South Australia

Statutes Amendment (Computer Offences) Act 2004

An Act to amend the *Criminal Law Consolidation Act 1935* and the *Summary Offences Act 1953*.

Contents

Part 1—Preliminary

1 Short title
2 Commencement
3 Amendment provisions

Part 2—Amendment of *Criminal Law Consolidation Act 1935*

4 Insertion of Part 4A

Part 4A—Computer offences

86B Interpretation
86C Meaning of unauthorised access to or modification of computer data
86D Meaning of unauthorised impairment of electronic communication
86E Use of computer with intention to commit, or facilitate the commission of, an offence
86F Use of computer to commit, or facilitate the commission of, an offence outside the State
86G Unauthorised modification of computer data
86H Unauthorised impairment of electronic communication
86I Possession of computer viruses etc with intent to commit serious computer offence

Part 3—Amendment of *Summary Offences Act 1953*

5 Insertion of section 44A
44A Unauthorised impairment of data held in credit card or on computer disk or other device

The Parliament of South Australia enacts as follows:

Part 1—Preliminary

1—Short title

This Act may be cited as the *Statutes Amendment (Computer Offences) Act 2004*.

2—Commencement

This Act will come into operation on a day to be fixed by proclamation.

3—Amendment provisions

In this Act, a provision under a heading referring to the amendment of a specified Act amends the Act so specified.

Part 2—Amendment of *Criminal Law Consolidation Act 1935*

4—Insertion of Part 4A

After section 86A insert:

Part 4A—Computer offences

86B—Interpretation

In this Part—

computer data includes data in any form in which it may be stored or processed in a computer (including a computer program or part of a computer program);

electronic communication means the communication of computer data between computers by means of an electronic communication network;

electronic communication network means devices and systems by which computer data is communicated between computers and includes—

(a) a link or network that operates wholly or partially by wireless communication; and

(b) the world wide web;

impairment of electronic communication includes prevention or delay but does not include interception if the interception does not impair, prevent or delay the reception, at the intended destination, of the computer data that is being communicated;

modification of computer data includes—

(a) deletion or removal of the data;

(b) an alteration of the data;

(c) an addition to the data;

possession of computer data includes possession of the medium or device in which the computer data is stored;

serious computer offence means an offence against section 86E, 86F, 86G or 86H;

serious offence means an offence for which a maximum penalty of life imprisonment or imprisonment for a term of at least 5 years is prescribed;

use—a person uses a computer if the person causes the computer to perform a function.

86C—Meaning of unauthorised access to or modification of computer data

(1) Access to, or modification of, computer data is unauthorised unless it is done or made by the owner of the data or some other person who has an authorisation or licence (express or implied) from the owner of the data to have access or to make the modification.

(2) A person is to be regarded as the owner of computer data if—

(a) the person brought the data into existence or stored the data in the computer for his or her own purposes; or

(b) the data was brought into existence or stored in the computer at the request or on behalf of that person; or

(c) the person has a proprietary interest in, or possessory rights over, the medium in which the computer data is stored entitling the person to determine what data is stored in the medium and in what form.

(3) For the purposes of an offence against this Part, the onus of establishing that access to, or modification of, computer data was unauthorised lies on the prosecution.

86D—Meaning of unauthorised impairment of electronic communication

(1) An impairment of electronic communication is unauthorised unless it is caused by the person who is entitled to control use of the relevant electronic communication network or some other person who has an authorisation or licence (express or implied) from the person who is entitled to control use of the relevant electronic communication network to cause the impairment.

(2) A person is to be regarded as being entitled to control use of the relevant electronic communication network if the person is entitled by law to determine who is to have access to the network for the purpose of sending or receiving electronic communications.

(3) For the purposes of an offence against this Part, the onus of establishing that an impairment of electronic communication was unauthorised lies on the prosecution.

86E—Use of computer with intention to commit, or facilitate the commission of, an offence

(1) A person who—

(a) uses a computer to cause (directly or indirectly)—

(i) unauthorised access to or modification of computer data; or

(ii) an unauthorised impairment of electronic communication; and

(b) knows that the access, modification or impairment is unauthorised; and

(c) intends, by that access, modification or impairment to commit, or to facilitate the commission (either by that person or someone else) of, a serious offence (the ***principal offence***),

is guilty of an offence.

Maximum penalty: The maximum penalty for an attempt to commit the principal offence.

(2) An offence may be committed under this section—

(a) whether the principal offence was to be committed at the time the computer was used or later; and

(b) even though it would have been impossible in the circumstances to commit the principal offence.

(3) If the principal offence is in fact committed—

(a) this section does not prevent the person who used the computer from being convicted as a principal offender or as an accessary to the commission of the principal offence; but

(b) a person is not liable to be convicted of the principal offence (or as an accessory to the principal offence) and of an offence against this section.

(4) A person cannot be convicted of an attempt to commit an offence against this section.

86F—Use of computer to commit, or facilitate the commission of, an offence outside the State

(1) A person who—

(a) uses a computer in this State to cause (directly or indirectly)—

(i) unauthorised access to or modification of computer data; or

(ii) an unauthorised impairment of electronic communication; and

knows that the access, modification or impairment is unauthorised; and

(b) intends, by that access, modification or impairment, to commit, or to facilitate the commission (either by that person or someone else) of, a prohibited act in another jurisdiction (the ***relevant jurisdiction***),

is guilty of an offence.

Maximum penalty: The maximum penalty under the law of this State for an attempt to commit the prohibited act in this State.

(2) A ***prohibited act*** is an act that would—

(a) if committed with intent in the relevant jurisdiction, constitute an offence for which a maximum penalty of life imprisonment or imprisonment for a term of at least 5 years is prescribed; and

(b) if committed with intent in this State, constitute an offence for which a maximum penalty of life imprisonment or imprisonment for a term of at least 5 years is prescribed.

(3) A person may be convicted of an offence against this section—

(a) whether the prohibited act was to be committed at the time of the conduct to which the charge relates or later; and

(b) even though it would have been impossible in the circumstances to commit the prohibited act.

(4) A person cannot be convicted of an attempt to commit an offence against this section.

(5) In this section—

act includes an omission or state of affairs that is (if it occurred in this State) capable of constituting an element of an offence.

86G—Unauthorised modification of computer data

A person who—

(a) causes (directly or indirectly) an unauthorised modification of computer data; and

(b) knows that the modification is unauthorised; and

(c) intends, by that modification, to cause harm or inconvenience by impairing access to, or by impairing the reliability, security or operation of, computer data, or is reckless as to whether such harm or inconvenience will ensue,

is guilty of an offence.

Maximum penalty: Imprisonment for 10 years.

86H—Unauthorised impairment of electronic communication

A person who—

(a) causes (directly or indirectly) an unauthorised impairment of electronic communication; and

(b) knows that the impairment is unauthorised; and

(c) intends, by that impairment, to cause harm or inconvenience, or is reckless as to whether harm or inconvenience will ensue,

is guilty of an offence.

Maximum penalty: Imprisonment for 10 years.

86I—Possession of computer viruses etc with intent to commit serious computer offence

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

(a) produces, supplies or obtains proscribed data or a proscribed object; or

(b) is in possession or control of proscribed data or a proscribed object,

with the intention of committing, or facilitating the commission (either by that person or someone else) of, a serious computer offence.

Maximum penalty: Imprisonment for 3 years.

(2) In this section—

proscribed data means a computer virus or other computer data clearly designed or adapted to enable or facilitate the commission of a serious computer offence;

proscribed object means a document or other object clearly designed or adapted to enable or facilitate the commission of a serious computer offence.

Examples—

1 A disk, card or other data storage device containing a computer virus or other computer data adapted for the commission of a serious computer offence.

2 Instructions (whether in hard copy or electronic form) for carrying out a serious computer offence.

(3) If it is established in proceedings for an offence against this section that the defendant was in control of proscribed data, it is irrelevant—

(a) whether the data is stored inside or outside the State; or

(b) whether the defendant owned or was in possession of the medium or device in which the data was stored.

(4) A person may be convicted of an offence against this section even though it would have been impossible in the circumstances to commit the intended offence.

(5) A person cannot be convicted of an attempt to commit an offence against this section.

Part 3—Amendment of *Summary Offences Act 1953*

5—Insertion of section 44A

After section 44 insert:

44A—Unauthorised impairment of data held in credit card or on computer disk or other device

(1) A person who—

(a) causes (directly or indirectly) an unauthorised impairment of data held in a credit card or on a computer disk or other device used to store data by electronic means; and

(b) knows that the impairment is unauthorised; and

(c) intends, by that impairment, to cause harm or inconvenience, or is reckless as to whether harm or inconvenience will ensue,

is guilty of an offence.

Maximum penalty: Imprisonment for 2 years.

(2) An impairment of data is unauthorised unless it is made by the owner of the data or some other person who has an authorisation or licence (express or implied) from the owner of the data to cause the impairment.

(3) A person is to be regarded as the owner of data if—

(a) the person brought the data into existence or stored the data in the credit card or on the computer disk or other device for his or her own purposes; or

(b) the data was brought into existence or stored in the credit card or on the computer disk or other device at the request or on behalf of that person; or

(c) the person has a proprietary interest in, or possessory rights over, the medium in which the data is stored entitling the person to determine what data is stored in the medium and in what form.

(4) The onus of establishing that an impairment of data was unauthorised lies on the prosecution.