REPUBLIC OF SINGAPORE

GOVERNMENT GAZETTE

ACTS SUPPLEMENT

Published by Authority

The following Act was passed by Parliament on 28th May 1993 and assented to by the President on 9th July 1993:—

COMPUTER MISUSE ACT 1993

(No. 19 of 1993)

ARRANGEMENT OF SECTIONS

PART III

MISCELLANEOUS AND GENERAL

REPUBLIC OF SINGAPORE

No. 19 of 1993.

I assent.

(LS)

WEE KIM WEE
President.
9th July 1993.

An Act to make provision for securing computer material against unauthorised access or modification and for matters related thereto.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

PART I

PRELIMINARY

Short title and commencement

1. This Act may be cited as the Computer Misuse Act 1993 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

Interpretation

2.—(1) In this Act, unless the context otherwise requires —

"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 an automated typewriter or typesetter, a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

"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;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"electronic, acoustic, mechanical or other device" means any device or apparatus that is used or 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.

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

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

(*a*) causes the program to be executed; or

(*b*) is itself a function of the program.

(4) For the purposes of subsection (2)(*d*), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or 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 by him of the kind in question to the program or data from any person who is so entitled.

(6) A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; 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 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.

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

PART II

OFFENCES

Unauthorised access to computer material

3.—(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds $10,000, a person convicted of the offence shall be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(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.

Unauthorised access with intent to commit or facilitate commission of further offences

4.—(1) Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(2) This section shall apply to offences involving property, fraud, dishonesty or which causes bodily harm punishable on conviction with imprisonment for a term of 2 years or more.

(3) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorised access is secured or on any future occasion.

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 conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds $10,000, a person convicted of the offence shall be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(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 interception 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 electromagnetic, 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 conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage caused by an offence under this section exceeds $10,000, a person convicted of the offence shall be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(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.

Abetments and attempts punishable as offences

7.—(1) Any person who 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 conviction to the punishment provided for the offence.

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

PART III

MISCELLANEOUS AND GENERAL

Territorial scope of offences under this Act

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

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

    (*a*) the accused was in Singapore at the material time; or

    (*b*) the computer, program or data was in Singapore at the material time.

Jurisdiction of Courts

9. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act.

Order for payment of compensation

10.—(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.

Evidence from computer records

11.—(1) Notwithstanding sections 35 and 36 of the Evidence Act (Cap. 97), in any proceedings under this Act, any relevant computer output shall be admissible as evidence of any fact stated therein if it is shown —

(*a*) that there is no reasonable ground for believing that the output is inaccurate because of improper use of the computer and that no reason exists to doubt or suspect the truth or reliability of the output; or

(*b*) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the output or the accuracy of its contents.

(2) For the purpose of deciding whether or not such output is so admissible, the court may draw any reasonable inference from the circumstances in which the output was made or otherwise came into being.

(3) The Minister may make rules requiring that, in any proceedings where it is desired to give a statement in evidence by virtue of this section, such information concerning the statement as may be required by the rules shall be provided in such form and at such time as may be so required.

Supplementary provisions on evidence

12.—(1) In any proceedings where it is desired to admit computer output in evidence in accordance with section 11, a certificate —

(*a*) identifying the computer output and describing the manner in which it was produced;

(*b*) giving such particulars of any device involved in the production of that computer output as may be appropriate for the purpose of showing that the output was produced by a computer;

(*c*) dealing with any of the matters mentioned in section 11(1); and

(*d*) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer at all relevant times,

shall be admitted in those proceedings as evidence of anything stated in the certificate.

(2) If the person referred to in subsection (1)(*d*) who occupies a responsible position in relation to the operation of the computer did not have control or access over any relevant records and facts in relation to the production by the computer of the computer output, a supplementary certificate signed by another person who had such control or access and made in accordance with subsection (1)(*a*) to (*c*) shall be evidence of anything stated in the certificate.

(3) For the purposes of subsections (1) and (2), it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(4) Notwithstanding subsection (1) or (2), a court may require oral evidence to be given of anything of which evidence could be given by a certificate under that subsection.

(5) Any person who in a certificate tendered under subsection (1) or (2) in a court makes a statement which he knows to be false or does not believe to be true shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 2 years or to both.

(6) In estimating the weight, if any, of any admissible computer output, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output and, in particular —

   (*a*) to the question whether or not the information which the output reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and

   (*b*) to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the admissible computer output was produced by it, had any incentive to conceal or misrepresent the facts.

(7) For the purposes of subsection (6), information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment.

Proof by document or copy thereof

13. Notwithstanding the provisions of the Evidence Act (Cap. 97), where in any proceedings any computer output is admissible in evidence in accordance with section 11, it may be proved —

   (*a*) by the production of that computer output; or

(*b*) (whether or not that computer output is still in existence) by the production of a copy of that output, or of the material part of it,

authenticated in such manner as the court may approve.

Powers of police officer to investigate and require assistance

14. In connection with the exercise of his powers of investigations under the Criminal Procedure Code (Cap. 68), a police officer —

(*a*) shall be entitled at any time to have access to, and inspect and check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act; and

(*b*) may require —

(i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or

(ii) any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material,

to provide him with such reasonable assistance as he may require for the purposes of paragraph (*a*).

Arrest by police without warrant

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

———————