AS TABLED IN THE HOUSE OF ASSEMBLY

A BILL

entitled

COMPUTER MISUSE ACT 2024

TABLE OF CONTENTS

WHEREAS it is expedient to repeal the Computer Misuse Act 1996 and replace it with a comprehensive statutory scheme that updates the law by re-enacting and enhancing criminal offences relating to unauthorised access of computers, which scheme is in line with international best practice as contained in the Council of Europe Convention on Cybercrime signed in Budapest on 23 November 2001; and to provide for matters related to the foregoing;

Be it enacted by The King'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:

PART 1

PRELIMINARY

Citation

1 This Act may be cited as the Computer Misuse Act 2024.

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—

(a) an automated typewriter or typesetter;

(b) a portable hand-held calculator;

(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, by notice in the Gazette, prescribe;

"Criminal Code" means the Criminal Code Act 1907;

"damage" shall be construed as provided in section 6;

"data" means any representation of facts, information or concepts in a form suitable for processing in a computer, including a programme suitable to cause a computer to perform a function, and includes a reference to "data" as provided in subsection (6);

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

"Minister" means the Minister of National Security;

"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;

"program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function, and includes a reference to "program" as provided in subsection (6);

"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 subsection (2);

"unauthorised" in relation to access to or modification of any program or data held in a computer, has the meaning assigned by subsection (5).

(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 the person—

(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) are to be read accordingly.

(3) For the purposes of subsection (2)(c), a person uses a program if the function the person 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)—

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

(b) the person does not have consent to such access from the person who is so entitled.

(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 if the person—

(a) is not himself entitled to control access of the kind in question to the program or data; and

(b) does not have consent to such access from the person who is so entitled.

(6) References 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.

(7) An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)—

(a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and

(b) does not have consent to the act from any such person.

(8) In subsection (7) "act" includes a series of acts.

(9) References to a program include references to part of a program.

PART 2

COMPUTER MISUSE OFFENCES

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 or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function 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 $18,000 or to both.

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

4 (1) A person is guilty of an offence under this section if he commits an offence under section 3 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;

(b) to facilitate the commission of 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 $18,000 or to both;

(b) on conviction on indictment to imprisonment for 5 years or to a fine of $60,000 or to both.

Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

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

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act—

(a) to impair the operation of any computer;

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

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

(d) to enable any of the things mentioned in paragraphs (a) to (c) to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2).

(4) The intention referred to in subsection (2), or the recklessness referred to in subsection (3), need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act " includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction to imprisonment for 6 months or to a fine of $18,000, or to both;

(b) on conviction on indictment to imprisonment for 5 years or to a fine of $60,000 or to both.

Unauthorised acts causing, or creating risk of, serious damage

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

(a) the person does any unauthorised act in relation to a computer;

(b) at the time of doing the act the person knows that it is unauthorised;

(c) the act causes, or creates a significant risk of, serious damage of a material kind; and

(d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.

(2) Damage is of a "material kind" for the purposes of this section if it is damage to—

(a) human welfare in any place;

(b) the environment of any place;

(c) the economy of any country; or

(d) the national security of any country.

(3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes—

(a) loss to human life;

(b) human illness or injury;

(c) disruption of a supply of money, food, water, energy or fuel;

(d) disruption of a system of communication;

(e) disruption of facilities for transport; or

(f) disruption of services relating to health.

(4) It is immaterial for the purposes of subsection (2) whether or not an act causing damage—

(a) does so directly;

(b) is the only or main cause of the damage.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.

(6) A person guilty of an offence under this section is (unless subsection (7) applies) liable, on conviction on indictment, to imprisonment for 14 years, or to a fine of $100,000, or to both.

(7) Where an offence under this section is committed as a result of an act causing or creating a significant risk of—

(a) serious damage to human welfare of the kind mentioned in subsection (3)(a) or (3)(b); or

(b) serious damage to national security,

a person guilty of the offence is liable, on conviction on indictment, to imprisonment for life, or to a fine of $1,000,000 or to both.

Making, supplying or obtaining articles for use in offence under section 3, 5 or 6

7 (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 3, 5 or 6.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 3, 5 or 6.

(3) A person is guilty of an offence if he obtains any article—

(a) intending to use it to commit, or to assist in the commission of, an offence under section 3, 5 or 6; or

(b) with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 3, 5 or 6.

(4) In this section "article " includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction to imprisonment for 6 months or to a fine of $18,000, or to both;

(b) on conviction on indictment, to imprisonment for a term of two years or to a fine of $60,000, or to both.

PART 3

JURISDICTION

Territorial scope of offences under this Act

8 (1) Except as provided in this section, it is immaterial for the purposes of any offence under section 3, 5 or 6—

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

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

(2) Subject to subsection (3), in the case of such an offence at least one significant link with Bermuda must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 3 to be established in proof of an allegation to that effect in proceedings for an offence under section 4.

(4) Where—

(a) any such link does in fact exist 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 offence in question.

(5) It is immaterial for the purposes of an offence under section 5 whether the accused was in Bermuda at the time of any act or other event, proof of which is required for conviction of the offence, if there is a significant link with Bermuda in relation to the offence.

Significant links with Bermuda

9 (1) The following provisions of this section apply for the interpretation of section 8.

(2) In relation to an offence under section 3, 5, 6 or 7, where the accused was in a country outside Bermuda at the time of the act constituting the offence there is a significant link with Bermuda if—

(a) at that time the accused was—

(i) a person possessing Bermudian status or who was a permanent resident (within the meaning of the Bermuda Immigration and Protection Act 1956);

(ii) a person holding a work permit granted under that Act; or

(iii) a body corporate as defined in section 11.

(b) the act constituted an offence under the law of the country in which it occurred.

(3) In subsection (2), "country" includes territory.

(4) In relation to an offence under section 3, any of the following is a significant link with Bermuda—

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

(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; or

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

(5) In relation to an offence under section 5, either of the following is a significant link with Bermuda—

(a) that the accused was in Bermuda at the time when the offence was committed;

(b) that the unauthorised act was done in relation to a computer in Bermuda.

(6) In relation to an offence under section 6, any of the following is a significant link with Bermuda—

(a) that the accused was in Bermuda at the time when he did the unauthorised act (or caused it to be done);

(b) that the unauthorised act was done in relation to a computer in Bermuda;

(c) that the unauthorised act caused, or created a significant risk of, serious damage of a material kind (within the meaning of that section) in Bermuda.

Territorial scope of inchoate offences

10 (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 (6) to (10) apply for the purposes of this subsection.

(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) A person is guilty of an offence triable by virtue of subsection (2) 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.

(7) For the purposes of subsection (6), 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.

(8) 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 (7).

(9) 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.

(10) A notice under subsection (7) 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 Director of Public Prosecutions.

Offences by bodies corporate

11 (1) This section applies for purposes of section 9(2) if an offence under that section is committed by a body corporate.

(2) If the offence is proved to have been committed with the consent or connivance of—

(a) a senior officer of the body corporate; or

(b) a person purporting to act in such a capacity,

the senior officer or person (as well as the body corporate) is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) In this section—

"body corporate" means—

(a) a body which is incorporated or formed under the law of Bermuda and which carries on a business (whether in Bermuda or elsewhere);

(b) any other body corporate (wherever incorporated) which carries on a business, or part of a business in Bermuda;

(c) a partnership which is formed under the law of Bermuda and which carries on a business (whether in Bermuda or elsewhere); or

(d) any other partnership (wherever formed) which carries on a business, or part of a business, in Bermuda;

"director" in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate;

"senior officer" means a director, manager or other similar officer of the body corporate.

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

(a) on summary conviction to imprisonment for 6 months or to a fine of $18,000, or to both;

(b) on conviction on indictment, to imprisonment for a term of two years or to a fine of $60,000, or to both.

PART 4

ENFORCEMENT AND INVESTIGATIONS

Proceedings for offence under section 3

12 (1) Notwithstanding section 80 of the Criminal Jurisdiction and Procedure Act 2015, proceedings for an offence under section 3 may be brought within a period of 12 months—

(a) after the offence is committed; or

(b) from the date on which evidence sufficient in the opinion of the Director of Public Prosecutions to warrant the proceedings came to his knowledge,

whichever is the later.

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

(3) For purposes of subsection (1)(b), a certificate purporting to be under the hand of the Director of Public Prosecutions 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.

Conviction of section 3 offence as alternative to section 4, 5, 6 or 7

13 (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, 6 or 7 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 12 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

14 (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 8(1) of the Police and Criminal Evidence Act 2006 (power of magistrate to authorize entry and search of premises) 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 19(2) and (4) of the Police and Criminal Evidence Act 2006 (general power of seizure etc.) include computers, removable storage mediums or other computer equipment, on a request being made by the person to whom those items belong or from under whose control they were taken, and subject to subsection (4), the police officer who has seized the items—

(a) may, in accordance with section 21 of the Police and Criminal Evidence Act 2006 (access and copying), make copies of such programs or data held in the computer, removable storage medium or other equipment as may be required for the investigation or prosecution of the offence;

(b) shall give copies of those copies to the person charged in relation to the offence ("the accused person"); and

(c) shall cause the items to be returned to the person from whom they were taken 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 a request for copies 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, removable storage mediums or other equipment, the harm which may be caused to the business or other interests of the person to whom those items belong or from under whose control they are taken 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

15 (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).

PART 5

MISCELLANEOUS PROVISIONS

Regulations

16 (1) The Minister may make regulations for purposes of this Act, prescribing anything that is necessary or expedient to be prescribed for the carrying out of the provisions of this Act or to give effect to it.

(2) Regulations made under this Act are subject to the negative resolution procedure.

Consequential amendments

17 The Minister may, by regulations, make amendments to such enactments or instruments as appear to the Minister to be necessary or expedient in consequence of, or for the purposes of, this Act or regulations made under this Act.

Repeal of Computer Misuse Act 1996 and savings

18 (1) The Computer Misuse Act 1996 is repealed (the "repealed Act").

(2) The repeal of the repealed Act shall not affect the liability of any person to prosecution under that Act for an offence committed before the commencement of this

Act, and the repealed Act shall continue to apply in relation to such an offence as if this Act had not been enacted.

Commencement

19 This Act shall come into operation on such day as the Minister may appoint by notice published in the Gazette.

COMPUTER MISUSE BILL 2024

EXPLANATORY MEMORANDUM

This Bill seeks to repeal the Computer Misuse Act 1996 (the current Act) and replace it with a comprehensive statutory scheme that updates the law by re-enacting and enhancing criminal offences relating to unauthorised access of computers, which scheme is mostly in line with provisions of the UK Computer Misuse Act 1990 that meet international best practice as contained in the Council of Europe Convention on Cybercrime signed in Budapest on 23 November 2001; and to provide for matters related to the foregoing.

Clause 1 provides a citation for the Bill.

Clause 2 provides for the definitions of some of the terms and expressions in the Bill. The new definitions in the Bill include the definitions of the terms "computer", "damage", "data" and "output". Subsections (2) to (9), which provide detailed definitions of specific expressions used in the Bill, are taken from section 6 of the current Act and have been updated in accordance with the applicable provisions of section 17 of the UK Computer Misuse Act 1990.

Clause 3 provides an update to the offence in section 3 of the current Act of "unauthorised access to computer material" in accordance with section 1 of the UK Computer Misuse Act 1990. The offence is punishable on summary conviction with imprisonment for six months or a fine of $18,000 or both.

Clause 4 provides for "unauthorised access committed with intent to commit or facilitate commission of further offences" in accordance with section 4 of the current Act. The offence is punishable on summary conviction with imprisonment for six months or a fine of $18,000 or both; or on conviction on indictment, with imprisonment for five years or a fine of $60,000 or both.

Clause 5 is a new provision, which prohibits "unauthorised acts with intent to impair operation of computer, etc.". The offence occurs when a person does with recklessness any unauthorised acts with the intention to impair the operation of any computer; to prevent or hinder access to any program or data; or to impair the operation of any such program or reliability of such data. The provision is adapted from section 3 of the UK Computer Misuse Act 1990. The offence is punishable on summary conviction with imprisonment for six months or a fine of $18,000 or both; or on conviction on indictment, with imprisonment for five years or a fine of $60,000 or both.

Clause 6 is a new provision, which prohibits "unauthorised acts that cause or create the risk of serious damage". The offence occurs when a person does any unauthorised acts to cause or create a significant risk of serious damage of a material kind and the act is done with recklessness as to whether such damage is caused. The clause defines damage of a "material kind" to include damage to human welfare in any place; damage to the environment of any place; damage to the economy of any country; or damage to the national security of any country. The provision is adapted from section 3ZA of the UK

Computer Misuse Act 1990. The offence is punishable on conviction on indictment with imprisonment for life or a fine of $1,000,000 or both.

Clause 7 is a new provision, which prohibits the making, adapting, supplying or offering to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 3, 5 or 6. The provision is adapted from section 3A of the UK Computer Misuse Act 1990. The offence is punishable on summary conviction with imprisonment for six months or a fine of $18,000 or both; or on conviction on indictment, with imprisonment for five years or a fine of $60,000 or both.

Clause 8 provides for territorial scope of offences under this Act and updates the provisions of section 7(1) of the current Act. Under this clause it is immaterial for the purposes of any offence under section 3, 5 or 6 as to whether the act or event occurred in Bermuda or whether the accused was in Bermuda at the time of the offence, but at least one significant link with Bermuda must exist in the circumstances of the case for the offence to be committed.

Clause 9 provides the criteria for determining significant links with Bermuda in relation to an offence under section 3, 5, 6 or 7, where an offence is committed outside Bermuda. The clause is adapted from section 5 of the UK Computer Misuse Act 1990.

Clause 10 provides for the territorial scope of inchoate offences, which do not take place wholly in Bermuda. The clause is an updated version of section 8 of the current Act.

Clause 11 provides for offences under the Bill that are committed by bodies corporate (as defined). Where it is proved that the offence is committed with the consent or connivance of a senior officer of the body corporate or any person acting in that capacity, such person shall also be guilty of the offence. The clause is adapted from section 20 of the Bribery Act 2016. The offence is punishable on summary conviction with imprisonment for six months or a fine of $18,000 or both; or on conviction on indictment, with imprisonment for five years or a fine of $60,000 or both.

Clause 12 provides for proceedings for the offence under section 3 to be brought within a period of twelve months either after the offence is committed or from the date on which evidence that warrants proceedings came to the knowledge of the Director of Public Prosecutions. The clause is an updated version of section 9 of the current Act.

Clause 13 provides for instances where a conviction of a section 3 offence can be an alternative to section 4, 5, 6 or 7. The clause is an updated version of section 10 of the current Act.

Clause 14 provides for police powers of investigation, entry and seizure. The clause is an updated version of section 11 of the current Act, with reference now being made to the powers of the police under the Police and Criminal Evidence Act 2006.

Clause 15 provides for forfeiture of any property in a person's possession or under his control at the time of the offence which was used to commit or facilitate the commission of an offence under this Act or was intended to do so. The clause is an updated version of section 12 of the current Act.

Clause 16 provides for the Minister's powers to make regulations.

Clause 17 empowers the Minister to make consequential amendments to other legislation by order subject to the negative resolution procedure.

Clause 18 provides for the repeal of Computer Misuse Act 1996 and savings to preserve the repealed Act in relation to offences committed before the commencement of this Act.

Clause 19 provides for the commencement of the Act.