Computer Misuse and Cybersecurity (Amendment) Bill

Bill No. 15/2017.

Read the first time on 9 March 2017.

A BILL

i n t i t u l e d

An Act to amend the Computer Misuse and Cybersecurity Act (Chapter 50A of the 2007 Revised Edition).

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

Short title and commencement

1. This Act is the Computer Misuse and Cybersecurity (Amendment) Act 2017 and comes into operation on a date that the Minister appoints by notification in the *Gazette*.

Amendment of section 2

2. Section 2(1) of the Computer Misuse and Cybersecurity Act (called in this Act the principal Act) is amended by deleting the words "or apparatus" in the definition of "electro-magnetic, acoustic, mechanical or other device" and substituting the words ", apparatus or program".

New sections 8A and 8B

3. The principal Act is amended by inserting, immediately after section 8, the following sections:

"**Supplying, etc., personal information obtained in contravention of certain provisions**

8A.—(1) A person shall be guilty of an offence if the person, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 —

(*a*) obtains or retains the personal information; or

(*b*) supplies, offers to supply, transmits or makes available, by any means the personal information.

(2) It is not an offence under subsection (1)(*a*) if the person obtained or retained the personal information for a purpose other than —

(*a*) for use in committing, or in facilitating the commission of, any offence under any written law; or

(*b*) for supply, transmission or making available by any means for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law.

(3) It is not an offence under subsection (1)(*b*) if —

(*a*) the person did the act for a purpose other than for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law; and

(*b*) the person did not know or have reason to believe that the personal information will be or is likely to be used to commit, or facilitate the commission of, any offence under any written law.

Example 1.— *A* comes across a list of credit card numbers on the Internet belonging to individuals who are customers of *B*, which *A* has reason to believe were obtained by securing access without authority to *B*'s server. *A* downloads the list for the purpose of reporting the unauthorised access to *B*'s server to the police.

A retains the list of credit card numbers and transmits it to *B* for the purpose of informing *B* of the unauthorised access to *B*'s server.

A has downloaded and retained the list of credit card numbers for purposes other than those mentioned in subsection (2)(*a*) and (*b*). Therefore *A* does not commit an offence under subsection (1)(*a*) by reason of subsection (2).

A has transmitted the list to *B* for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If *A* did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then *A* does not commit an offence under subsection (1)(*b*) by reason of subsection (3).

Example 2.— *C*, an employee of *B*, after receiving the list from *A* in *Example* 1, transmits it to *D*, another employee of *B*, for the purpose of facilitating *B*'s investigation of the unauthorised access of *B*'s server.

C has transmitted the list to *D* for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If *C* did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then *C* does not commit an offence under subsection (1)(*b*) by reason of subsection (3).

(4) For the purposes of subsection (1)(*b*), a person does not transmit or make available personal information merely because the person provides, or operates facilities for network access, or provides services relating to, or provides connections for, the transmission or routing of data.

(5) A person guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(6) For the purpose of proving under subsection (1) that a person knows or has reason to believe that any personal information was obtained by an act done in contravention of section 3, 4, 5 or 6, it is not necessary for the prosecution to prove the particulars of the contravention, such as who carried out the contravention and when it took place.

(7) In this section —

(*a*) personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password; and

(*b*) a reference to an offence under any written law includes an offence under subsection (1).

Obtaining, etc., items for use in certain offences

8B.—(1) A person shall be guilty of an offence if the person —

(*a*) obtains or retains any item to which this section applies —

(i) intending to use it to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7; or

(ii) with a view to it being supplied or made available, by any means for use in committing, or in facilitating the commission of, any of those offences; or

(*b*) makes, supplies, offers to supply or makes available, by any means any item to which this section applies, intending it to be used to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7.

(2) This section applies to the following items:

(*a*) any device, including a computer program, that is designed or adapted primarily, or is capable of being used, for the purpose of committing an offence under section 3, 4, 5, 6 or 7;

(*b*) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

(3) A person guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.".

Amendment of section 11

4. Section 11 of the principal Act is amended —

(*a*) by deleting the words "subsection (2)" in subsection (1) and substituting the words "subsection (3)"; and

(*b*) by deleting subsection (3) and substituting the following subsections:

"(3) For the purposes of this section, this Act applies if —

(*a*) for the offence in question, the accused was in Singapore at the material time;

(*b*) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8), the computer, program or data was in Singapore at the material time; or

(*c*) the offence causes, or creates a significant risk of, serious harm in Singapore.

(4) In subsection (3)(*c*), "serious harm in Singapore" means —

(*a*) illness, injury or death of individuals in Singapore;

(*b*) a disruption of, or a serious diminution of public confidence in, the provision of any essential service within the meaning of section 15A(12) in Singapore;

(*c*) a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board; or

(*d*) damage to the national security, defence or foreign relations of Singapore.

Example 1.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the provision of an essential service:

(*a*) publication to the public of the medical records of patients of a hospital in Singapore;

(*b*) providing to the public access to the account numbers of customers of a bank in Singapore.

Example 2.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a

statutory board, or a part of the Government, an Organ of State or a statutory board:

(*a*) providing to the public access to confidential documents belonging to a ministry of the Government;

(*b*) publication to the public of the access codes for a computer belonging to a statutory board.

(5) For the purposes of subsection (3)(*c*), it is immaterial whether the offence that causes the serious harm in Singapore —

(*a*) causes such harm directly; or

(*b*) is the only or main cause of the harm.

(6) In subsection (4)(*c*), "statutory board" means a body corporate or unincorporate established by or under any public Act to perform or discharge a public function.".

New section 11A

5. The principal Act is amended by inserting, immediately after section 11, the following section:

"**Amalgamation of charges**

11A.—(1) This section applies when a person is alleged to have committed 2 or more acts —

(*a*) each of which is an offence under the same provision in Part II;

(*b*) that involve the same computer; and

(*c*) that are committed in a period that does not exceed 12 months.

(2) Despite section 124 of the Criminal Procedure Code (Cap. 68), it is sufficient for the charge in respect of those acts to specify —

(*a*) particulars of that computer; and

(*b*) the dates between which the acts are alleged to have been committed,

without specifying the exact dates the acts are committed.

(3) A charge framed in accordance with subsection (2) is treated as a charge of one offence.

(4) If the particulars mentioned in subsection (2)(*a*) and (*b*) do not give the accused sufficient notice of what the accused is charged with, then the charge must also give details of how the alleged offence was committed as will be sufficient for that purpose.".

EXPLANATORY STATEMENT

This Bill seeks to amend the Computer Misuse and Cybersecurity Act (Cap. 50A), primarily to deal with the changing modus operandi with which computer offences are carried out.

Clause 1 relates to the short title and commencement.

Clause 2 amends the definition of "electro-magnetic, acoustic, mechanical or other device" in section 2 (Interpretation). That term is used in section 6(1)(*b*). Section 6(1)(*b*) criminalises the unauthorised interception of a computer function by means of an electro-magnetic, acoustic, mechanical or other device. The definition is amended to expressly mention a software program that is used or capable of being used for such interception.

Clause 3 introduces 2 new offences in the Act.

The new section 8A covers acts done in relation to personal information of individuals that the perpetrator knows or has reason to believe has been obtained by committing a computer crime. The prohibited acts are obtaining, retaining, supplying, offering to supply, transmitting or making available the personal information. It is not an offence (in relation to the act of obtaining or retaining the information) if the perpetrator did the act for a legitimate purpose. It is not an offence (in relation to the other acts) if the perpetrator did the act for a legitimate purpose, and did not know or have reason to believe that the information will be or is likely to be used to commit or facilitate the commission of an offence.

In proving whether the perpetrator knows or has reason to believe that the personal information was obtained by committing a computer crime, it is not necessary for the prosecution to prove the exact details of the commission of the

crime. For example, if a person comes across personal information the nature of which suggests that it could only have been obtained by an unauthorised access to another person's computer, the person must not do any of the prohibited acts with that information whether or not the person who carried out the unauthorised access is known or can be discovered.

The new section 8B covers various acts done in connection with an item that is designed or adapted or is capable of being used to commit a computer crime, or by which a computer or part of a computer is capable of being accessed. The acts include —

(*a*) obtaining or retaining such an item intending to use it to commit or to facilitate the commission of a computer crime, or with a view to it being supplied or made available for such use; and

(*b*) making, supplying, offering to supply or making available such item intending it to be used to commit or to facilitate the commission of a computer crime.

Clause 4 amends section 11 (Territorial scope of offences under this Act) to give extraterritorial application to computer offences, where the act causes or creates a significant risk of serious harm in Singapore.

Currently, offences in the Act have extraterritorial effect only if the accused or the computer, program or data was in Singapore at the material time. This prevents enforcement action from being taken against a person who was overseas at the material time and who targeted an overseas computer, even though the act resulted in serious harm, or a significant risk of such harm, in Singapore.

"Serious harm in Singapore" has been defined to include, among other things, illness, injury or death of individuals in Singapore, disruption of essential services in Singapore, and disruption of the carrying out of governmental duties and functions.

An amendment is also made to the rule in existing subsection (3)(*b*) (an offence has extraterritorial effect if the computer, program or data was in Singapore at the material time) to clarify that it only applies for the offences under section 3, 4, 5, 6, 7 or 8.

Finally an amendment is made to subsection (1) of section 11 to amend a cross-reference.

Clause 5 introduces a new section 11A which allows the prosecution to amalgamate as a single charge of one offence, 2 or more acts that are the same computer offence, and are committed over a 12-month or shorter period in relation to the same computer.

A criminal may carry out multiple unauthorised acts on a computer over a period of time in order to prepare for an actual attack on the computer. Currently, a

separate charge must be framed for each act. Amalgamating the multiple acts as a single charge will allow the attack to be described as a whole, rather than as a series of acts. Where the acts together cause "damage", provisions like sections 3(2) and 5(2) — which apply enhanced punishment where the offence resulted in any "damage" as defined in section 2(1) — can then be applied.

EXPENDITURE OF PUBLIC MONEY

This Bill will involve the Government in extra financial expenditure, the exact amount of which cannot at present be ascertained.