ARRANGEMENT OF SECTIONS

Section

I assent,

(LS)

CUTHBERT M SEBASTIAN

Governor-General.

26th November, 2009.

SAINT CHRISTOPHER AND NEVIS

No. 27 of 2009

AN ACT to prohibit unauthorised access to and abuse of computers, computer systems as well as the information contained on those systems and for related matters.

[*Published 26th November 2009, Official Gazette No. 53 of 2009.*]

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the National Assembly of Saint Christopher and Nevis and by the authority of the same as follows:

Part I
Preliminary

1. This Act may be cited as the Electronic Crimes Act, 2009. Short title.

2. (1) In this Act, unless the contrary intention appears: Interpretation.

"Chief of Police" means the Commissioner of Police appointed pursuant to section 11 of the Police Act, 2003.

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

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

"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 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 but the term does not include calculators that are not programmable or are incapable of being used in conjunction with external files;

"damage" includes any impairment to a computer system, the integrity or availability of any data or program held in a computer system or of the confidentiality of information held in a computer system;

"device" includes any electronic, electro-magnetic, acoustic or mechanical equipment or apparatus that is used or capable of being used to intercept any function of a computer;

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

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

"seize" includes

(a) the making and retaining a copy of computer data, including by using on-site equipment;

(b) rendering inaccessible, or removing computer data from the accessed computer system; and

(c) taking a printout of output of computer data.

"service provider" means

(a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; or

(b) any other entity that processes or stores computer data on behalf of that entity or those users;

"storage medium" means any type of any device or material on which data can be electronically placed, kept, and retrieved.

"traffic data" means computer data that

(a) relates to a communication by means of a computer system;

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

(c) shows the origin, destination, route, time, date, size, duration of the communication or the type of underlying services used to generate the data.

(2) In this Act, access of any kind by a person to any program or data held in a computer is "unauthorised" or "obtained" without authority if the person is not entitled to access of the kind in question to the particular program or data.

(3) A reference in this Act to any "program" or "data" held in a computer includes a reference to

(a) any program or data held in any removable storage medium which is for the time being in the computer; or

(b) any program or data held in any storage medium which is external to the computer, but which is connected to it.

(4) In this Act, a "modification of the contents of any computer" occurs 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 existing program or data held in the computer; or

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

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

(5) Any modification referred to in subsection (4) 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 the person who is entitled to consent to the modification.

Jurisdiction.

3. This Act applies to an act done or an omission made:

(a) in or outside of Saint Christopher and Nevis; or

(b) on a ship or aircraft registered in Saint Christopher and Nevis.

PART II
OFFENCES

Illegal access.

4. (1) A person who, without lawful excuse or justification, knowingly gains access to the whole or any part of a computer system and thereby causes a computer to perform any function, but particularly,

(a) causes a program to be executed;

(b) uses a program to gain access to any data;

(c) copies or moves the program or data

(i) to any storage medium other than that in which that program or data is held; or

(ii) to a different location in the storage medium in which the program or data is held; or

(d) alters or erases the program or data

commits an offence and shall be liable, on summary conviction, to a fine of five thousand dollars or to imprisonment for a term of one year in the case of a first conviction and in the case of a second or subsequent conviction to a fine of ten thousand dollars or to imprisonment for a term of two years or to both such fine and imprisonment.

(2) If any damage results from an offence committed under this section, notwithstanding the penalties referred to in subsection (1), a person convicted of that offence shall be liable to a fine of twenty thousand dollars or to imprisonment for a term of three years or to both such fine and imprisonment.

(3) For the purposes of subsection (1), the form in which any program is obtained or copied and, in particular, whether or not it represents a form in which it is capable of being executed, is immaterial.

Interfering with data.

5. (1) A person who, knowingly and without lawful excuse or justification, does any of the following acts:

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data;

(d) obstructs, interrupts or interferes with any person in the lawful use of data;

(e) denies access to data to any person entitled to it;

commits an offence and is liable upon conviction on indictment to a fine of one hundred thousand dollars, or to imprisonment for a term of seven years or to both such fine and imprisonment.

(2) The provisions of subsection (1) are applicable whether the person's act is of temporary or permanent effect.

Interfering with computer. system.

6. (1) A person who, knowingly and without lawful excuse or justification:

(a) impairs the functioning of a computer system by

(i) preventing the supply of electricity to a computer system;

(ii) causing electromagnetic interference to a computer system;

(iii) corrupting the computer system by any means;

(iv) adding, deleting or altering computer data;

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

commits an offence and is liable on conviction on indictment, to a fine of fifty thousand dollars or to imprisonment for a term of five years or both such fine and imprisonment.

(2) The provisions of subsection (1) shall be applicable whether the person's act is of temporary or permanent effect.

Illegal interception.

7. A person who, knowingly and without lawful excuse or justification, intercepts by technical means:

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

(b) electromagnetic emissions that are carrying computer data from a computer system;

commits an offence and is liable on conviction on indictment, to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment.

Illegal devices.

8. (1) A person who knowingly and without lawful excuse or justification

(a) supplies, 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 4, 5, 6, or 7; 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 4, 5, 6, or 7; or

(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession

commits an offence and is liable on conviction on indictment to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment.

Unlawful access.

9. A person who knowingly uses 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 involving property, fraud or dishonesty commits an offence and is liable on conviction on indictment to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment.

Unlawful disclosure of access code.

10. (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 ten thousand dollars or to imprisonment for a term of twelve months or to both such fine and imprisonment, and in the case of a second or subsequent conviction, to a fine of twenty thousand dollars or to imprisonment for a term of two years or to both such fine and imprisonment.

(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 conviction on indictment to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine of one hundred thousand dollars or to imprisonment for a term of seven years or to both such fine and imprisonment.

Unauthorised access to restricted computer system.

11. (1) Where a person who does not possess the relevant authorisation for gaining access to a restricted computer system

(a) gains access to the system, that person commits an offence and is liable on conviction on indictment to a fine of seventy-five thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment;

(b) gains access to a restricted computer system in the course of the commission of an offence under section 4, 5, 6 or 7, the person convicted of that offence is, in lieu of the penalty prescribed in those sections, is liable, on conviction on indictment, to a fine of one hundred thousand dollars or to imprisonment for a term of seven years or to both such fine and imprisonment.

(2) For the purposes of subsection (1), a "restricted computer system" shall be treated as such 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 St. Christopher and Nevis;

(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;

(d) the protection of public safety and public health, including systems related to essential emergency services such as police, civil defence and medical services;

(e) any other service so designated by the Minister by Order to be restricted.

(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 access to computer program or data.

12. (1) Where a person who is not authorised

(a) to have a program or computer data; or

(b) to have access to any program or data held in a computer,

has in his custody or control any program or computer data or other information which is held in any computer or retrieved from any computer, with the intent to commit an offence, the person shall be deemed to have committed the offence of unlawfully obtaining access to a program or computer data unless the contrary is proved.

(2) A person who commits an offence under this section is liable on conviction on indictment to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment.

Child pornography.

13. (1) A person who knowingly:

(a) publishes child pornography through a computer system;

(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 for the purpose of publication

commits an offence and is liable on conviction on indictment

(a) in the case of an individual, to a fine of fifty thousand dollars or to imprisonment for a term of five years or to both such fine and imprisonment;

(b) in the case of a corporation, to a fine of two hundred and fifty thousand dollars.

(2) The provisions of subsection (1) paragraph (a) or (c) shall not be applicable to a person who establishes that the child pornography was for 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;

"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).

Unlawful communications.

14. (1) Where a person without lawful excuse or justification knowingly uses a computer system to send a message, letter, or electronic communication that

(a) is obscene,

(b) constitutes a threat; or

(c) is menacing in character,

to a recipient and intends to cause the recipient or any other person who is the subject of that message or letter or electronic communication to feel intimidated, molested, harassed or threatened, he commits an offence and is liable on summary conviction to a fine of ten thousand dollars or to imprisonment for a term of twelve months or to both such fine and imprisonment.

(2) Where a person without lawful excuse or justification publishes the message, letter or electronic communication referred to in subsection (1), to any other person not being a person who is the subject of the message, letter or electronic communication, then that first person commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars or to imprisonment for a term of two years or to both such fine and imprisonment.

PART III
PROCEDURAL POWERS

Warrant.

15. (1) Where a magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting 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.

(2) A warrant issued under this section may authorise or require

(a) a police officer to

(i) 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;

(ii) have access to and inspect and check the operation of any computer to which this section applies;

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

(iv) have access to any information, code or technology which has the capability of converting 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) an authorised person to render assistance to the police officer in the execution of the warrant.

(c) any person in possession of decryption information necessary to decrypt data required for the purpose of investigating any such offence.

(3) A police officer executing a warrant in accordance with this section shall be entitled to require a person who is in possession or control of a computer data storage medium or computer system that is the subject of the search to assist him or an authorised person to

(a) access and use a computer system or storage medium to search any computer data available to or in the system;

(b) obtain and copy computer data referred to in paragraph (a);

(c) use equipment to make copies;

(d) obtain access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence; and

(e) obtain an intelligible output from a computer system in a plain text format that can be read by a person.

(4) Any person who obstructs the lawful exercise of the powers under subsection (2) (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 conviction to a fine of ten thousand dollars or to imprisonment for a term of 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 convert encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been converted scrambled or transformed, from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilized for such conversion 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 converted transformed or scrambled, to an unreadable or incomprehensible format.

(6) For the purposes of this Part "authorised person" means a person who has the relevant training and skill in computer systems and who is authorised in writing by the Chief of Police.

Order for production of data.

16. If a magistrate is satisfied on the basis of an ex parte application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that

(a) a person in St. Christopher and Nevis in control of a computer system, produce from the system specified computer data or a printout or other intelligible output of that data; and

(b) an Internet service provider in St. Christopher and Nevis produce information about persons who subscribe to or otherwise use the service;

Record of and access to seized data.

17. (1) If a computer system or computer data has been removed or rendered inaccessible, following a search or a seizure under section 15, the person who made the search shall, 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 system.

(2) Subject to subsection (3), on request, a police officer or another authorised person shall:

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

(b) give the person a copy of the computer data.

(3) The police officer or another authorised 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.

Traffic data.

18. If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system 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 system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

(b) the path through which the communication was transmitted.

Interception of electronic communications.

19. (1) If a magistrate is satisfied on the basis of an information on oath that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation or criminal proceedings, the magistrate may:

(a) order an internet service provider whose service is available in St. Christopher and Nevis, 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 system; or

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

(2) An internet service provider who without lawful authority discloses

(a) the fact that an order under subsection (1), or sections 15 to 18 has been 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.

(3) An internet service provider is not liable under a civil or criminal law of St. Christopher and Nevis for the disclosure of any data or other information that he discloses under this section or sections 15 to 18.

Evidence.

20. Notwithstanding the provisions of any Act to the contrary, any electronic evidence that is collected pursuant to this Act shall be treated in the same manner as evidence that is non-electronic.

Arrest without warrant.

21. A police officer may arrest without warrant any person reasonably suspected of committing an offence under this Act.

PATRICE NISBETT
Deputy Speaker

Passed by the National Assembly this 21st day of October, 2009.

JOSÉ LLOYD
Clerk of the National Assembly

GOVERNMENT PRINTERY
ST KITTS W I