THE COMPUTER MISUSE BILL, 2000

Explanatory Note (These notes form no part of the Bill but are intended only to indicate its general purport.)

The main purpose of this Bill is to prohibit the unauthorised access, use of or interference to any program or data held in a computer and to a computer itself.

The Bill therefore seeks to enhance computer security by giving protection to the integrity of computer systems and by providing stringent penalties for specified computer related offences. The Bill also provides enhanced penalties in case where the offence results in damage, which includes financial loss, injury, or harm. This Bill is divided into three parts.

- **PART 1 will provide for preliminary matters.**
  - **Clause 1 of the Bill would provide the short title.**
  - **Clause 2 would provide the interpretation provision.**

- **PART II would provide for numerous computer related offences.**

  - **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.**

  - **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 section 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 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.**

- **PART III would provide for certain general provisions.**

  - **Clause 12 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 the State at the material time, or damage occurred within the State whether or not he or the computer was within the State at the material time.**

  - **Clause 13 would provide the 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 14 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 15 would preserve the power of a police office to conduct investigations as permitted under any written law.**

  - **Clause 16 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 17 would allow a police officer to arrest a person without warrant for the commission of any offence under this Act.**

  - **Clause 18 would provide that a person can be prosecuted for an offence, except an offence under section 9, within one year from the date the offence was committed.**

BILL - An Act to prohibit any unauthorised access, use or interference with a computer and for other related matters.

PART I - PRELIMINARY

1. Short title This Act may be cited as the Computer Misuse Act, 2000.

2. Interpretation (1). In this Act -

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

- an automated typewriter or typesetter;
- a portable hand held calculator;
- a similar device which is non-programmable or which does not contain any data storage facility; or
- such other device as the Minister may prescribe by Order ;

"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 -

- produced by a computer; or
- accurately translated from a statement or representation so produced;

"computer service" includes computer time, computer output, data processing and the storage or retrieval of a program or data;

"damage", except for the purposes of section 13, includes any impairment to a computer or the integrity or availability of any program or data held in a computer that -

- causes loss aggregating at least ten 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;
- modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of a person;
- causes or threatens physical injury or death to a person; or
- threatens the public interest;

"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 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;

"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, 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

3. Unauthorised access to computer program or data

(1). Subject to subsection (2), 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 $15,000 and to imprisonment for 2 years and, in the case of a second or subsequent conviction, to a fine of $30,000 and to imprisonment for 4 years.

(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 a fine of $20,000 and to imprisonment for three years.

(3) 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.

(4) 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.

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

(6) For the purposes of subsection (4)(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. Access with intent to commit or facilitate commission of offence

(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 -
(a) involving property, fraud, dishonesty or which causes bodily harm; and
(b) which is punishable on conviction with imprisonment for more than 1 year, commits an offence and is liable on summary conviction to a fine of $15,000 and to imprisonment for 2 years.

(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 this section 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. Unauthorised modification of computer program or data

(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 $15,000 and to imprisonment for 2 years and, in the case of a second or subsequent conviction, to a fine of $30,000 and to imprisonment for 4 years.

(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 $20,000 and to imprisonment for 3 years.

(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;

(c) 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.

6. Unauthorised use or interception of computer service

(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 $15,000 and to imprisonment for 2 years and, in the case of a second or subsequent conviction, to a fine of $30,000 and to imprisonment for 4 years.**

(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 $20,000 and to imprisonment for 3 years.

(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.**

7. Unauthorised obstruction of use or use of computer

(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 $15,000 and to imprisonment for 2 yrs and, in the case of a second or subsequent conviction, to a fine of $30,000 and to imprisonment for four years.

(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 $20,000 and to imprisonment for three years.

8. Unauthorised disclosure of access code

(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 $15,000 and to 2 yrs imprisonment and, in the case of a second or subsequent conviction, to a fine of $30,000 and to imprisonment for four years.

(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 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 $30,000 and to imprisonment for four years and, in the case of a second or subsequent conviction, to a fine of fifty thousand dollars and to imprisonment for five years.

9. Enhanced punishment for offences involving protected computers

(1) Where access to any protected computers is obtained in the course of the commission of an offence under section 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 one hundred and fifty thousand dollars and to imprisonment for ten years.

(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.

10. Unauthorised receiving or giving access to computer program or data

(1) A person who receives or is given access to any program or data held in a computer, or who is not authorised to receive or have access to that program or data, from another person whether or not 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 $15,000 and to imprisonment for 2 yrs.

(2) A person who is authorised to receive or have access to any program or data held in a computer and who receives that program or data from another person knowing that that person has obtained that program or data through unauthorised means commits an offence and is liable on summary conviction to a fine of $15,000 and to imprisonment for 2 yrs.

(3) 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 $15,000 and to imprisonment for 2 yrs.

(4) A person who has obtained any program or data held in a computer through unauthorised means and gives that program or data to another person whether or not he knows that that other person is authorised to receive or have access to that program or data commits an offence and is liable on summary conviction to a fine of $15,000 and to imprisonment for 2 yrs.

11. Causing a computer to cease to function

(1) A person who engages in conduct which causes a computer 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.

(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) impair the operation of the computer,**

but the intent need not be directed at a particular computer.

PART III - GENERAL PROVISIONS

12. Territorial scope of offence under this Act

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

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question -
- **(a) the accused was in the State at the material time;**
- **(b) the computer, program or data was in the State at the material time; or**
- **(c) the damage occurred within the State, whether or not paragraph (a) or (b) applies.**

13. Jurisdiction of court

(1) A 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 section 9, 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.**

14. Order for payment of compensation

(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.

15. Saving for investigations by police officer

(1) 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.

16. Power of police officer to access computer program and data

(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 use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

(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 $15,000 and to imprisonment for 2 yrs.

(7) For the purposes of this section -
- (a) "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;
- (b) "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;
- (c) "plain text version" means a program or original data before it has been transformed or scrambled to an unreadable or incomprehensible format

17. Arrest by police officer without warrant

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

18. Limitation period

Not withstanding any other written law, a person who commits an offence under this Act, except an offence under section 9, may be prosecuted at any time within twelve months after the commission of the offence.