ANTIGUA AND BARBUDA

THE COMPUTER MISUSE ACT, 2006

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

PART II

OFFENCES

PART III

PROCEDURAL POWERS

ANTIGUA AND BARBUDA

THE COMPUTER MISUSE ACT, 2006

NO. OF 2006

A BILL FOR

AN ACT to prohibit the unauthorised access, use of or interference to any program or data held in a computer and to a computer itself and to facilitate the gathering and use of electronic evidence

ENACTED by the Parliament of Antigua and Barbuda as follows:

Part 1 Preliminary

1. This Act may be cited as the Computer Misuse Act, 2006. Short title

2. (1) In this Act- Interpretation

"computer" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program or electronic instructions, performs automatic processing of data or any other function but does not include-

(a) a portable hand held calculator;

(b) an automated typewriter or typesetter;

(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 prescribe by Order.

"computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions commonly called viruses or worms which are self-replicating or self-propagating and which are designed to contaminate other computer programs or computer data; consume computer resources;

modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network;

"computer network" means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities;

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

(a) produced by a computer; or

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

"computer service" includes, but are not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.;

“computer system” means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files;

"damage", except for the purposes of section 18, includes any impairment to a computer or the integrity or availability of any program or data held in a computer that -

(a) causes loss aggregating at least five thousand dollars in value, or such other larger amount as the Minister may prescribe by Order, except that any loss incurred or accrued more than one year after the date of the loss 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;

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

(a) threatens the public interest;

"data" means any representation of facts, information or concepts in a form suitable for processing in a computer, including a program suitable to cause a computer to perform a function;

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

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

Minister means the minister in charge of telecommunications;

"program or computer program" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(2) 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 done without authority 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 access the kind of program or data in question from the person who is entitled to control access.

(3) A reference in this Act to a 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; and a computer is to be regarded as containing any program or data held in any such medium.

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

(5) For the purposes of this Act -

(a) a program or data held in a computer or in any storage medium capable of being accessed and printed into readable form through a computer is a document; and
(b) it is immaterial that access to a program or data held in a computer is achieved through the use of that or any other computer or by any other means.

Part II - Offences

Unauthorised access to computer program or data

3. (1) A person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

(2) For the purposes of this section, it is not material 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.

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

(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner,

and references to access to a program or data and to an intent to secure such access shall be read accordingly.

(4) For the purposes of subsection (3)(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.

(5) For the purposes of subsection (3)(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.

4. (1) A person who knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer with intent to commit an offence -

Access with intent to commit or facilitate commission of offence

(a) involving property, fraud, dishonesty or which causes bodily harm; and
(b) which is punishable on conviction with imprisonment for more than one year, or

commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both.

(2) For the purposes of this section, it is not material whether -

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

(b) the offence to which subsection (1) applies is-

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

(ii) punishable summarily or indictably.

5. (1) Subject to subsection (2), a person who does a direct or an indirect act without authority which he knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

Unauthorised modification of computer program or data

(2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of thirty thousand dollars and to imprisonment for three years or to both.

(3) For the purposes of this section -

(a) it is not material that the act in question is not directed at -

(i) any particular program or data;

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

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

(b) it is not material whether an unauthorised modification is, or is intended to be, permanent or merely temporary;

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

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

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

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

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

(4) Any modification referred to in this section 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 the person who is so entitled.

Unauthorised use or 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 fifteen thousand dollars and to imprisonment for two years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

(2) If any damage is caused as a result of an offence under subsection (1), a person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years or to both.

(3) For the purposes of this section, it is not material 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 or use of computer

7. (1) Subject to subsection (2), 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 fifteen thousand dollars and to imprisonment for two years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

(2) If any damage is caused as a result of an offence committed under subsection (1) the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for three years or to both.

Unauthorised disclosure of access code

8. (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 if he did so -

(a) for any unlawful gain, whether to himself or to another person;
(b) for any unlawful purpose; or
(c) knowing that it is likely to cause unlawful damage,

is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for three years or to both and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for three years or to both.

Punishment for offences involving protected computers

9. (1) Where access to any protected computers is obtained in the course of the commission of an offence under sections 3, 5, 6 or 7 the person convicted of such an offence shall, in lieu of the penalty prescribed in those sections, be liable on conviction on indictment to a fine of twenty thousand dollars and to imprisonment for ten years or to both.

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

Unauthorised receiving or giving access to computer program or data

10. (1) A person who receives or is given access to any program or data held in a computer who is not authorised to receive or have access to that program or data, from another person and he knows that that person has obtained that program or data through authorised or unauthorised means commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both.

(2) 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 and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for two years or to both.

Causing a computer to cease to function

11. (1) A person who engages in conduct, including in introducing any computer contaminant into any computer, computer system, or computer network, which causes a computer or such system or network to cease to function permanently or temporarily and at the time he engages in that conduct he 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 fifty thousand dollars and to imprisonment for ten years or to both.

(2) For the purposes 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) impairs the operation of the computer,

but the intent need not be directed at a particular computer, computer system, or computer network.

Denial of service attacks

12..(1) A person who without authorization does any act-

(a) which causes; or

(b) which he intends to cause,

directly or indirectly, a degradation, failure, or other impairment of function of a computer, program, computer system, computer network or any part thereof commits an offence and is liable on summary conviction to a fine of fifty thousand dollars and to imprisonment for ten years or to both.

(2) A person is guilty of an offence in subsection (1)(a) even if the act was not intended to cause a effect, provided that a reasonable person could have anticipated that the act would have caused the effect.

(3) For the purposes of subsection (1) , the act is without authorisation if the person doing it-

(a) is not the owner of the relevant computer, program, computer system, computer network or part thereof; or

(b) does not have the permission of the owner.

13.(1) A person commits an offence if the person- Illegal devices

(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available-

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against sections 3 to 9 or 12; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence against sections 3 to 9 or 12; or

(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against sections 3 to 9 or 12.

(2) A person found guilty of an offence against this section is liable on conviction to a fine of fifty thousand dollars and to imprisonment for ten years or to both.

(3) Where a person possesses more than five item(s) mentioned in subparagraph (i) or (ii), a court may, having regard to all the circumstances, infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against sections 3 to 9 or 12.

14. A person who uses a computer or knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer with intent to impersonate another person or steal or impersonate their identity commits an offence and is liable on conviction to a fine of fifty thousand dollars and to imprisonment for three years or to both. Identity theft

15.(1)A person who, intentionally, does any of the following acts- Child pornography

(a) publishes child pornography through a computer; 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;

commits an offence punishable on conviction to a fine of two hundred and fifty thousand dollars and to imprisonment for ten years or to both.

(2) It is a defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose.

(3) In this section-

"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.

"minor" means a person under the age of 16 years.

"publish" includes-

(a) 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; or
(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 –Procedural Powers

Definitions for this Part

16. In this Part-

"thing" includes-
(a) a computer or part of a computer; and
(b) another computer, if-
  (i) computer data from that computer s is available to the first computer being searched; and
  (ii) there are reasonable grounds for believing that the data sought is stored in the other computer; and

(c) a computer data storage medium

"seize" includes-
(a) make and retain a copy of data, including by using on-site equipment; and
(b) render inaccessible, or remove, r data in the accessed computer; and
(c) take a printout of output of computer data.

Territorial scope of offence under this Act

17. (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 Antigua and Barbuda; and where an offence under this Act is committed by a person in any place outside of Antigua and Barbuda, he may be dealt with as if the offence had been committed within Antigua and Barbuda.

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

(a) the accused was in Antigua and Barbuda at the material time;
(b) the computer, program or data was in Antigua and Barbuda at the material time; or
(c) the damage occurred within Antigua and Barbuda, whether or not paragraph (a) or (b) applies.

Jurisdiction of court

18. (1) A High Court shall have jurisdiction to hear and determine all offences committed under this Act.

(2) A summary court shall have jurisdiction to hear and determine any offence, except under sections 9, 11, 12, 13 and 15 and 29, if-

(a) the accused was within the magisterial district at the time when he committed the offence;

(b)any computer containing any program or data which the accused used was within the magisterial district at the time when he committed the offence; or

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

Order for payment of compensation

19. (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 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 for compensation under this section shall be recoverable as a civil debt.

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

Savings for investigations by police officer

20. Nothing in this Act prohibits a police officer or a person authorised in writing by the Commissioner of Police ("authorised person") from lawfully conducting investigations pursuant to any powers conferred under any written law.

Power of police officer to access computer program and data

21. (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 used 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, he 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 twenty-eight 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 has been disclosed in the course of the lawful exercise of the powers under this section;

(iv) to 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 or any authorised person with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); and

(c) entitled to require 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 fifteen thousand dollars and to imprisonment for two years or to both.

(7) For the purposes of this section -

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted program or data from its 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 utilized for such

transformation or scrambling and irrespective of the medium in which such program or data occur or can be found for the purposes 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.

Record of and access to seized data

22.(1) If a computer or data has been removed or rendered inaccessible, following a search or a seizure under section 21 the person who made the search must, at the time of the search or as soon as practicable after the search-

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and
(b) give a copy of that list to-
(i) the occupier of the premises; or
(ii)the person in control of the computer .

(2) Subject to subsection (3), on request, a police officer or another authorized person must-

(a) permit a person who had the custody or control of the computer or someone acting on their behalf to access and copy data on the computer;
(b) give the person a copy of the computer data.

(3) The police officer or another authorized person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the 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.

Production of data

23. If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that-

(a) a person in the territory of Antigua and Barbuda in control of a computer produce from the computer specified data or a

printout or other intelligible output of that data;

(b) an Internet service provider in Antigua and Barbuda produce information about persons who subscribe to or otherwise use the service; or

(c) a person in the territory of Antigua and Barbuda who has access to a specified computer process and compile specified computer data from the computer and give it to a specified person.

Disclosure of stored traffic data

24. If a magistrate is satisfied on the basis of an ex parte application by a police officer that specified data stored in a computer is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer disclose sufficient traffic data about a specified communication to identify-

(a) the service providers; and
(b) the path through which the communication was transmitted.

Preservation of data

25.(1)If a police officer is satisfied that-

(a) data stored in a computer is reasonably required for the purposes of a criminal investigation; and
(b) there is a risk that the data may be destroyed or rendered inaccessible;

the police officer may, by written notice given to a person in control of the computer , require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

(2) The period may be extended beyond 7 days if, on an ex parte application, a judge authorizes an extension for a further specified period of time.

Interception of electronic communications

26. If a judge is satisfied on the basis of information on affidavit that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judge may-

(a) order an Internet service provider whose service is available in Antigua and Barbuda through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer ; or

(b) authorize a police officer to collect or record that data through application of technical means.

Interception of traffic data

27. If a judge is satisfied on the basis of information on affidavit there are reasonable grounds believe that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate may authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Evidence

28. In proceedings for an offence against a law of Antigua and Barbuda, the fact that-

(a) it is alleged that an offence of interfering with a computer has been committed; and

(b) evidence has been generated from that computer ;

does not of itself prevent that evidence from being admitted.

Confidentiality and limitation of liability

29. (1) An Internet service provider who without lawful authority discloses-

(a) the fact that an order under sections 21 and 23 to 27 has made; or

(b) anything done under the order; or

(c) any data collected or recorded under the order;

commits an offence and is liable on conviction to a fine of fifty thousand dollars.

(2) An Internet service provider is not liable under a civil or criminal law of Antigua and Barbuda for the disclosure of any data or other information that he discloses under sections 21 to 27.

Limitation period

30. (1) Notwithstanding any other written law, a person who commits an offence under this Act, except an offence under sections 9, 11, 12, 14 or 15, may be prosecuted at any time within forty eight months after the commission of the offence.

(2) A person who commits an offence under sections 9, 11, 12, 14 or 15 may be prosecuted at any time within six years after the commission of the offence.

Passed by the House of Representatives
this day of 2006.

Speaker

Passed by the Senate
this day of 2006.

President

MEMORANDUM

This Act is divided into three parts.

Part I provides for the short title and definitions.

Part II would provide for various computer related offences.

Part III would provide for the necessary procedural powers.

Clause 3 would make it a summary offence for a person knowingly to have unauthorised access to any program or data held in a computer, and an increased penalty would be imposed where that unauthorised access causes damage.

Clause 4 would make it a summary offence for a person, with or without authority, to access a computer program or data with intent to commit or facilitate the commission of a specified category of offences. It also makes it an offence to use a computer or access a program or data to steal someone's identity or impersonate someone.

Clause 5 would make it a summary offence if a person does an act, whether temporary or permanent, which he knows shall cause an unauthorised modification of any program or data held in a computer and where such an act result in damage, an increased penalty would be imposed.

Clause 6 would make it a summary offence for a person knowingly to use any computer service or intercept a computer function without authority and where the use or interception result in damage, an increased penalty would be imposed.

Clause 7 would make it a summary offence for a person knowingly to interfere with, impede or obstruct the use of a computer or impede access to any program or data held in a computer and where such obstruction result in damage, an increased penalty would be imposed.

Clause 8 would make it a summary offence for a person, knowingly and without authority, to disclose any access code of a computer if the disclosure results in any wrongful gain or damage or is used for an unlawful purpose.

Clause 9 would make it an indictable offence 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 national security, law enforcement purposes, the provision of numerous public services, or the protection of the public interest.

Clause 10 would make it a summary offence for a person to knowingly receive or give access to any program or data held in a computer without authority.

Clause 11 would make it a summary offence for a person to cause a computer to cease to function permanently or temporarily.

Clause 12 would denial of service attacks an offence**.**

Clause 13 would make it an offence for a person to produces, sells, procures for use, imports, exports, distributes or otherwise makes available a device, including a computer program, that is designed or adapted for the purpose of committing an offence against sections 3 to 9 or 12; or a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence against sections , 3 to 9 or 12.

Clause 14 would make identity theft an offence.

Clause 15 would provide for the prohibition of use of a computer to publish child pornography. Other matters such as obscenity are already covered under Antigua and Barbuda law, therefore repetitive and conflicting provisions are not to be introduced.

PART III would provide for certain general and procedural provisions.

Clause 16 would provide for the definitions for this Part.

Clause 17 would provide for the territorial scope of offences under this Act, for which this is the Bill, whether the offender is a citizen or not, provided, however, that he or the computer was in Antigua and Barbuda at the material time, or damage occurred within Antigua and Barbuda whether or not he or the computer was within Antigua and Barbuda at the material time.

Clause 18 would provide the high court with jurisdiction to try any offence committed under this Act but would restrict the jurisdiction of a summary court to offences committed by a person within the magisterial district or where damage occurred within such a district, whether the person or computer was within the district.

Clause 19 would allow the court to make an order for payment of compensation by the offender to any person for any damage caused to that person's computer or any program or data held in his computer, and this order will not prevent that person from bringing any other proceedings for damages at common law.

Clause 20 would preserve the power of a police office to conduct investigations as permitted under any written law.

Clause 21 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.

Clause 22 would require the police to make a record of and allow access to seized data.

Clause 23 would provide for a magistrate to be able to order production of data required for the purpose of a criminal investigation or criminal proceedings.

Clause 24 would allow a magistrate to authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means where there are reasonable grounds to suspect that traffic data is reasonably required for the purposes of a criminal investigation.

Clause 25 would provide for the preservation of data where data stored in a computer system is reasonably required for the purposes of a criminal investigation; and where there is a risk that the data may be destroyed or rendered inaccessible.

Clauses 26 and 27 would provide that a judge can order an internet service provider to intercept electronic communications and data traffic where necessary for criminal investigations.

Clause 28 would make provisions for evidence.

Clause 29 would make provisions with respect to confidentiality and limitation of liability of internet service providers.

Clause 30 would provide that a person can be prosecuted for an offence, except an offence under section 9, 11, 12, 14 or 15 within two years from the date the offence was committed. A person can be prosecuted for an offence under sections 9, 11, 12, 14 or 15 within six years from the date the offence was committed