BERMUDA
1996 : 16

COMPUTER MISUSE ACT 1996

[Date of Assent 1 July 1996]

[Operative Date 1 July 1996]

ARRANGEMENT OF CLAUSES

WHEREAS it is expedient to make provision for securing computer material against unauthorised access and for related matters;

Be it enacted by The Queen's Most Excellent Majesty, by and with the advice and consent of the Senate and the House of Assembly of Bermuda, and by the authority of the same, as follows:—

Short title

1 This Act may be cited as the Computer Misuse Act 1996.

Interpretation

2 (1) References in this Act to any program or data held in a computer include references 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.

(2) In this Act—

"Criminal Code" means the Criminal Code Act 1907;

"modification" has the meaning assigned by section 6;

"program" includes part of a program;

"related inchoate offence", in relation to an offence under this Act, means an offence under section 32, 33, 230 or 231 of the Criminal Code (attempt, incitement, conspiracy etc) deriving from such an offence;

"securing access" has the meaning assigned by section 6;

"unauthorised", in relation to access to or modification of any program or data held in a computer, has the meaning assigned by section 6.

Unauthorised access to computer material

3 (1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section is liable on summary conviction to imprisonment for 6 months or to a fine of $6000 or to both.

Unauthorised access with intent to commit further offence

4 (1) A person is guilty of an offence under this section if he commits an offence under section 3 above ("the unauthorised access offence") with intent—

(a) to commit a further offence which is punishable on conviction on indictment by a term of imprisonment of two years or more; or

(b) to facilitate the commission of such a further offence (whether by himself or by any other person).

(2) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or any future occasion.

(3) 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.

(4) A person guilty of an offence under this section is liable—

(a) on summary conviction to imprisonment for 6 months or to a fine of $6000 or to both;

(b) on conviction on indictment to imprisonment for 5 years or to a fine of $20,000 or to both.

Unauthorised modification of computer material

5 (1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b)—

"requisite intent" is the intent to cause a modification to the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data;

but the intent need not be directed at any particular computer, any particular program or data or program or data of any particular kind, or any particular modification or a modification of any particular kind; and

"requisite knowledge" is knowledge that any modification which is intended to be caused is unauthorised.

(3) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it is, or is intended to be, permanent or merely temporary.

(4) A person guilty of an offence under this section is liable—

(a) on summary conviction to imprisonment for 6 months or to a fine of $6000 or to both;

(b) on conviction on indictment to imprisonment for 5 years or to a fine of $20,000 or to both.

Meaning of "securing access", "modification" and "unauthorised"

6 (1) A person secures access to any program or data held in a computer if by causing a computer to perform a function he—

(a) alters or erases the program or data;

(b) copies or moves it—

(i) to a different location in the storage medium in which it is held, or

(ii) to any other storage medium;

(c) uses it; or

(d) has it 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 an intent so to do shall be construed accordingly.

(2) For the purposes of subsection (1)(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.

(3) For the purposes of subsection (1)(d)—

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or other data is output is immaterial (including in particular whether any instructions are in a form which is capable of being executed or any data of being processed by a computer).

(4) Access of any kind by a 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 the person who is so entitled.

(5) 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 is altered or erased; or

(b) any program or data is added to its contents;

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

(6) Such a modification 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.

Significant link with Bermuda

7 (1) So long as the circumstances of any offence under section 3 or 5 above show a significant link with Bermuda, it is immaterial for the purposes of any such offence—

(a) whether any act or other event proof of which is required for conviction for the offence occurred in Bermuda; or

(b) whether the accused was in Bermuda at the time of any such act or event;

but there is no need for a significant link to exist for the commission of an offence under section 3 above to be established in proof of an allegation to that effect in proceedings for an offence under section 4 above.

(2) "Significant link", in relation to an offence under section 3, means—

(a) that the accused was in Bermuda at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in Bermuda at that time.

(3) "Significant link", in relation to an offence under section 5, means—

(a) that the accused was in Bermuda at the time when he did the act which caused the unauthorised modification; or

(b) that the unauthorised modification took place in Bermuda.

(4) Subject to subsection (5), where—

(a) a significant link exists in the case of an offence under section 3; and

(b) commission of that offence is alleged in proceedings for an offence under section 4;

section 4 shall apply as if anything the accused intended to do or facilitate in any place outside Bermuda which would be an offence to which section 4 applies if it took place in Bermuda were the further offence in question.

(5) A person is guilty of an offence triable by virtue of subsection (4) only if what he intended to do or facilitate would involve

the commission of an offence under the law in force where the whole or any part of it was intended to take place ("the relevant foreign law"); and

an act or omission which is punishable by or under any provision of the law in force in any place is an offence under that law for the purposes of this subsection however it is described.

(6) For the purposes of subsection (5), a person's conduct shall be taken to constitute an offence under the relevant foreign law unless not later than 21 days before summary trial of, or on committal for, an offence under this Act the defence serves on the prosecution a notice—

(a) stating that the facts as alleged do not in their opinion constitute an offence under the relevant foreign law;

(b) showing their grounds for that opinion; and

(c) requiring the prosecution to prove that the conduct does amount to an offence under the relevant foreign law.

(7) The court may, if it thinks fit, permit the defence to require the prosecution to prove that the defendant's conduct amounts to an offence under the relevant foreign law without the prior service of a notice in accordance with subsection (6).

(8) In proceedings in the Supreme Court, the question whether the defendant's conduct amounts to an offence under the relevant foreign law shall be decided by the judge alone.

(9) A notice under subsection (6) may be given to the prosecution by delivering it, sending it by registered letter, or, in the case of a prosecution brought by the Crown, by delivering it to the Attorney-General.

Territorial scope of inchoate offences

8 (1) This section has effect to supplement the provisions of the Criminal Code in relation to the jurisdiction of the courts of Bermuda to try offences which do not take place wholly in Bermuda.

(2) A person may be guilty of an offence under section 32 of the Criminal Code (attempts)—

(a) if he does any act in Bermuda which would constitute an attempt to commit an offence under section 5 of this Act but for the fact that the offence, if completed, would not be triable in Bermuda; and

(b) if what he was attempting would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place;

and subsections (5) to (9) of section 7 apply for the purposes of this subsection as they apply for the purposes of section 7(4).

(3) A person may also be guilty of an offence under section 32 of the Criminal Code if he does any act in any place outside Bermuda which constitutes an attempt to commit an offence under section 5 of this Act.

(4) A person may be guilty of an offence under section 33 of the Criminal Code (soliciting, inciting or attempting to procure offence) if in any place outside Bermuda he solicits, incites or attempts to procure another person to commit an offence under this Act.

(5) A person may be guilty of an offence under section 230 of the Criminal Code (conspiracy) if he conspires in any place outside Bermuda with any other person to commit an offence under this Act, and —

(a) any party to the conspiracy (or his agent) did anything in Bermuda in relation to it before its formation or did or omitted to do anything in Bermuda in pursuance of it; or

(b) at least one of the parties to the conspiracy became a party in Bermuda (either directly or through his agent).

(6) In proceedings for an offence under section 231(1) of the Criminal Code (conspiracy to commit offence outside Bermuda), where the principal offence within the meaning of that provision is an offence under this Act—

(a) subsections (5) to (9) of section 7 shall apply for the purposes of that offence as they apply for the purposes of an offence triable by virtue of section 7(4); and

(b) section 231(2) of the Criminal Code (defence to prove action not offence under foreign law) shall not apply.

Proceedings for offence under section 3

9 (1) Proceedings for an offence under section 3 may be brought within a period of six months from the date on which evidence sufficient in the opinion of the Attorney-General to warrant the proceedings came to his knowledge.

(2) But no such proceedings shall be brought more than three years after the commission of the offence.

(3) A certificate purporting to be under the hand of the Attorney-General and specifying the date upon which such facts first came to his notice shall be evidence that such facts first came to his notice on that date.

(4) This section has effect in place of section 452 of the Criminal Code (limitation of time for commencing summary prosecutions).

Conviction of section 3 offence as alternative to section 4 or 5

10 (1) If on the trial on indictment of a person charged with—

(a) an offence under section 4; or

(b) an offence under section 5 or any related inchoate offence,

the jury find him not guilty of the offence charged they may find him guilty of an offence under section 3 or any related inchoate offence if on the facts shown he could have been found guilty of that offence if proceedings had been brought within the time limit specified in section 9 for that offence.

(2) The Supreme Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section 3 or any related inchoate offence as the court of summary jurisdiction would have on convicting him of the offence.

(3) This section is without prejudice to sections 492 to 499 of the Criminal Code (conviction of alternative indictable offence).

Police powers

11 (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 464(1) of the Criminal Code (search and seizure of evidence etc) 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 464(1) of the Criminal Code include computers, disks or other computer equipment, the magistrate before whom those items are brought in accordance with section 467 of the Criminal Code (detention and disposal of property seized) 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 72 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 subsections (2) or (3) shall, for the purposes of admissibility in any proceedings, be treated as if they were themselves the items seized.

Forfeiture

12 (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).

Evidence

13 In proceedings for an offence under this Act, or any related inchoate offence, the fact that an offence involving interference with a computer is alleged to have been committed shall not of itself be sufficient to prevent computer records from being admissible in the proceedings on the basis that the condition in section 43B(2)(c) of the Evidence Act 1905 (which requires appropriate measures to be in force for preventing unauthorised interference with the computer) has not been satisfied.

[this page intentionally left blank]