Cybercrime Act 2001

Act No. 161 of 2001 as amended

This compilation was prepared on 6 September 2004

[This Act was amended by Act No. 127 of 2004]

Amendments from Act No. 127 of 2004

[Schedule 5 (item 9) amended Schedule 1
Schedule 5 (item 9) commenced on 21 December 2001]

Prepared by the Office of Legislative Drafting,
Attorney-General's Department, Canberra

Contents

An Act to amend the law relating to computer offences, and for other purposes

[*Assented to 1 October 2001*]

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *Cybercrime Act 2001*.

2 Commencement

(1) Subject to subsection (2), this Act commences on a day to be fixed by Proclamation.

(2) If this Act does not commence under subsection (1) within the period of 6 months beginning on the day on which it receives the Royal Assent, it commences on the first day after the end of that period.

3 Schedule(s)

Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

4 Application—*Criminal Code* amendments

(1) The amendments of the *Criminal Code* made by Schedule 1 apply to conduct that takes place after that Schedule commences.

(2) For the purposes of this section, if conduct is alleged to have taken place between 2 dates, one before and one on or after the day on which Schedule 1 commences, the conduct is alleged to have taken place before Schedule 1 commences.

Schedule 1—Computer offences

Australian Security Intelligence Organisation Act 1979

1 Subsection 25A(4) (note)

Omit "section 76D or 76E of the *Crimes Act 1914*", substitute "Part 10-7 of the *Criminal Code*".

Crimes Act 1914

2 Part VIA

Repeal the Part.

Criminal Code Act 1995

3 The Schedule (paragraphs 4.1(1)(b) and (c) of the *Criminal Code*)

Repeal the paragraphs, substitute:

(b) a result of conduct; or

(c) a circumstance in which conduct, or a result of conduct, occurs.

4 The Schedule (before the Dictionary in the *Criminal Code*)

Insert:

Part 10.7—Computer offences

Division 476—Preliminary

476.1 Definitions

(1) In this Part:

access to data held in a computer means:

(a) the display of the data by the computer or any other output of the data from the computer; or

(b) the copying or moving of the data to any other place in the computer or to a data storage device; or

(c) in the case of a program—the execution of the program.

Commonwealth computer means a computer owned, leased or operated by a Commonwealth entity.

data includes:

(a) information in any form; or

(b) any program (or part of a program).

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

data storage device means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.

electronic communication means a communication of information in any form by means of guided or unguided electromagnetic energy.

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication; or

(b) the impairment of any such communication on an electronic link or network used by the computer;

but does not include a mere interception of any such communication.

modification, in respect of data held in a computer, means:

(a) the alteration or removal of the data; or

(b) an addition to the data.

telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both.

unauthorised access, modification or impairment has the meaning given in section 476.2.

(2) In this Part, a reference to:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer;

is limited to such access, modification or impairment caused, whether directly or indirectly, by the execution of a function of a computer.

476.2 Meaning of *unauthorised access, modification or impairment*

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it.

(4) For the purposes of subsection (1), if:

(a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and

(b) the person does so under a warrant issued under the law of the Commonwealth, a State or a Territory;

the person is entitled to cause that access, modification or impairment.

476.3 Geographical jurisdiction

Section 15.1 (extended geographical jurisdiction—Category A) applies to offences under this Part.

476.4 Saving of other laws

(1) This Part is not intended to exclude or limit the operation of any other law of the Commonwealth, a State or a Territory.

(2) Subsection (1) has effect subject to section 476.5.

476.5 Liability for certain acts

(1) A staff member or agent of ASIS or DSD (the ***agency***) is not subject to any civil or criminal liability for any computer-related act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the act:

(i) taken together with a computer-related act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that computer-related act, event, circumstance or result, would not amount to an offence; and

(c) the act is done in the proper performance of a function of the agency.

(2A) Subsection (2) is not intended to permit any act in relation to premises, persons, computers, things, or telecommunications services in Australia, being:

(a) an act that ASIO could not do without a Minister authorising it by warrant issued under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part III of the *Telecommunications (Interception) Act 1979*; or

(b) an act to obtain information that ASIO could not obtain other than in accordance with section 283 of the *Telecommunications Act 1997*.

(2B) The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act was done in the proper performance of a function of an agency.

(2C) In any proceedings, a certificate given under subsection (2B) is prima facie evidence of the facts certified.

(3) In this section:

ASIS means the Australian Secret Intelligence Service.

civil or criminal liability means any civil or criminal liability (whether under this Part, under another law or otherwise).

computer-related act, event, circumstance or result means an act, event, circumstance or result involving:

(a) the reliability, security or operation of a computer; or

(b) access to, or modification of, data held in a computer or on a data storage device; or

(c) electronic communication to or from a computer; or

(d) the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or

(e) possession or control of data held in a computer or on a data storage device; or

(f) producing, supplying or obtaining data held in a computer or on a data storage device.

DSD means that part of the Department of Defence known as the Defence Signals Directorate.

staff member means:

(a) in relation to ASIS—the Director-General of ASIS or a member of the staff of ASIS (whether an employee of ASIS, a consultant to ASIS, or a person who is made available by another Commonwealth or State authority or other person to perform services for ASIS); and

(b) in relation to DSD—the Director of DSD or a member of the staff of DSD (whether an employee of DSD, a consultant to DSD, or a person who is made available by another Commonwealth or State authority or other person to perform services for DSD).

Division 477—Serious computer offences

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

Intention to commit a serious Commonwealth, State or Territory offence

(1) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a telecommunications service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

(2) Absolute liability applies to paragraph (1)(b).

(3) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth, a State or a Territory; or

(b) a serious offence.

Intention to commit a serious Commonwealth offence

(4) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

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

(c) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth (whether by that person or another person) by the access, modification or impairment.

(5) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth; or

(b) a serious offence.

Penalty

(6) A person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence.

Impossibility

(7) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

No offence of attempt

(8) It is not an offence to attempt to commit an offence against this section.

*Meaning of **serious offence***

(9) In this section:

serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years.

477.2 Unauthorised modification of data to cause impairment

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised modification of data held in a computer; and

(b) the person knows the modification is unauthorised; and

(c) the person is reckless as to whether the modification impairs or will impair:

(i) access to that or any other data held in any computer; or

(ii) the reliability, security or operation, of any such data; and

(d) one or more of the following applies:

(i) the data that is modified is held in a Commonwealth computer;

(ii) the data that is modified is held on behalf of the Commonwealth in a computer;

(iii) the modification of the data is caused by means of a telecommunications service;

(iv) the modification of the data is caused by means of a Commonwealth computer;

(v) the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer;

(vi) the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer;

(vii) the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a telecommunications service.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:
   (a) access to data held in a computer; or
   (b) the reliability, security or operation, of any such data.

(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3 (unauthorised impairment of electronic communication).

477.3 Unauthorised impairment of electronic communication

(1) A person is guilty of an offence if:
   (a) the person causes any unauthorised impairment of electronic communication to or from a computer; and
   (b) the person knows that the impairment is unauthorised; and
   (c) one or both of the following applies:
      (i) the electronic communication is sent to or from the computer by means of a telecommunications service;
      (ii) the electronic communication is sent to or from a Commonwealth computer.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(c).

(3) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.2 (unauthorised modification of data to cause impairment).

Division 478—Other computer offences

478.1 Unauthorised access to, or modification of, restricted data

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modification of, restricted data; and

(b) the person intends to cause the access or modification; and

(c) the person knows that the access or modification is unauthorised; and

(d) one or more of the following applies:

(i) the restricted data is held in a Commonwealth computer;

(ii) the restricted data is held on behalf of the Commonwealth;

(iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) In this section:

restricted data means data:

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

478.2 Unauthorised impairment of data held on a computer disk etc.

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on:

(i) a computer disk; or

(ii) a credit card; or

(iii) another device used to store data by electronic means; and

(b) the person intends to cause the impairment; and

(c) the person knows that the impairment is unauthorised; and

(d) the computer disk, credit card or other device is owned or leased by a Commonwealth entity.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

478.3 Possession or control of data with intent to commit a computer offence

(1) A person is guilty of an offence if:

(a) the person has possession or control of data; and

(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of possession or control of data

(4) In this section, a reference to a person having possession or control of data includes a reference to the person:

(a) having possession of a computer or data storage device that holds or contains the data; or

(b) having possession of a document in which the data is recorded; or

(c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia).

478.4 Producing, supplying or obtaining data with intent to commit a computer offence

(1) A person is guilty of an offence if:

(a) the person produces, supplies or obtains data; and

(b) the person does so with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of producing, supplying or obtaining data

(4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person:

(a) producing, supplying or obtaining data held or contained in a computer or data storage device; or

(b) producing, supplying or obtaining a document in which the data is recorded.

Education Services for Overseas Students Act 2000

5 Subsection 109(5) (note 2)

Repeal the note, substitute:

Note 2: A person who obtains unauthorised access to information on the system that is protected by an access control system could be guilty of an offence against Part 10-7 of the *Criminal Code*.

Telecommunications (Interception) Act 1979

6 Subsection 5D(5)

Omit "Part VIA of the *Crimes Act 1914*", substitute "Part 10-7 of the *Criminal Code*".

Note: The heading to subsection 5D(5) is altered by omitting "*Part VIA of the Crimes Act 1914*" and substituting "*Part 10-7 of the Criminal Code*".

Schedule 2—Law enforcement powers relating to electronically stored data

Crimes Act 1914

1 Subsection 3C(1)

Insert:

data includes:

(a) information in any form; or

(b) any program (or part of a program).

2 Subsection 3C(1)

Insert:

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

3 Subsection 3C(1)

Insert:

data storage device means a thing containing, or designed to contain, data for use by a computer.

4 Subsection 3K(1)

Omit "things found at the premises in order to determine whether they are things", substitute "a thing found at the premises in order to determine whether it is a thing".

5 Subsection 3K(2)

Repeal the subsection, substitute:

(2) A thing found at the premises may be moved to another place for examination or processing in order to determine whether it may be seized under a warrant if:

(a) both of the following apply:

(i) it is significantly more practicable to do so having regard to the timeliness and cost of examining or processing the thing at another place and the availability of expert assistance;

(ii) there are reasonable grounds to believe that the thing contains or constitutes evidential material; or

(b) the occupier of the premises consents in writing.

6 Subsection 3K(3)

Omit "things are", substitute "a thing is".

7 After subsection 3K(3)

Insert:

(3A) The thing may be moved to another place for examination or processing for no longer than 72 hours.

(3B) An executing officer may apply to an issuing officer for one or more extensions of that time if the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 72 hours or that time as previously extended.

(3C) The executing officer must give notice of the application to the occupier of the premises, and the occupier is entitled to be heard in relation to the application.

8 Subsection 3L(1)

Repeal the subsection, substitute:

(1) The executing officer or a constable assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:

(a) the data might constitute evidential material; and

(b) the equipment can be operated without damaging it.

Note: An executing officer can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 3LA.

(1A) If the executing officer or constable assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:

(a) copy the data to a disk, tape or other associated device brought to the premises; or

(b) if the occupier of the premises agrees in writing—copy the data to a disk, tape or other associated device at the premises;

and take the device from the premises.

(1B) If:

(a) the executing officer or constable assisting takes the device from the premises; and

(b) the Commissioner is satisfied that the data is not required (or is no longer required) for:

(i) investigating an offence against the law of the Commonwealth, a State or a Territory; or

(ii) judicial proceedings or administrative review proceedings; or

(iii) investigating or resolving a complaint under the *Complaints (Australian Federal Police) Act 1981* or the *Privacy Act 1988*;

the Commissioner must arrange for:

(c) the removal of the data from any device in the control of the Australian Federal Police; and

(d) the destruction of any other reproduction of the data in the control of the Australian Federal Police.

9 Paragraph 3L(2)(b)

Omit "or".

10 Paragraph 3L(2)(c)

Repeal the paragraph.

11 Paragraph 3L(3)(a)

Repeal the paragraph, substitute:

(a) it is not practicable to copy the data as mentioned in subsection (1A) or to put the material in documentary form as mentioned in paragraph (2)(b); or

12 After section 3L

Insert:

3LA Person with knowledge of a computer or a computer system to assist access etc.

(1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on warrant premises;

(b) copy the data to a data storage device;

(c) convert the data into documentary form.

(2) The magistrate may grant the order if the magistrate is satisfied that:

(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and

(b) the specified person is:

(i) reasonably suspected of having committed the offence stated in the relevant warrant; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms a part; or

(ii) measures applied to protect data held in, or accessible from, the computer.

(3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment.

3LB Accessing data held on other premises—notification to occupier of that premises

(1) If:

(a) data that is held on premises other than the warrant premises is accessed under subsection 3L(1); and

(b) it is practicable to notify the occupier of the other premises that the data has been accessed under a warrant;

the executing officer must:

(c) do so as soon as practicable; and

(d) if the executing officer has arranged, or intends to arrange, for continued access to the data under subsection 3L(1A) or (2)—include that information in the notification.

(2) A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer.

13 Paragraph 3N(2)(a)

Omit "paragraph 3L(2)(b) or (c)", substitute "subsection 3L(1A) or paragraph 3L(2)(b)".

Customs Act 1901

14 Subsection 4(1)

Insert:

data includes:

(a) information in any form; or

(b) any program (or part of a program).

15 Paragraph 67EU(1)(b)

Omit "or programs associated with its use are damaged or corrupted".

16 Subsection 67EU(1)

Omit "compensation for the damage or corruption is payable by Customs to the owner of the equipment or the user of the data or programs concerned", substitute "compensation for the damage is payable by Customs to the owner of the equipment or the user of the data concerned".

17 Subsection 67EU(3)

Omit "or program".

18 Subsection 183UA(1)

Insert:

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

19 Subsection 183UA(1)

Insert:

data storage device means a thing containing, or designed to contain, data for use by a computer.

20 Subsection 200(1)

Omit "things found on or in the premises in order to determine whether they are things", substitute "a thing found on or in the premises in order to determine whether it is a thing".

21 Subsection 200(2)

Repeal the subsection, substitute:

(2) A thing found at the premises may be moved to another place for examination or processing in order to determine whether it may be seized under a warrant if:

(a) both of the following apply:

(i) it is significantly more practicable to do so having regard to the timeliness and cost of examining or

processing the thing at another place and the availability of expert assistance;

(ii) there are reasonable grounds to believe that the thing contains or constitutes evidential material; or

(b) the occupier of the premises consents in writing.

22 Subsection 200(3)

Omit "things are", substitute "a thing is".

23 After subsection 200(3)

Insert:

(3A) The thing may be moved to another place for examination or processing for no longer than 72 hours.

(3B) An executing officer may apply to a judicial officer for one or more extensions of that time if the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 72 hours or that time as previously extended.

(3C) The executing officer must give notice of the application to the occupier of the premises, and the occupier is entitled to be heard in relation to the application.

24 Subsection 201(1)

Repeal the subsection, substitute:

(1) The executing officer or a person assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:

(a) the data might constitute evidential material; and

(b) the equipment can be operated without damaging it.

Note: An executing officer can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 201A.

(1A) If the executing officer or person assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:

(a) copy the data to a disk, tape or other associated device brought to the premises; or

(b) if the occupier of the premises agrees in writing—copy the data to a disk, tape or other associated device at the premises;

and take the device from the premises.

(1B) If:

(a) the executing officer or person assisting takes the device from the premises; and

(b) the CEO is satisfied that the data is not required (or is no longer required) for:

(i) investigating an offence against the law of the Commonwealth, a State or a Territory; or

(ii) judicial proceedings or administrative review proceedings; or

(iii) investigating or resolving a complaint under the *Ombudsman Act 1976* or the *Privacy Act 1988*;

the CEO must arrange for:

(c) the removal of the data from any device in the control of Customs; and

(d) the destruction of any other reproduction of the data in the control of Customs.

25 Paragraph 201(2)(b)

Omit "so produced; or", substitute "so produced.".

26 Paragraph 201(2)(c)

Repeal the paragraph.

27 Subsection 201(3)

Omit "put the material in documentary form as mentioned in paragraph (2)(b) or to copy the material as mentioned in paragraph (2)(c)", substitute "copy the material as mentioned in subsection (1A) or to put the material in documentary form as mentioned in paragraph (2)(b)".

28 After section 201

Insert:

201A Person with knowledge of a computer or a computer system to assist access etc.

(1) An executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on warrant premises;

(b) copy the data to a data storage device;

(c) convert the data into documentary form.

(2) The magistrate may grant the order if the magistrate is satisfied that:

(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and

(b) the specified person is:

(i) reasonably suspected of having committed the offence stated in the relevant warrant; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms a part; or

(ii) measures applied to protect data held in, or accessible from, the computer.

(3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment.

201B Accessing data held on other premises—notification to occupier of that premises

(1) If:

(a) data that is held on premises other than the warrant premises is accessed under subsection 201(1); and

(b) it is practicable to notify the occupier of the other premises that the data has been accessed under a warrant;

the executing officer must:

(c) do so as soon as practicable; and

(d) if the executing officer has arranged, or intends to arrange, for continued access to the data under subsection 201(1A) or (2)—include that information in the notification.

(2) A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer.

29 Subsection 202(1)

Repeal the subsection, substitute:

(1) If:

(a) damage is caused to equipment as a result of it being operated as mentioned in section 200 or 201; or

(b) the data recorded on or accessible from the equipment is damaged;

and the damage was caused as a result of:

(c) insufficient care being exercised in selecting the person who was to operate the equipment; or

(d) insufficient care being exercised by the person operating the equipment;

compensation for the damage is payable to the owner of the equipment or the user of the data concerned.

30 Paragraph 202A(2)(a)

Omit "paragraph 201(2)(b) or (c)", substitute "subsection 201(1A) or paragraph 201(2)(b)".

31 Application of amendments

The amendments made by this Schedule apply to warrants issued after the commencement of this Schedule.

[*Minister's second reading speech made in—*

(129/01)

House of Representatives on 27 June 2001
Senate on 26 September 2001]