtain a computer service or to intercept a computer function. Where damage above the prescribed limit results from such activity there is an enhanced penalty.

Clause 7 makes it an offence knowingly and without authority or lawful excuse to interfere with the lawful use of a computer or impair in any way the usefulness of any program or data stored on a computer. An enhanced penalty is imposed where damage above the prescribed limit results from the interference or impairment.

Clause 8 creates an offence of knowingly and without authorisation disclosing any means of gaining access to any program or data held on a computer for any wrongful gain, unlawful purpose or knowing that it is likely to cause wrongful loss to any person.

Clause 9 makes an offence indictable if an offence committed under sections 3,5,6 or 7 involved access to a protected computer. A protected computer is one which the person knew or ought to have known was used for specified purposes including national security, law enforcement purposes, the provision of public services, banking and financial services, communications infrastructure, public key infrastructure, transportation and public safety.

Clause 10 provides that conspiracy, attempt, incitement, aiding and abetting or any other act preparatory to or in furtherance of the commission of any offence under the Act should be punishable on conviction with the same penalty provided for the offence.

Clause 11 provides for the territorial scope of offences under the Act, which subjects the offender to this jurisdiction whether he is a citizen or not, provided that he or the computer, program or data was in The Bahamas at the

material time.

Clause 12 provides that the proceedings for offences under the Act can be brought within twelve (12) months from the date on which the Attorney General certifies that sufficient evidence has come to his attention to warrant prosecution of an offence. The time limit for bringing such prosecution is three years.

Clause 13 allows the court to make an order for payment of compensation by an offender to any person for any damage caused to that person's computer. This order does not prevent that person bringing any other proceedings for damages at common law.

Clause 14 preserves the power of a police officer to conduct investigations as permitted under any written law.

Clause 15 would allow a Magistrate to issue a search warrant to a police officer, who, upon executing it, may seize any article, data, document or information if he believes it is evidence that an offence has been committed. This clause would also allow a police office to have access to any computer, or program or data held in any computer and to require any person concerned to assist him in his investigations, including giving him access codes. However, in certain circumstances, these powers cannot be exercised except with the consent of the Attorney-General.

Clause 16 empowers the police or any person authorised by the Commissioner of Police, pursuant to a Magistrate's warrant to access computer and data, where there is reasonable cause to suspect that a computer is, or has been in use in connection with any offence under the Bill or any other offence which has been disclosed in the course of the lawful exercise of the powers of the police under this clause.

Clause 17 provides the court with discretion to

forfeit any items seized if the person is found guilty of the offence.