The Parliament of the Commonwealth of Australia

Senate Legal and Constitutional Legislation Committee

Consideration of legislation referred to the Committee

Inquiry into the Provisions of the Cybercrime Bill 2001

AUGUST 2001

ISSN 1326-9364

This document was produced from camera-ready copy prepared by the Senate Legal and Constitutional Legislation Committee, and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Members of the Legislation Committee

Members

Senator M Payne **(Chair)** LP
Senator J McKiernan **(Deputy Chair)** ALP
Senator H Coonan LP
Senator B Cooney ALP
Senator B Mason LP
Senator B Greig AD

Participating Members

Senator A Bartlett
Senator B Brown
Senator G Chapman
Senator A Eggleston
Senator A Ferguson
Senator M Forshaw
Senator B Harradine
Senator S Knowles
Senator J. Ludwig
Senator N Stott Despoja
Senator J Tierney
Senator the Hon N Bolkus
Senator P Calvert
Senator W Crane
Senator the Hon. J Faulkner
Senator J Ferris
Senator the Hon. B Gibson
Senator L Harris
Senator R Lightfoot
Senator J McGauran
Senator T Tchen
Senator J Watson

Secretariat

Dr Pauline Moore (Secretary to the Committee)
Mr Peter Gibson (Principal Research Officer)
Ms Christine Wilson (Executive Assistant)

PARLIAMENT HOUSE
CANBERRA ACT 2600
Tel: (02) 6277 3560 Fax: (02) 6277 5794

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Background

1.1 The *Cybercrime Bill 2001* ('the Bill") was introduced into the House of Representatives on 27 June 2001.

1.2 On 28 June 2001, the Senate Selection of Bills Committee[1] referred the provisions of the Bill to the Legal and Constitutional Legislation Committee ("the Committee") for inquiry and report by 21 August 2001. The Senate agreed to this reference.

Purpose of the Bill

1.3 The Bill proposes to amend the *Criminal Code Act 1995* (Criminal Code) by enacting new computer offences. The new offences have been based on the recommendations of the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (SCAG) in their Report *Damage and Computer Offences*[2] and are consistent with the terms of the draft Council of Europe Convention on Cybercrime. The Standing Committee of Attorneys-General has agreed to give priority to the enactment of updated computer offences. New South Wales has already enacted the *Crimes Amendment (Computer Offences) Act 2001* based on the Model Criminal Code.

1.4 The Explanatory Memorandum states that the effectiveness of existing computer offences, which were inserted into the *Crimes Act 1914* in 1989, has been reduced with the emergence and expansion of new technologies. Current provisions do not sufficiently address the impairment of electronic communications, damage to electronic data stored on devices such as computer disks or credit cards, or the unauthorised use of a computer to commit another offence.[3]

1.5 The Explanatory Memorandum states that the proposed computer offences are directed at conduct that impairs the security, integrity and reliability of computer data and electronic communications. Advances in computer technology and electronic communications have created new means and possibilities for committing cybercrime such as hacking, denial of service attacks and virus propagation. The proposed offences are designed to address these new forms of cybercrime and to remedy the deficiencies in the existing offences.[4]

---

1 Selection of Bills Committee, *Report, No. 10* of 2001

2 Model Criminal Code, Damage and Computer Offences (January 2001)

3 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 4

4 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 4

Provisions of the Bill

1.6 Proposed section 3 provides for the amendment of various Acts specified in Schedules 1 and 2 including the repeal of the existing computer offences in Part VIA of the *Crimes Act 1914*.

1.7 The proposed new computer offences will be inserted as Part 10.7 of the *Criminal Code Act 1995*.

Definitions

1.8 The definitions, which are contained in proposed section 476.1 of Part 10.7 of the Criminal Code are, with the exception of "Commonwealth computer" and "telecommunications service", based on the definitions proposed in the Model Criminal Code *Damages and Computer Offences Report* (sections 4.2.1 and 4.2.2, pages 120-147).[5]

1.9 As outlined in the Explanatory Memorandum, the definitions for the terms are as follows:[6]

> **Access to data held in a computer** is defined to mean the display of data by the computer or any other output of the data from the computer, such as the printing of data; the copying or moving of data to another place in the computer or to a device designed to contain data for use by a computer or, in the case of a computer program, the execution of that program. This is more explicit than existing Australian legislation but avoids the complexity of the UK *Computer Misuse Act 1990*. Access is not a clear concept in the context of computers and warrants definition in a Criminal Code.
>
> **Commonwealth computer** is defined to mean a computer owned, leased or operated by the Commonwealth or a Commonwealth authority. This follows the approach of the existing Commonwealth provisions by partly anchoring jurisdiction to Commonwealth computers (see section 76A, *Crimes Act 1914*).
>
> **Data** includes information in any form or any program or part of a program. This follows the Model Criminal Code, but does not vary in substance from the existing definition.
>
> **Data held in a computer** includes data held in any removable data storage device, such as a computer disk, or any data held in a data storage device on a computer network of which the computer forms a part.
>
> **Data storage device** is defined to mean a thing, such as a disk or file server, that contains, or is designed to contain, data for use by a computer. This definition is consistent with the *Electronic Transactions Act 1999*.
>
> **Electronic communication** is defined to mean a communication of information in any form by means of guided or unguided electronic energy. This definition is consistent with the *Electronic Transactions Act 1999*.

---

5 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 4

6 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 4

Impairment of electronic communication to or from a computer includes the prevention of any electronic communication or the impairment of any electronic communication on an electronic link or network used by the computer, but does not include a mere interception of an electronic communication.

Modification of data held in a computer is defined to mean the alteration or removal of data or an addition to the data.

Telecommunications service is defined to mean a service for carrying communications by means of guided or unguided electromagnetic energy or both. This definition is consistent with the terminology of the *Telecommunications Act 1997*.

Unauthorised access, modification or impairment is defined in proposed section 476.2.

1.10 Proposed subsection 476.1(2) limits the scope of the terms "access to data held in a computer", "modification of data held in a computer" and "impairment of electronic communications to or from a computer". Where these terms are used in the proposed computer offences they refer to any such access, modification or impairment caused by the execution of a function of a computer. Any such access, modification or impairment effected otherwise than by the execution of a function of a computer, for example, by causing physical damage to computer hardware, is not within the scope of the proposed offences. The description of an offender's conduct as "causing a computer to execute a function" ensures that the offences extend beyond obvious cases in which an offender uses a keyboard or other direct physical means to commit an offence, to cover offenders, such as those who put a virus infected disk into circulation, who cannot be described as "using a computer" in the usual sense. [7]

1.11 "Computer" has not been defined in order to ensure the proposed computer offences will encompass new developments in technology which may perform all the functions of a computer and which may not be covered by a restrictive definition.[8]

1.12 Proposed section 476.2, which is based on section 4.2.2 of the Model Criminal Code,[9] defines unauthorised access, modification and impairment.

1.13 Proposed subsection 476.2(1) provides that where a person causes:

(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 in a computer disk, credit card or other device used to store data by electronic means,

---

7 Explanatory Memorandum, *Cybercrime Bill 2001*, pp. 5-6

8 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 5

9 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 6

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

1.14 Proposed subsection 476.2(2) provides that any such access, modification or impairment is not unauthorised merely because the person causes the access, modification or impairment for a purpose other than that for which they are entitled to cause access, modification or impairment.

1.15 Proposed subsection 476.2(3) specifies that, for the purposes of the proposed Part, a person causes access to data held in a computer, modification of data held in a computer, impairment of electronic communications to or from a computer or impairment of data on a disk etc if the person's conduct substantially contributes to the access, modification or impairment.

Geographical jurisdiction

1.16 Proposed section 476.3 applies Category A geographical jurisdiction, as set out in section 15.1 of the Criminal Code, to the proposed computer offences. This means that the offences would extend to situations where

a) the conduct constituting the offence occurs partly in Australia or on board an Australian ship or aircraft;

b) the result of the conduct constituting the offence occurs partly in Australia or on board an Australian ship or aircraft; or

c) the person committing the offence is an Australian citizen or an Australian company.

1.17 The Explanatory Memorandum states that this approach is broadly consistent with the draft Council of Europe Convention on Cybercrime, which recommends that parties to the convention establish jurisdiction over offences committed on board their ships or aircraft or by one of their nationals (Draft No 25, Article23). It is also consistent with the Model Criminal Code which, although a model State and Territory code, also includes broad geographical jurisdiction for these offences.[10]

1.18 As explained in the Explanatory Memorandum, the application of Category A jurisdiction would mean that, regardless of where conduct constituting an offence occurs, if the results of that conduct affects Australia, the person responsible would generally be able to be prosecuted in Australia. An Australian citizen who travels to a country where hacking is not an offence and, while there, uses a laptop computer to hack into a computer in a third country, would also be caught by the proposed jurisdiction.[11]

Saving of other laws

1.19 Proposed section 476.4 provides for the concurrent operation of Commonwealth, State and Territory laws. This ensures that there are no gaps in jurisdiction and also allows computer crimes to be prosecuted in whatever forum is most convenient.

---

10 Explanatory Memorandum, *Cybercrime Bill 2001*, pp. 6-7

11 Explanatory Memorandum, *Cybercrime Bill 2001*, pp. 7

1.20 The Explanatory Memorandum states that State and Territory computer offences would cover computer crime activities committed by employees using an internal computer network. As computer crime on internal computer networks does not involve use of the telecommunications system the Commonwealth cannot regulate this conduct.[12]

Liability for certain acts

1.21 Proposed section 476.5 provides limited immunity from civil and criminal liability for staff or agencies whose activities, in the proper performance of their functions, are intended and required by Government. These activities might otherwise be prohibited by Australian laws dealing with computer-related acts.[13]

Serious computer offences

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

1.22 Proposed section 477.1 would make it an offence to cause any unauthorised access to data held in a computer, any unauthorised modification of data held in a computer or any unauthorised impairment of electronic communications to or from a computer, knowing the access, modification or impairment is unauthorised and with the intention of committing or facilitating the commission of a serious offence. The offence is based on section 4.2.4 of the Model Criminal Code.[14]

1.23 Subsection 477.1(9) defines a serious offence to be 'an offence that is punishable by imprisonment for life or a period of 5 or more years."

1.24 Proposed subsection 477.1(6) provides that an offence would carry a maximum penalty equal to the maximum penalty for the serious offence the person is intending to commit.

1.25 As paragraph 477.1(1)(a) does not specify the fault elements that apply to a person's conduct or the result of that conduct, then default elements set out in section 5.6 of the Criminal Code would apply. This means that the offence requires intention to do an act, which causes unauthorised access, modification or impairment, and recklessness as to whether the act will cause that access, modification or impairment.[15]

1.26 The Explanatory Memorandum states that where the unauthorised access, modification or impairment is caused by means of a telecommunications service, the offence would apply whether the serious offence the person intends to commit is a Commonwealth, State or Territory offence. In all other cases, the offence would apply only where the serious offence the person intends to commit is a Commonwealth offence. In establishing that a person has committed this offence it would not be necessary for the prosecution to prove that the defendant knew the offence he or she was intending to commit was an offence against the law of the Commonwealth, a State or a Territory or that he or she knew that the offence is

12 Explanatory Memorandum, *Cybercrime Bill 2001*, pp. 7

13 Explanatory Memorandum, *Cybercrime Bill 2001*, pp. 7

14 See pp 148-155 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

15 Explanatory Memorandum, *Cybercrime Bill 2001*, pp. 7-8

punishable by imprisonment for life or a period of 5 or more years. This is consistent with recently enacted Criminal Code offences (eg, section 132.4, which concerns burglary). It is not appropriate to require the prosecution to prove jurisdictional elements of offences in these circumstances.[16]

1.27 The proposed offence is designed to cover the unauthorised use of computer technology to commit serious crimes such as fraud or stalking. The offence is particularly targeted at situations where preparatory action is taken by a person but the intended offence is not completed.

Unauthorised modification of data to cause impairment

1.28 Proposed section 477.2 makes it an offence for a person to cause any unauthorised modification of data held in a computer, where the person knows that the modification is unauthorised, and intends by that modification to impair access to, or the reliability, security or operation of, any data held in a computer or is reckless as to any such impairment. The offence is based on section 4.2.5 of the Model Criminal Code.[17] The maximum penalty of 10 years imprisonment for the offence is equivalent to the penalty for the existing computer offences under the *Crimes Act 1914* (paragraphs 76C(a) and 76E(a)) and the penalty for fraud and forgery offences in the Criminal Code.[18]

1.29 The offence would only be committed where one or more of the Commonwealth jurisdictional connections set out in proposed paragraph 477.2(1)(d) applies. Absolute liability would apply to the jurisdictional connections. This obviates the need for the prosecution to prove, for example, that a defendant knew the computer data he or she was modifying was owned, leased or operated by the Commonwealth.

1.30 The elements in paragraph 477.2(1)(d) are included merely to trigger Commonwealth jurisdiction and do not have any bearing on the gravity of the offence.

1.31 The proposed offence is limited to instances where a person modifying computer data intends to impair data or is reckless as to causing impairment.

Unauthorised impairment of electronic communication

1.32 Proposed section 477.3 makes it an offence for a person to cause unauthorised impairment of electronic communication to or from a computer, where the person knows that impairment is unauthorised, and either intends to impair electronic communication or is reckless as to any impairment. The offence is based on section 4.2.6 of the Model Criminal Code.[19] The maximum penalty of 10 years imprisonment for the offence recognises the

16 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 8

17 See pp. 156-169 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

18 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 8

19 See pp 170-173 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

importance of reliable computer-facilitated communication and the considerable damage that can result if that communication is impaired.[20]

1.33 The offence would only be committed where the electronic communication that is impaired occurs by means of a telecommunication service from a Commonwealth computer. Absolute liability would apply to these Commonwealth jurisdictional connections.

1.34 Subsection 6.2(2) of the Criminal Code provides that if a law that creates an offence provides that absolute liability applies to a particular physical element of the offence (eg, the electronic communication is sent to or from a Commonwealth computer), then a fault element (eg, knowledge) does not have to be proved and there is no defence of mistake of fact.

1.35 This proposed offence is designed to target tactics such as 'denial of service attacks', where an e-mail address or web site is inundated with a large volume of unwanted messages, thus overloading the computer system and disrupting, impeding or preventing its functioning.

Other computer offences

Unauthorised access to, or modification of, restricted data

1.36 Proposed 478.1 makes it an offence for a person to cause unauthorised access to, or modification of, restricted data held in a computer, where the person intends to cause the access or modification and knows that the access or modification is unauthorised. The offence is based on the Model Criminal Code summary offence of "Unauthorised access to, or modification of, restricted data".[21]

1.37 The offence would only be committed where one or more of the Commonwealth jurisdictional connections set out in proposed paragraph 478.1(d) applies. Absolute liability would apply to the jurisdictional connections.[22]

1.38 The proposed offence relates only to unauthorised access or modification of *restricted data* rather than any data. 'Restricted data' is defined as "data held on a computer to which access is restricted by an access control system associated with a function of the computer". This means a person would only commit an offence if he or she by-passed an access control system, such as a password or other security feature.

Unauthorised impairment of data held in a computer disk etc

1.39 Proposed section 478.2 makes it an offence for a person to cause any unauthorised 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, where the person intends to cause the impairment and knows that the impairment is unauthorised. The offence is based on the Model Criminal Code summary offence of "Unauthorised impairment of data".[23]

---

20 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 9

21 See pp. 186-197 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

22 Subsection 6.2(2) of the Criminal Code also applies to this offence. See paragraph 1.34 above

23 See pp. 198-199 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

1.40 There is currently no equivalent offence, as the existing *Crimes Act 1914* offences pertain only to data stored in a computer, and do not extend to electronic data held in other devices.

1.41 The offence would only be committed where the computer disk, credit card or other device is owned or leased by the Commonwealth or a Commonwealth authority. Absolute liability would apply to this element of the offence.[24]

1.42 This offence is a counterpart to the more serious proposed offence of unauthorised modification of data to cause impairment in proposed section 477.2. There are important differences between the two offences. First, this lesser offence applies to data stored electronically on disks, credit cards, tokens or tickets, while the proposed 477.2 offence applies to 'data held in a computer'. Second, the section 477.2 offence requires that modification of data be caused by the execution of a computer function, whereas this offence is designed to cover impairment of data caused by other means such as passing a magnet over a credit card.

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

1.43 Proposed section 478.3 makes it an offence for a person to possess or control data with the intention of committing or facilitating the commission of an offence against proposed section 477.1, 477.2 or 477.3 by that person or another person. The offence is based on section 4.2.7 of the Model Criminal Code.[25] This offence and the offence in proposed section 478.4 are intended to match the requirements of the draft Council of Europe Convention on Cybercrime.[26]

1.44 This offence is designed to cover persons who intend to hack into other people's computer systems or impair data or electronic communication and who possess or control programs or technology designed for these purposes.

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

1.45 Proposed section 478.4 makes it an offence to produce, supply or obtain data with the intention of committing or facilitating a computer offence by that person or another person. The offence is based on section 4.2.8 of the Model Criminal Code.[27]

1.46 The proposed offence is similar in application to the offence in proposed section 478.3. However, this offence is primarily targeted at those who devise, propagate or publish programs which are intended for use in the communication of an offence against proposed section 477.1, 477.2 or 477.3, whereas the offence in proposed section 478.3 is targeted at those who have such programs in their possession or control.

---

24 Subsection 6.2(2) of the Criminal Code also applies to this offence. See paragraph 1.34 above

25 See pp. 174-181 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

26 Council of Europe Convention on Cybercrime, Draft No.25, Article 6

27 See pp. 182-185 of the Model Criminal Code *Damages and Computer Offences Report* for further discussion

Law enforcement powers relating to electronically stored data

1.47 The Bill proposes to amend the investigation powers in the *Crimes Act 1914* and the *Customs Act 1901* that relate to the search and seizure of electronically stored data. Search powers need to be updated in light of recent developments in technology. Existing search powers, for example, do not enable law enforcement agencies to require a person with knowledge of a relevant computer system to assist investigators to access encrypted information or to gain access to information secured by passwords. The proposed enhancement of search and seizure powers will assist law enforcement officers in overcoming these problems. The proposed amendments bring the investigation powers up to date with aspects of the draft Council of Europe Convention on Cybercrime.[28]

Crimes Act 1914

Use of equipment to examine or process things

1.48 The existing subsection 3K(2) of the *Crimes Act 1914* only permits things at the warrant premises to be moved to another place to be examined or processed if it is not practicable to do so at the premises (or if the occupier of the premises consents). This provision reflects the difficulties involved in moving computers at the time it was enacted. This is no longer the case, with computers becoming increasingly portable.

1.49 The proposed amendment to subsection 3K(2) would allow a thing to be moved from the search premises to another place for examination or processing, with or without the occupier's consent, where it is significantly more practicable than processing the thing at the premises and where there are reasonable grounds to believe that the thing contains or constitutes evidential material. Proposed subparagraph 3K(2)(a)(i) provides that, in determining whether it is significantly more practicable to process or examine the thing at another place, the executing officer or constable assisting must have regard to the timeliness and cost of processing or examining the thing at another place rather than on site and to the availability of expert assistance.

Time limit

1.50 Proposed subsection 3K(3A) provides that a thing that is moved to another place for examination and processing under proposed subsection 3K(2) may only be moved to that place for up to 72 hours. Proposed subsection 3K(3B) provides that the officer responsible for executing the search warrant may apply to an issuing officer for an extension of the 72 hour time period if he or she believes on reasonable grounds that the thing cannot be examined or processed within 72 hours. Proposed subsection 3K(3C) provides that the executing officer must give notice of the application for a extension of time to the occupier of the warrant premises and that the occupier is entitled to be heard by the issuing officer in relation to that application.

Use of electronic equipment at premises

1.51 Proposed subsection 3L(1) would clarify that the existing power to operate electronic equipment on premises to find evidential material includes material physically located away from the premises. An executing officer or constable assisting would be able to

28 Explanatory Memorandum, *Cybercrime Bill 2001*, p. 14

use a computer on search premises to access data held on other computers situated elsewhere, where he or she believes on reasonable grounds that data held on other computers may contain evidential material of a kind covered by the search warrant. The proposed amendment will remove any doubt as to whether the existing provision permits access to material not held at warrant premises.

1.52 As most business computers are networked to other desktop computers and to central storage computers, files physically held on one computer are often accessible from another computer. In some cases these computer networks can extend across different office locations. Accordingly, it is critical that law enforcement officers executing a search warrant are able to search not only material in computers located on the search premises but also material accessible from those computers but located elsewhere.[29]

1.53 An executing officer would not be required to notify operators of computers not on search premises if data held on those computers is examined under warrant. The existing subsection 3L(1) permits an officer to operate equipment on site to see whether evidential material is accessible by doing so. The provision only requires that the data be accessible from equipment on site, it does not require that it be held on site. In contrast, the proposed provision will only allow an officer to access data if he or she believes on reasonable grounds that it may contain evidential material.[30]

1.54 Proposed subsection 3L(1A) would enable law enforcement officers executing a search warrant to copy data held on any electronic equipment or associated devices at search premises to a device where there are reasonable grounds for suspecting that the data contains evidential material. This will permit officers to copy all data held on a computer hard drive or data storage device if some of the data contains evidential material or if there are reasonable grounds to suspect the data contains evidential material.[31]

1.55 The existing provision only allows material to be copied.[32] Electronic equipment, such as a computer hard drive, can hold large amounts of data. It is often not practicable for officers to search all the data for evidential material while at the search premises and to then copy only the evidential material which is found. The proposed provision would allow officers to copy all the data on a piece of electronic equipment in situations where an initial search of the data uncovers some evidential material or where the officer believes on reasonable grounds that the equipment might contain evidential material.[33]

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

1.56 Proposed section 3LA would enable a law enforcement officer executing a search warrant to apply to a magistrate for an 'assistance' order. The person to whom the order is directed would be required to provide the officer, to the extent reasonably practicable, with such information or assistance as is necessary to enable the officer to access data on the computer system, copy it to a storage device or convert it to documentary form.

---

29 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 16

30 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 16

31 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 16

32 Paragraph 3L(2)(c) of the *Crimes Act 1914*

33 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 17

1.57 To grant the order, the magistrate would have to be satisfied:

a) (i) of the existence of reasonable grounds to suspect a computer on search premises contains evidence of an offence;

b) (ii) that the subject of the order is reasonably suspected of the offence or is the owner of the computer or computer system, or a current employee of the owner; and

c) (iii) that the subject of the order has knowledge of the functioning of the computer or system or measures applied to protect the computer or system.

1.58 While there is no requirement to provide such assistance under the existing *Crimes Act 1914* search warrant provisions and assistance requirements are common in Commonwealth regulatory legislation. Such a power is also contained in the Cybercrime Convention being developed by the Council of Europe (Draft No. 25, Article 19).[34]

Customs Act 1901

1.59 The provisions in the *Customs Act 190*1 relating to searches of electronic equipment and associated devices are identical to the provisions in the *Crimes Act 1914*. The proposed amendments to the *Customs Act 1901* would ensure that the two sets of provisions remain consistent. As the processing of imports and exports is increasingly computerised, it is also important that the *Customs Act 1901* provisions are updated to enable effective searches of electronically stored material.

Consequential amendments

1.60 The proposed new computer offences will require minor consequential amendments to the following legislation:

- *Australian Security Intelligence Organisation Act 1979*
- *Education Services for Overseas Students Act 2000*
- *Telecommunications (Interception) Act 1997*

34 Explanatory Memorandum, *Cybercrime Crime Bill 2001*, p. 18

CHAPTER 2

ISSUES

2.1 The Bill raises several issues which are of concern to the Committee and these have also been reflected in many of the submissions received and during the hearings. The major issues concern:

- the breadth of the proposed offences;
- some of the definitions;
- the investigative powers; and
- privacy issues.

Basis of the Bill

2.2 The Explanatory Memorandum states that the Bill is based on the recommendations of the January 2001 Model Criminal Code *Damage and Computer Offences Repor*t.[1] However, submissions and witnesses challenged this statement, claiming that there had been some divergence from the recommendations and substance of the Model Criminal Code without any indication of reasons.[2]

2.3 The Attorney-General's Department stated that the only divergence from the recommendations related to the jurisdictional aspects of the legislation and the enhancement of the law enforcement powers.[3] They stated that the Model Criminal Code has been developed on the basis of state jurisdiction and that when it is adopted for Commonwealth criminal matters, the Commonwealth must take into account its constitutional limitations. This is the reason why reference has been made in the Bill to telecommunications service and to Commonwealth computers.[4]

Breadth of Offences

2.4 Several submissions expressed serious concerns about the breadth of offences in the Bill. Some considered that:

- the offences were not sufficiently precise enough to ensure they would be applied only to truly criminal behaviour;

---

1 Explanatory Memorandum, *Cybercrime Bill 200*1, p.1

2 *Submission 1*, Australian Computer Society Inc, p.1; *Submission 15*, Electronic Frontiers Australia, p.1; *Transcript of evidenc*e, Australian Computer Society Inc, p.10

3 *Transcript of evidenc*e, Attorney-General's Department, p.10

4 *Transcript of evidenc*e, Attorney-General's Department, p.43

- many of the offences lacked the traditional elements of cause, knowledge, malicious intent and actual damage that are normally associated with criminal offences; and

- quite innocuous and even legitimate activities may be inadvertently caught and vulnerable to prosecution.[5]

Issue of intent

2.5 In relation to the criticism that the offences would catch innocent individuals and innocuous activities, the Attorney-General's Department maintained that this would not be the case. They stated that the proposed computer offences apply only to unauthorised conduct and contain appropriate fault elements to ensure they do not catch such activities:

> A lot of the offences require proof of intention. There has been some mention in some of the submissions about recklessness. However, the test for recklessness in the (Criminal Code) has quite a firm fault element. It is used universally for all similar serious offences where you are referring to circumstances or results of conduct.[6]

2.6 It was suggested by the Legislative Subcommittee of the New South Wales Society for Computers and the Law that the proposed new computer offences in the Bill could create an alternative regime to the laws relating to copyright, and greatly expand the protection of data beyond that contemplated by the *Copyright Act 1968*.[7] The Attorney-General's Department stated that they were:

> confident that the Cybercrime Bill 2001 will not affect the copyright law regime. Firstly, the conduct described in many of the subcommittee's examples would not constitute offences under the proposed legislation. The proposed offences apply only to conduct which affects Commonwealth data or involves the use of a telecommunications service.
>
> Secondly, these offences deal with access to data which is unauthorised, and the sorts of situations there that have been raised would suggest that we are talking about something that is authorised. Finally, even if there were some glimmer that one of these offences could apply, where a person accesses restricted copyright material for a permitted purpose within the terms of subsection 116A(3) or 132(5F) of the Copyright Act 1968, the defence of lawful authority, which is in section 10.5 of the Criminal Code, applies. Section 10.5 of the Criminal Code provides that a person is not criminally responsible for an offence if the conduct constituting the offence is justified or excused under a law….Subsections 116A(3) and 132(5F) of the Copyright Act allow the use of a circumvention device to be supplied to a qualified person for a permitted purpose. As the Copyright Act suggests, there is permission for qualified persons to use circumvention devices in accessing copyright material for a permitted purpose. Where it is authorised, such persons would be able to raise the defence of lawful authority in a prosecution for unauthorised access to restricted data.[8]

---

5 *Submission 10*, Legislative Subcommittee of the NSW Society for Computers and the Law, Foreward, p.2; *Submission 1*, Australian Computer Society Inc, p.4; *Submission 14*, Australian Competition & Consumer Commission, p. 1; *Submission 15*, Electronic Frontiers Australia Inc, p.2

6 *Transcript of evidenc*e, Attorney-General's Department, p.41

7 *Submission 10*, Legislative Subcommittee of the NSW Society for Computers and the Law, pp.5-7

8 *Transcript of evidenc*e, Attorney-General's Department, p.38

Absolute liability

2.7 Another issue that was of concern was the application of absolute liability in subsections 477.1(2), 477.2(2), 477.3(2), 478.1(2) and 478.2(2). Electronic Frontiers Australia pointed out that such a provision was not included in the Model Criminal Code and no explanation has been given for its inclusion in the Bill.[9]

2.8 The Explanatory Memorandum explains that the elements in paragraph 477.2(1)(d) are included:

> merely to trigger Commonwealth jurisdiction and do not have any bearing on the gravity of the offence.[10]

2.9 In evidence before the Committee, the Attorney-General's Department explained that:

> this relates to jurisdictional elements with the Criminal Code. It requires us to be very clear about what the fault element is for each element; otherwise fault elements do apply. Because there are Commonwealth aspects to the matter, we have to provide for absolute liability, simply to reflect the way in which the law would have otherwise operated. It does not affect the key culpability of what is going on here.[11]

2.10 The Attorney-General's Department submitted that the application of absolute liability to the jurisdictional elements of an offence under the Bill was appropriate and was consistent with other Commonwealth offences such as the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*.[12]

2.11 The Committee considers that the application of absolute liability to a particular physical element of an offence is acceptable as it does not affect the culpability element of the offence which, still has to be proven by the prosecuting authority.

2.12 It was submitted that the Bill should contain some exculpatory provision which would allow a court to find that "in all the circumstances the accused's conduct ought not be regarded as criminal."[13]

2.13 The Committee considers that many of the actions referred to in the various submissions would not be regarded as offences under the Bill. The Committee is satisfied that the proposed computer offences apply only to unauthorised conduct and contain appropriate fault elements of intention and recklessness, which are defined in the *Criminal Code Act 1995*.[14]

---

9 *Submission 15*, Electronic Frontiers Australia, pp.2-3

10 Explanatory Memorandum, *Cybercrime Bill 200*1, p.9

11 *Transcript of evidenc*e, Attorney-General's Department, pp.40-41

12 *Submission 20A*, Attorney-General's Department, p.6

13 *Submission 1*, Australian Computer Society Inc, p.4

14 *Transcript of evidenc*e, Attorney-General's Department, p.41

Computer offences

Definitions

'Computer'

2.14 The Committee was concerned that 'computer' had not been defined and questioned whether this could be seen as a weakness in the Bill. None of the witnesses saw this as a problem preferring to leave it to the courts to determine this matter in light of continuing changes in technology, rather than attempting to fit these changes within a definition.[15] While the failure to define 'computer' may be seen by some as Parliament abdicating its legislative responsibility, the Committee agrees with the view expressed in the Model Criminal Code Report that the best definition is to be found in the evolving common understanding of that term.[16]

2.15 The Australian Competition & Consumer Commission, while not suggesting that the term 'computer' should be defined, did consider that, with the rapid development in technology, reference in the Bill should be to 'computer or other electronic device used to store and process data in a digital form', rather than merely referring to a 'computer'.[17] The Committee does not consider that this is necessary as such devices would be caught by the general understanding of what a computer is.

'Data held in a computer'

2.16 The Committee queried why the definition of 'data held in a computer' differed from that contained in the Model Criminal Code. The definition in the Model Criminal Code included 'data entered or copied into the computer' which is not contained in the definition in the Bill.[18] The Attorney-General's Department advised that:

> The reference to 'data entered or copied into a computer' was removed because it was not necessary. The definition of 'data held in a computer' is an inclusive definition. It is necessary to refer to data held in a removable data storage device or a data storage device on a computer network as this data may not be covered by the ordinary meaning of 'data held in a computer'. However, data entered or copied into a computer is so clearly within the term 'data held in a computer' that there is no need to expressly include it.[19]

2.17 The Committee accepts the Attorney-General's Department explanation.

'Modification'

2.18 The Committee also queried why reference to a 'data storage device' in the definition of 'modification' in the Model Criminal Code is not included in the definition of

---

15 *Transcript of evidenc*e, National Crime Authority, p.5; Australian Computer Society Inc, p.12; Attorney-General's Department, pp.29-30

16 Model Criminal Code *Damages and Computer Offences Repor*t, p.129

17 *Submission 14*, Australian Competition & Consumer Commission, p.1

18 *Transcript of evidence*, p.44

19 *Submission 20A*, Attorney-General's Department, p.2

'modification' in the Bill.[20] The Attorney-General's Department explained that this was excluded because it was not considered necessary.

> The proposed offences refer only to modification of data held in a computer. The definition of 'data held in a computer' expressly includes data held in a removable data storage device or a data storage device on a computer network of which the computer forms a part. There is therefore no need to include a separate reference to a data storage device in the definition.[21]

2.19 The Committee accepts the Attorney-General's Department's explanation.

'Telecommunications service'

2.20 In relation to the definition of 'telecommunication service' the Australian Computer Society Inc considered this to be:

> vastly broader than…would be regulated under the Telecommunications Act.
>
> It would include the network running in your home. If you have two computers joined by a cable, the link between them is a telecommunications service within the definition in the bill. That means that every single link activity performed on a computer other than an activity performed on a physical computer that you are sitting in front of - in other words, any data accessed other than on the C drive of the computer you are attached to - must be effected by means of a telecommunication service, as defined in this bill. Therefore this bill will cover the field of everything.
>
> It may well do so unintentionally….Our view would be that, by having this broad definition of telecommunication service, the bill has inadvertently confined state law to applying to what you do on the C Drive of a PC or on a stand-alone personal assistant or some other thing.[22]

2.21 The Australian Computer Society Inc went on to say that this could result in:

> State agencies prosecuting people, who would have a very sound defence that they have been prosecuted under unconstitutional legislation because what they did was something that involved a computer other than the one they were attached to which is the subject of a Commonwealth law and not the state law. Unless there is a provision which says explicitly 'it is not intended to oust the concurrent operation of state law', I would have thought that there was going to be a serious problem very quickly.[23]

2.22 The Attorney-General's Department advised that it had:

> Sought legal advice on the scope of the Commonwealth's power to enact new computer offences in reliance on section 51(v). The advice we received indicated that it is doubtful whether a computer network within an organisation that uses lines provided by the organisation itself constitutes a communications "service" within the meaning of section 51(v). Therefore, the proposed computer offences would arguably not cover access to, or

---

20 *Transcript of evidence*, p.44

21 *Submission 20A*, Attorney-General's Department, p.2

22 *Transcript of evidenc*e, Australian Computer Society Inc, p.10; *Submission 1*, Australian Computer Society Inc, p.2

23 *Submission 1*, Australian Computer Society Inc, pp.2-3

> modification or impairment of, computer data caused solely by means of an internal computer network.[24]

2.23 In light of the Attorney-General's Department's advice, the Committee is satisfied that the definition of 'telecommunications service' does not mean that the offences will apply to persons using an internal computer network.

Recommendation 1

The Committee **recommends** that the Explanatory Memorandum be amended to make it clear that the offences under the Bill do not apply to persons using an internal computer network.

2.24 In relation to neighbourhood networks, the Attorney-General's Department advised that as 'telecommunications service' is technology neutral, such networks would generally fall within the proposed offences.

'Restricted data'

2.25 It was submitted that the definition does not make it clear that it is access to data that is restricted, not access to the computer itself.[25] The Committee does not agree. It considers the definition makes it quite clear that it is access to the data that is restricted.

2.26 It was further submitted that the definition of 'restricted data' was too wide. As most computers have some access control, be it by way of a password or identification code, this would mean that any unauthorised access is converted to restricted access under the definition. It was submitted that the definition needed to be amended to remove doubt as to what constitutes an 'access control system'. The Legislative Subcommittee of the New South Wales Society for Computers and the Law submitted that:

> It would be preferable to replace the words 'access control system' by 'security control'.[26]

2.27 The Australian Computer Society Inc considered the definition of 'restricted data' was an attempt to cover every possible experience that one could come across. They considered a better approach would be to say:

> if you use technological means to commit any currently known crime, then that is itself a crime[27]

2.28 The Australian Consumers' Association also expressed concern with the definition. They submitted:

> that the definition of restricted data in terms of a computer with an access control systems is insufficient. At the very least, the access control should apply specifically to the data in question. It would be better if the access control system were defined in terms of intent i.e. is

---

24 *Submission 20*, Attorney-General's Department, pp.1-2

25 *Submission 17*, Alex Steel , p. 4

26 *Submission 10*, Legislative Subcommittee of the NSW Society for Computers and the Law, Part A, p.2

27 *Transcript of evidenc*e, Australian Computer Society Inc, p.14

> it intended that the system will limit access to the data in question for the purposes of keeping it secure or confidential? Simply to have a general computer system subject to some kind of access system (which virtually all but the most primitive devices have) should not invoke the draconian sanction of criminal penalty simply for *accessing* data.[28]

2.29 The Committee agrees with the view expressed by the Legislative Subcommittee of the New South Wales Society for Computers and the Law that the definition of 'restricted data' needs to be amended to remove doubt as to what constitutes 'an access control system'. It agrees that this can be achieved by substituting 'a security control' for 'an access control system' in the definition.

Recommendation 2

The Committee **recommends** that the definition of 'restricted data' in section 478.1 be amended by deleting the words 'to which access' and substituting the following words 'where the access to the data'.

2.30 The Australian Consumers' Association saw difficulty with the definition of 'restricted data' in relation a network system such as the World Wide Web.

> it may prove confusing to nominate the data is held on a computer (singular) with an access control system. It may be a network that has the system, and one computer will validate the user (maybe for billing and identification rather then data security specifically) and then allow the user access to data held on multiple computers. By some interpretations, the entire World Wide Web would become restricted data because a user logs on to an ISP via an access control system. The section fails to grapple with the networked nature of modern data and applications management, and so illustrates the difficulty of creating criminal liability in uncertain technological environments.[29]

2.31 The Australian Competition & Consumer Commission expressed a similar view.[30]

2.32 The Attorney-General's Department submitted that, as with the meaning of 'computer', 'network' should not be defined. It should be left to the courts to determine having regard to changes in technology and the evolving common understanding of the term.[31]

2.33 The Committee considers that to define 'network' could limit the application of the proposed offences and that it would be best if the meaning was to be allowed to develop with advances in computer technology.

Law Enforcement Powers

2.34 Almost without exception, all private submissions and witnesses, as distinct from government agencies, expressed serious concerns about the breadth of the law enforcement

---

28 *Submission 5*, Australian Consumers' Association, p. 2

29 *Submission 5*, Australian Consumers' Association, pp. 2-3

30 *Submission 14*, Australian Competition & Consumer Commission, p. 3

31 *Submission 20A*, Attorney-General's Department, p.5

provisions in Schedule 2 of the Bill. They considered these provisions raised serious civil liberty and invasion of privacy issues.

2.35 Particular concerns were expressed about the power of authorities:

- to access data at premises other than warrant premises where a computer at the warrant premises is part of a network;
- to remove a 'thing' from premises; and
- to obtain a court order requiring a person to provide information or assistance.

2.36 It was submitted that the issuing of a search warrant should be conditional on the warrant affording no more access than is reasonably necessary to obtain what is needed and should not take the form of a general warrant.[32]

2.37 The Explanatory Memorandum sought to justify the need for the enhanced criminal investigations powers in the *Crimes Act 1914* and *Customs Act 1901* on the basis of the amount of data which can be stored on computer drives and disks and the protection of data by complex security measures, such as encryption and passwords.[33]

2.38 The Attorney-General's Department stated that the proposed law enforcement powers:

> reflect experience with the existing provisions and will assist in overcoming the problems investigators face in searching computer data that is held in different computers on a network or protected by complex security measures such as encryption and passwords. The proposed powers can only be exercised where an investigating officer has reasonable grounds to believe that data held on electronic equipment might constitute evidential material.
>
> Aspects of the current provisions are arguably broader than those proposed. For example, the existing subsection 3L(1) permits an officer to operate equipment on site to see whether evidential material is accessible by doing so. The provision only requires that the data be accessible from equipment on site, it does not require that it be held on site. In contrast, the proposed provision will only allow an officer to access data if he or she believes on reasonable grounds that it may contain evidential material. The existing provision that allows for things to be moved to another place for examination or processing (subsection 3K(3)) does not require that an officer have reasonable grounds for believing the thing contains evidential (material) before moving it nor does the provision place a limit on the time for which the thing may be moved. The (new) provision would do both.[34]

Search warrants

2.39 The National Crime Authority, the Australian Federal Police and the Attorney-General's Department did not consider the enhanced enforcement powers to be too broad.

---

32 *Transcript of evidenc*e, Australian Computer Society Inc, pp.9 and 14

33 Explanatory Memorandum, *Cybercrime Bill 200*1, p.2

34 *Submission 20*, Attorney-General's Department, pp. 2-3

2.40 The National Crime Authority saw the powers as no different to their existing powers.

> With our powers at the moment, it is possible for us to take …(a) complete filing cabinet if there are documents in there that relate to the offence (being investigated), and you may have other information caught up in amongst those documents that would not form part of the evidence in relation to the matter you are investigating.
>
> You need time to go away and be able to go through those files to identify what you would seize as evidence and identify those documents that you would return to the individual concerned.[35]
>
> it is a bit like other privacy intrusive tools of investigation that are available to law enforcement – for example, telephone interception and use of listing devices. Telephone conversations are intercepted but only those that are of evidentiary value are ever used. There are strict guidelines as to how we must behave and use that type of thing. It is the same with the listening devices. I am sure there will be guidelines and processes put in place to ensure that these things are managed the same way.[36]

2.41 The Australian Federal Police, while acknowledging that the search powers in the Bill were indeed an 'increase in power', considered these to be necessary if they were to operate effectively. They saw them as being:

> an extrapolation of the mechanisms…in the paper world.[37]
>
> the proposed amendments cater for the modern technological environment, especially with regard to clarifying that the search can apply to the network of which the computer forms part. In that sense, they are an expansion of powers to apply to new elements in the technological environment.[38]

2.42 They said that the proposed amendments do nothing to alter the existing requirements that need to be met in seeking a search warrant. The provision relating to the issuing of a search warrant under the *Crimes Act 1914* (section 3E) requires that the application be as specific as possible. It must specify the offence, the premises and/or persons to be searched and the object of the search, in essence, the collection of relevant and admissible evidence to the investigation of the identified offence.[39] A similar provision is contained in section 198 of the *Customs Act 1901*.

2.43 In relation to items that may be lawfully seized under a warrant, the Australian Federal Police said that they apply a 'three condition model'. Under this model, three 'tests' must be satisfied before something can be lawfully seized. The conditions are:

---

35 *Transcript of evidenc*e, National Crime Authority, p.2

36 *Transcript of evidenc*e, National Crime Authority, p.4

37 *Transcript of evidenc*e, Australian Federal Police, p.19

38 *Submission 24*, Australian Federal Police, pp. 7-8

39 *Submission 24*, Australian Federal Police, p. 6

- Firstly, to describe the class of the document or thing sought (e.g. journal, bankbook, correspondence.

- Secondly, to limit the description by demonstrating that the document or thing relates to specified people, companies or transactions, for example.

- Thirdly, to further narrow the scope by requiring that there must be reasonable grounds to suspect that the document or thing will provide evidence of the offence. A thing cannot be seized if there are no reasonable grounds to suspect that it has evidential value.[40]

2.44 The Committee acknowledges and accepts the concerns expressed in the various submissions in relation to search warrant powers. In most criminal investigations, material which is not connected to an investigation, will be gathered or accessed by law enforcement authorities in executing a search warrant. The Committee believes that one can expect that the same result will occur when authorities execute a search warrant in respect of investigations into cybercrime. Accordingly, the Committee does not consider the provisions in the Bill relating to the seizure and removal of a thing pursuant to a search warrant are too broad, but expects that the authorities and agencies involved will continue to observe the guidelines and controls currently in place for the execution of search warrants.

Privacy issues

2.45 When asked what privacy protections are in place to protect material of other persons who are unconnected to the suspected offence and which may be collected in the investigation process, both the National Crime Authority[41] and the Australian Federal Police[42] referred to the protection offered by internal rules and guidelines.

2.46 The Attorney-General's Department stated that discussions had already taken place with the Office of the Federal Privacy Commissioner and the view was that existing privacy guidelines would need to be revised after the legislation has been passed but before it commences.[43] The Department also pointed out that:

> There are various safeguards to protect the privacy of information that is gathered under a search warrant. Australian Federal Police officers are bound by the Information Privacy Principles in the *Privacy Act 1988* and are subject to a maximum penalty of 2 years imprisonment under the secrecy provisions in the *Australian Federal Police Act 1979* for any improper recording or disclosure of information.[44]

2.47 The Federal Privacy Commissioner considered there are privacy issues in relation to the collection of personal information that is not related to an investigation or is about innocent third parties. The Commissioner stated that it was unlikely that subjects of this information would ever become aware that information about them had been disclosed for law enforcement purposes:

---

40 *Submission 24*, Australian Federal Police, p. 7

41 *Transcript of evidenc*e, National Crime Authority, p.3

42 *Transcript of evidenc*e, Australian Federal Police, p.20

43 *Transcript of evidenc*e, Attorney-General's Department, p.28

44 *Submission 20A*, Attorney-General's Department, p.4

> As a safeguard we suggest that this provision include a requirement to destroy personal information that is not relevant to the investigation within a specified time frame. This could be after, say, three months with provision to extend the time frame with the authorisation of a senior officer. If such a provision is not included we suggest that the law enforcement agencies that are likely to be using this provision develop guidelines for handling and destruction of personal information collected under this provision. The guidelines should include some provision to record details of personal information collected and when it was destroyed, if this is not already covered under existing accountability procedures relating to the use of search warrants.[45]

2.48 The Committee sought advice from the Federal Privacy Commissioner on why he had suggested that authorisation for an extension of the time frame be approved by a senior officer instead of by way of a court order. The Commissioner advised that:

> The Office sees the destruction of irrelevant information as desirable but recognises that the timing of this needs to take reasonable account of the progress of an investigation. The aim of the recommendation to extend the time frame for destruction on the recommendation of a senior officer, as opposed to a court order, was to achieve appropriate privacy safeguards without imposing undue additional costs and processes.
>
> We understand that the approach to the destruction of irrelevant information collected under warrants issued under the *Telecommunications (Interception) Act 1979* (TIA) also uses an administrative rather than a judicial level of decision making.[46]

2.49 The Committee accepts that, with the continuing growth in and reliance on computer technology, law enforcement powers need to adjust to meet the challenge of those who may threaten the integrity, security and reliability of this technology. The powers set out in Schedule 2 should ensure that law enforcement agencies are able to meet this challenge.

2.50 However, any increase in law enforcement powers must be tempered to protect the privacy of innocent parties, who may be caught up in an investigation. The Committee considers the most effective way of ensuring the privacy of innocent parties is to have it enshrined in the legislation, as has been suggested by the Federal Privacy Commissioner. The Committee recommends the Bill be amended to include a provision to require the destruction of all personal information that is not relevant to an investigation within a specified time frame.

2.51 The Committee accepts that there will be investigations where it is necessary to hold information beyond a specified period. Where this occurs, provision needs to be made to allow for the retention of the information. The Committee accepts the recommendation of the Federal Privacy Commissioner that in such cases authorisation must be sought to extend the time frame. It also accepts that by having a senior officer approve such authorisations, as opposed to seeking a court order, this will be administratively cost effective, while maintaining appropriate privacy safeguards.

---

45 *Submission 11*, Office of the Federal Privacy Commissioner, p.3

46 *Submission 11A*, Office of the Federal Privacy Commissioner, p.2

Recommendation 3

The Committee **recommends** that the Bill be amended to provide for the destruction of all personal information collected by law enforcement agencies, which is not relevant to an investigation, after a period of 3 months but subject to this time frame being extended on the authorisation of a senior officer.[47]

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

2.52 The Bill provides that an executing officer may obtain an order from a magistrate requiring a 'specified person' to provide any information or assistance that is reasonable and necessary to allow the officer to access data held in, or accessible from, a computer that is on warrant premises, to copy the data to a data storage device or to convert the data into documentary form.[48]

2.53 It seems clear from the Explanatory Memorandum that the justification for this provision is to assist investigating officers overcome problems associated with encryption and passwords.[49] Several submissions expressed concerns about the breadth of this provision. It was submitted that it may be difficult for a person to prove that they do not possess the knowledge or have access to the required information.

2.54 Electronic Frontiers Australia suggested that:

> the proposed legislation should provide an indication as to how those served with assistance orders requiring plain text or encryption keys can successfully demonstrate that they cannot comply with the notice.[50]

They also considered that a problem could arise in relation to single encryption keys, which often serve the dual purpose of ensuring confidentiality and providing secure authentication of the signatory to a document. Revealing this key can compromise the integrity of the owner's digital signature. They suggested that an order should only be made against those people with 'relevant' knowledge and that a person should only be regarded as having committed an offence if they failed 'without lawful excuse' to comply with the order.[51]

2.55 Both Electronic Frontiers Australia and the Group known as 2600 Australia queried whether the forced disclosure of a password or decryption key violated the common law privilege against self-incrimination.[52]

---

47 'Senior officer' has not been defined as it will depend on the legislation of the particular law enforcement agency and the delegation power under that legislation.

48 *Cybercrime Bill 200*1, Schedule 2, Items12 and 28

49 Explanatory Memorandum, *Cybercrime Bill 200*1, p.2

50 *Submission 15*, Electronic Frontiers Australia, p.4

51 *Submission 1*, Australian Computer Society Inc, p.5

52 *Submission 4*, 2600 Australia, p.30; *Submission 15*, Electronic Frontiers Australia, p.5

2.56 The Attorney-General's Department advised that such an order does not affect the privilege against self-incrimination.

> The privilege arises where a person is required to produce certain documents or answer questions and entitles the person to refuse to produce those documents or answer the questions on the ground that it would incriminate him or her. An "assistance order" does not require a person to produce particular data; but only requires the person to provide information necessary to enable a law enforcement officer to access data on a particular computer. Having gained access to data on the computer the officer still have to search the data for evidential material. The person would not be required to assist officers in locating evidential material.[53]

2.57 While the Committee considers it reasonable for the executing officer to be able to obtain information and assistance in order to access and copy data which is protected by encryption or password and which he or she believes is relevant to the investigation, it believes there should be some requirement for the 'specified person' to be reasonably proximate to what is going on. The Committee considers this can be achieved by requiring the 'specified person' to have 'relevant' knowledge, as was suggested by the Australian Computer Society Inc. The Committee, however, does not consider subsection 201A(3) needs to be amended to include 'without lawful excuse'. The Committee considers a person who has 'relevant knowledge' should not be excused from providing it.

Recommendation 4

The Committee **recommends** that items 12 and 28 of Schedule 2 be amended by inserting 'relevant' before 'knowledge' in paragraph 3LA(2)(c) of the *Crimes Act 1914* and paragraph 201A(2)(c) of the *Customs Act 1901*.

Right to be present during an examination

2.58 Both the Australian Privacy Charter Council and 2600 Australia queried whether the amendments in the Bill to section 3 of the *Crimes Act 1914* and section 200 of the *Customs Act 1901* would remove the right of the occupier of premises or his or her representative to be present during the examination or processing of the thing that has been removed.[54]

2.59 The Attorney-General's Department advised that this right would not be affected as paragraphs 3K(3)(a) and (b) of the *Crimes Act 1914* and paragraphs 200(3)(a) and (b) of the *Customs Act 1901* give the occupier of search premises the right to be present at the processing of things taken from the premises.[55]

2.60 Two other matters were raised in relation to search warrants and assistance orders:

- an initial 72 hour time limit for holding a 'thing'; and
- the qualifications of magistrates to assess applications for a search warrant and assistance orders.

---

53 *Submission 20A*, Attorney-General's Department, p.5

54 *Submission 4*, 2600 Australia, p.28; *Submission 16*, Australian Privacy Charter Council, p.3

55 *Submission 20A*, Attorney-General's Department, p.5

72 hour time limit

2.61 Under the Bill, a 'thing' taken into possession by an 'executing officer' pursuant to a search warrant can only be held for a period of 72 hours. After this time the executing officer must apply to an issuing officer under the *Crimes Act 1914* or a judicial officer under the *Customs Act 1901* for an extension of that time if he or she believes that the thing cannot be examined or processed within 72 hours. In these circumstances the occupier must be given notice of the application and is entitled to be heard in relation to the application.[56]

2.62 Both the Queensland Police Service and the New South Wales Police Service expressed concern about this time limitation. The Queensland Police Service stated:

> Experience shows that where it is necessary to remove a computer or part of a computer for examination by experts, that process in every case exceeds 72 hours. Under the *Police Powers and Responsibilities Act 2000* (Qld), Chapter 11, Part 3, Queensland police officers are given 30 days to examine a thing before an application to extend the period for keeping the thing is required. These provisions have operated effectively for both police and persons interested in the thing seized.[57]

2.63 The New South Wales Police Service considered the 72 hour time limit to be impracticable on the basis of the possible need to transport items to Sydney from remote areas in the state, the limited number of computer experts available to examine the items and the time needed to carry out the forensic examination. They suggested that any time limit would be better expressed in working days rather than hours and suggested a minimum of 5 working days before an application for an extension of that time is required. They also queried whether there would be any limitation on the number of extensions that may be granted.[58]

2.64 The Committee considers the 72 hour time limit to be somewhat impracticable having regard to the likely subject matter of a search warrant. The Committee believes a more realistic time period would be 5 days. Such a period should reduce the number of applications for extension of time without causing undue hardship on the owner of the things removed or the owner of the premises from which they were removed.

Recommendation 5

The Committee **recommends** that the time period of 72 hours referred to in items 7 and 23 of Schedule 2 be amended to 5 days.

Number of applications for extension of time

2.65 In relation to the New South Wales Police Service query concerning the number of applications for an extension of time that can be made, the Attorney-General's Department advised that:

---

56 *Cybercrime Bill 200*1, Schedule 2, Items 7 and 23

57 *Submission 6*, Queensland Police Service

58 *Submission 13*, New South Police Service, p.2

> The provision permitting an executing officer to apply for an extension of time would allow more than one application to be made in respect of the same item.[59]

2.66 The Committee believes that the Bill needs to make it clear that more than one application can be made. It recommends that a provision similar to subsection 3E(8) of the *Crimes Act 1914,* which allows for successive search warrants, should be included in relation to applications under Items 7 and 23 of Schedule 2 of the Bill.

Recommendation 6

The Committee **recommends** that items 7 and 23 of Schedule 2 be amended by inserting a subsection into both the *Crimes Act 1914* and the *Customs Act 1901* to allow for successive applications to be made for an extension of time beyond the initial 5 days that a thing may be moved to another place for examination or processing.

Qualifications of issuing/judicial officers to assess whether to issue a search warrant/assistance order

2.67 Some submissions and witnesses queried the technical capacity of issuing/judicial officers to properly assess the basis of an application for a search warrant or an assistance order.[60] The Communication Law Centre suggested that this might be overcome by having 'a specialist judicial person' exercise this function. The Centre further suggested that the proposed provisions[61] which allow a magistrate to order a specified person to provide an executing officer with information or assistance 'that it is reasonable and necessary', is too ambiguous and that a more specific criterion should be identified:

> What assistance and information might be required, is not specified by the legislation other than to say that a magistrate must decide whether it is necessary and reasonably practicable to enable access. With due respect to magistrates, it is not an area of expertise that many are likely to have. Consideration should be given to some more specific criteria for the order being made and a specialist judicial person to exercise this function.[62]

2.68 The Committee, while appreciating these concerns, believes that issuing/judicial officers are called upon daily to make decisions on whether or not a search warrant should be granted in a range of subjects without the need for them to be an expert in the matter which may be the subject of the investigation. In deciding whether to issue a search warrant, they rely upon the information supplied in support of the application. The Committee therefore does not see any reason for having an application for a search warrant or an assist order under the Bill determined by a specialist judicial officer.

2.69 As for the suggestion that more specific criteria should be identified, other than 'reasonable and necessary', in determining what information and assistance is to be provided, the Committee considers that it would be neither appropriate nor desirable to restrict judicial

---

59 *Submission 20A*, Attorney-General's Department, p.1

60 *Transcript of evidenc*e, Australian Computer Society Inc, p.9; *Submission 3*, Communication Law Centre, p.1

61 *Cybercrime Bill 2001*, Schedule 2, Items 12 and 28

62 *Submission 3*, Communication Law Centre, p.1

discretion in such a way. Each application needs to be considered in light of the particular circumstances of the case.

Saving of other laws

2.70 The Australian Competition & Consumer Commission (ACCC) was concerned that, unless 'lawful activity of law enforcement agencies is exempted from prosecution' the investigative techniques which the Commission uses may be adversely affected by the application of the provisions relating to unauthorised access to a computer.[63]

2.71 The Commission further advised that:

> In its role as an enforcement agency, ACCC regularly accesses remote servers via a variety of means, some of which might potentially place its staff in breach of the proposed offences. A particular example is port scanning to determine the types of traffic that a computer can receive or send. More generally, staff monitor the software industry to remain aware of the latest tools that may be used to assist in identifying and locating persons and equipment used in contraventions of the Trade Practices Act 1974 (the TPA). Without clear guidance on the boundary between the public and private networks, the ACCC is at a disadvantage in knowing whether such tools may legally be used, and ensuring it has the capability to effectively investigate potential contraventions.
>
> It is our concern that the TPA contains no explicit power enabling the ACCC to investigate potential contraventions, and that therefore (section 476.4) on lawful authority may not extend to the ACCC. Accordingly, the possibility may exist that a respondent may argue that the use of port scanning or a similar technique is in contravention of the provisions contained in s478.1, and potentially place the proceedings at risk….
>
> The ACCC is keen to avoid doubt on the potential of the new offences to adversely affect the ability of the ACCC to investigate potential breaches of the Act. It is therefore suggested that consideration be given to ensuring continued investigative capability either by a consequential amendment to the TPA, or by excluding such investigative techniques from prosecution by reference in the Explanatory Memorandum.[64]

2.72 The Attorney-General's Department advised that:

> Port scanning does not constitute access to data and most certainly does not constitute access to restricted data and is therefore unaffected by the proposed offences.
>
> Spamming would only be caught by the proposed offences if the purpose of the spamming were to bring a system down.[65]

2.73 In relation to the definition of 'relevant offence' in the *National Crime Authority Act 1984,* the National Crime Authority submitted that:

> Although computer offences are not listed in the offences set out in paragraph (d) of the definition of 'relevant offence' in subsection 4(1) of the *National Crime Authority Act 1984* they could be investigated as activity related to 'relevant offences' as permitted by subsection

63 *Submission 14*, Australian Competition & Consumer Commission, p. 1

64 *Submission 14*, Australian Competition & Consumer Commission, pp.2-3

65 *Transcript of evidence*, Attorney-General's Department, p.40

> 4(2). However, it would be clearer and avoid any possible arguments about the jurisdiction exercised by the NCA, if the NCA Act were to be amended to include computer offences within the definition of 'relevant offence'.[66]

2.74 The Committee considers the matters raised by the Australian Competition & Consumer Commission and the National Crime Authority in respect of their investigation powers need to be addressed and any uncertainty removed. The most effective way of achieving this is by way of a consequential amendment in the Bill, which the Committee recommends.

Recommendation 7

The Committee **recommends** consequential amendments to both the *National Crime Authority Act 1984* and the *Trade Practices Act 1974* to ensure that the investigation powers of the respective agencies are not diminished by the offence provisions of the Bill.

Specific Offences-

2.75 The Committee does not consider that it is necessary to report on the specific offences in the Bill as the issues which have been raised in relation to them have been dealt with in other areas of this report.

66 *Submission 2*, National Crime Authority, p.1

CHAPTER 3

RECOMMENDATIONS

3.1 The Committee has raised a number of issues and made recommendations throughout this report. The recommendations are as follows:

Recommendation 1, following Paragraph 2.23

The Committee **recommends** that the Explanatory Memorandum be amended to make it clear that the offences under the Bill do not apply to persons using an internal computer network.

Recommendation 2, following Paragraph 2.29

The Committee **recommends** that the definition of 'restricted data' in section 478.1 be amended by deleting the words 'to which access' and substituting the following words 'where the access to the data'.

Recommendation 3, following Paragraph 2.51

The Committee **recommends** that the Bill be amended to provide for the destruction of all personal information collected by law enforcement agencies, which is not relevant to an investigation, after a period of 3 months but subject to this time frame being extended on the authorisation of a senior officer.

Recommendation 4, following Paragraph 2.57

The Committee **recommends** that items 12 and 28 of Schedule 2 be amended by inserting 'relevant' before 'knowledge' in paragraph 3LA(2)(c) of the *Crimes Act 1914* and paragraph 201A(2)(c) of the *Customs Act 1901*.

Recommendation 5, following Paragraph 2.64

The Committee **recommends** that the time period of 72 hours referred to in items 7 and 23 of Schedule 2 are amended to 5 days.

Recommendation 6, following Paragraph 2.66

The Committee **recommends** that items 7 and 23 of Schedule 2 be amended by inserting a subsection to both the *Crimes Act 1914* and the *Customs Act 1901* to allow for successive applications to be made for an extension of time beyond the initial 72 hours that a thing may be moved to another place for examination or processing.

Recommendation 7, following Paragraph 2.74

The Committee **recommends** consequential amendments to both the *National Crime Authority Act 1984* and the *Trade Practices Act 1974* to ensure that the investigation powers of the respective agencies are not diminished by the offence provisions of the Bill.

3.2 Subject to the above recommendations, the Committee **recommends** that the Bill proceed.

Senator Marise Payne

Chair

August 2001

APPENDIX 1

ORGANISATIONS THAT PROVIDED THE COMMITTEE WITH SUBMISSIONS

Organisation	Sub No.
Australian Computer Society	1
National Crime Authority	2
National Crime Authority	2A
Communications Law Centre	3
2600 Australia	4
Australian Consumers' Association	5
Queensland Police Force	6
Ajoy Ghosh Beng, MEM	7
Ctel Technologies Pty Ltd	8
The Australian Capital Territory Bar Association	9
Gilbert & Tobin	10
Office of the Federal Privacy Commissioner	11
Office of the Federal Privacy Commissioner	11A
Commissioner's Office, Department of Police and Public Safety, Tasmania	12
Ministry for Police	13
Australian Competition & Consumer Commission	14
Electronic Frontiers Australia	15
Australian Privacy Charter Council	16
Mr Alex Steel	17
Mr Alex Steel	17A
Silicon ChiC Pty Ltd	18
Internet Industry Association (IIA)	19

Attorney-General's Department	20
Attorney-General's Department	20A
The New South Wales Bar Association	21
Office of the Privacy Commissioner	22
The Victorian Bar	23
Australian Federal Police	24
NSW Council for Civil Liberties	25

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Public Hearing, Thursday 19 July 2001 (Sydney)

Mr Philip Argy, Vice President, Australian Computer Society

Mr Michael Atkins, Special Adviser Law Reform, Australian Federal Police

Mr Jonathan Boxall, Acting Team Leader, NII Incidence Analysis and Response Team, Australian Federal Police

Ms Sarah Chidgey, Legal Officer, Criminal Law Branch, Attorney-General's Department

Mr Geoffrey McDonald, Assistant Secretary, Criminal Law Branch, Attorney-General's Department

Mr Robert McDonald, National Director, National Crime Authority

Mr Stephen Orlowski, Consultant, Attorney-General's Department

Mr Robert Tebbet, National Manager, Technical Support and Physical Surveillance, National Crime Authority

Mr Mark Walters, Acting Director, Investigations and Technical Operations, Australian Federal Police

Public Hearing, Thursday 9 August 2001 (Canberra)

Ms Sarah Chidgey, Legal Officer, Attorney-General's Department

Mr Geoffrey McDonald, Assistant Secretary, Criminal Law Branch, Attorney-General's Department

Mr Gregory Taylor, Vice-Chair, Electronic Frontiers Australia

ADDITIONAL COMMENTS BY THE LABOR SENATORS

Drafting issues

1.1 This Bill is a bringing together of high technology, which is in its infancy, and the world of criminal law, which has a long history. In order to get these two worlds to meld in an acceptable way it is imperative that governments take the public with them, so that the public both understands the intended laws and accepts them.

1.2 In this context, this particular piece of legislation is both necessary and problematic. We acknowledge that it is important that the criminal laws keep pace with criminal activity, particularly in the world of technology. At the same time, we are aware that in many instances it is not possible for legislation to keep pace with technology, let alone with its criminal use.

1.3 The Cybercrime Bill 2001 presents a significant effort to legislate in a technical area in which it may be difficult to be effective. The Australian Labor Party has always been and will continue to be supportive of the intent and the work of the Model Criminal Code Committee, and to that extent Labor Members of the Committee support this legislation. However, there are a number of areas where we believe that the drafting of the Bill could be improved.

1.4 In addition to most of the majority recommendations, we recommend that the drafting amendments suggested by Mr Alex Steel in his submission (Number 17) be adopted, and that his other comments be given greater consideration. A further examination of this Bill and other legislation on related information and communications technology should be undertaken to ensure that all definitions used and applications of the legislation are consistent.

Lack of Consultation

1.5 A number of industry groups made submissions to the Committee. It was obvious from these submissions and other evidence given to the Committee that there is grave concern in the IT industry and in some legal circles about the impact of the Bill. The evidence from the Attorney-General's Department was that many of these fears are misguided or exaggerated. Yet, the mere fact that these genuine concerns were held is evidence that there is a dangerous communication gap between the Government and stakeholders.

1.6 It is abundantly clear that the Government did not include the information technology industry in the development of the legislation (as opposed to what happened with the Model Criminal Code process). This situation is unacceptable, given that the Model Criminal Code Committee Discussion Paper which contained the recommended computer offences was published in February last year, and the Officers' Report was published over 4 months ago.

1.7 Although the Government took more than twelve months to introduce this Bill, it appears that no effort was made during that time to consult with, or inform, all relevant stakeholders as to the intended content and application of the Bill. This has lead to the unfortunate situation where it appears that there is widespread, and in some instances unnecessary, concern.

1.8 Further, the law enforcement powers in the Bill were not part of the Model Criminal Code Process. The Government has chosen to include them in the Bill on the basis that they adopt some of the provisions from the draft Council of Europe Cybercrime convention. Prior to this Committee's hearings, there had been no public consultation or debate about the need for extended law enforcement powers, or the appropriateness of the provisions included in this Bill.

1.9 Labor Senators accept that it is important that Australia is abreast of international developments. However we think it is not an ideal situation that we include parts of the European convention into Australian law when Australia has played no part in the development of that convention. This is particularly so when there has been no domestic debate on the subject.

1.10 In addition, it appears from the evidence given to the Committee, that the law enforcement powers were included in the Bill without request from, or even consultation with, Commonwealth law enforcement agencies. The National Crime Authority, for example, appeared to have limited knowledge of the content of the Bill, or the extent of the law enforcement powers.

1.11 It also appeared that the various interagency committees concerned with E-commerce, information technology and law enforcement did not play an active role in the development of this legislation. This raises the question of how well coordinated the bureaucratic process is under this Government.

1.12 We accept that Australia's law enforcement agencies must be given suitable tools to fight sophisticated crimes. It may even be that the provisions included in this legislation are appropriate, with or without modification. However, we are strongly of the opinion that law enforcement should not be given new powers without appropriate public debate.

1.13 We disagree with the majority recommendation that the time limit for which a 'thing' may be held be extended from 72 hours to 5 days. Nearly all businesses and professional practices today are greatly reliant upon their information technology platform to conduct their day-to-day businesses. The removal of computers, or parts of computers for a 5-day period could have serious commercial and other consequences for business and professions that are unwarranted in relation to any evidential material obtained.

1.14 The AFP told the Committee, that law enforcement does not have the resources to investigate computer crimes. Strict laws should not be passed on the basis of making up for lack of resources. Rights should not be restricted because of lack of funds for law enforcement. There is a need to develop an appropriate relationship between the needs that business and professionals have for technology and the needs of law enforcement.

1.15 We recommend that further consideration be given to the appropriateness of these new powers.

Senator McKiernan	**Senator Cooney**	**Senator Ludwig**
Deputy Chair	**Member**	**Participating Member**

AUSTRALIAN DEMOCRATS

SUPPLEMENTARY REPORT

1. Introduction

1.1 The Democrats are generally in agreement with the Chair's report on the *Cybercrime Bill 2001*. The Bill is designed to protect the security, integrity and reliability of computer data and electronic communications. There are a number of significant flaws in the proposed Bill and we believe the Chair's proposed amendments go some way to ameliorate these defects.

1.2 The Democrats support the Chair's seven recommendations but, in addition, we will seek to further improve the Bill by bringing forward amendments to address some of the legitimate concerns about the implications to privacy.

2. The Bill

1.3 The Bill amends the *Criminal Code Act 1995* by enacting seven new computer offences that target people who access or modify computer data or communication to and from a computer that they did not have authority to access, modify or impair and do so with intention of committing a serious offence. The new offences are broadly consistent with the draft Council of Europe Convention on Cybercrime and are based on the recommendations of the Model Criminal Code Officers Committee of the Standing Committee of Attorney Generals. In addition, the Bill substantially strengthens criminal investigation powers and each offence is supported by additional extraterritorial jurisdiction.

3. Rationale for the Bill

1.4 Borderless virus, trojan and worm attacks and unauthorised hacking of major websites have focused media and public attention on 'cybercrime'.

1.5 It is notable, however, that while the case for the Bill's strengthened police powers and additional offences is plausible, at no stage was an adequate case made by the Government and enforcement agencies to show how the computer offences inserted in the Crimes Act in 1989 are inadequate.

1.6 For instance, in its submission, the Attorney General's Department argued the proposed strengthening of law enforcement powers "reflect experience with the existing provisions" without specifying that experience.[1]

1.7 As the Australian Privacy Charter Council point out:

> The Australian Federal Police received 320 electronic crime referrals between 1 July 2000 and 30 May 2001) more than a third from the Australian Broadcasting

---

[1] Attorney General's Department, *Submission No. 20,* p. 2

> Authority). In what proportion of these referrals were investigators inhibited by the absence of the powers now sought?[2]

1.8 The AFP took this question on notice in the public hearing and their subsequent submission stated that it could not answer the question "as the information is not readily available".[3]

1.9 In addition, the Democrats believe the uncritical use of unsourced and inflammatory assertions in the Minister's 2nd reading speech that Cybercrime costs companies $3 trillion per annum around the world do not throw light on the issues.

1.10 As noted above, while the Democrats accept the plausibility of the need for the additional powers, we wish to place on record our concern at the less than adequate arguments by the Government and agencies to articulate and defend the rationale for the Bill.

4. Privacy and Additional Powers

1.11 All submissions and witnesses apart from those of the government agencies expressed concerns about the increased powers in Schedule 2 of the Bill and the implications of these powers on privacy.[4] In particular, the concern was raised that the nature of electronically stored data means police searches through networks could see anyone attached to the network being vulnerable to investigation. This has significant implications for privacy as extensive private information could be collected either with or without the knowledge of third parties that is not relevant to the investigation.

1.12 While the Chair's report was sympathetic to some of these concerns and recommended that personal information obtained by law enforcement agencies in searches that are not relevant to an investigation must be destroyed, the Democrats believe there are additional concerns that need to be addressed to better safeguard privacy concerns.

Review of Bill's provisions

1.13 The Federal Privacy Commissioner recommended that there be a review of the use and application of the extended investigation powers and new offences 18 months after the commencement of the legislation.[5]

1.14 The Democrats strongly support the intent of the Privacy Commissioner's recommendation and will seek to amend the legislation along the lines outlined by the Commissioner.

---

[2] Australian Privacy Charter Council, *Submission No. 16*, p. 2

[3] Australian Federal Police, Committee Hansard, Sydney 19 July 2001, p. 21. AFP, *Submission No. 24*, p. 6

[4] See for instance, Australian Computer Society, *Submission No. 1*, Communications Law Centre, *Submission No. 3,* The Australian Privacy Charter Council, *Submission No. 16*

[5] Office of the Federal Privacy Commissioner, *Submission No. 11*, p. 1

Recommendation 1: That the legislation be amended to enable a review of the use and application of the extended investigation powers and new offences 18 months after the commencement of the legislation.

Annual reports of enforcement agencies

1.15 The Privacy Commissioner also recommended that relevant enforcement agencies include information regarding the use of these powers in their annual reports and that the Privacy Commissioner be consulted on the nature of these reports.[6] The Democrats believe that this recommendation has substantial merit in helping agencies analyse carefully the scope and nature of the additional powers, thus we will be moving amendments to give affect to this recommendation.

Recommendation 2: that relevant enforcement agencies include information regarding the use of the Bill's powers in their annual reports and that the Privacy Commissioner be consulted on the nature of these reports

Guidelines

1.16 The Committee was informed that the Australian Federal Police will review its guidelines on recording, disclosure and storage of information to take into account the new investigation powers and offences.[7] Mr Tebbet of the National Crime Authority told the Committee; "I am sure there will be guidelines and processes put in place to ensure that these things are managed the same way"[8] (as other privacy intrusive tools of investigation).

1.17 The Democrats are concerned that there is a significant asymmetry between the timing and scope of the legislation and consideration by enforcement agencies of operational scope and constraints.

1.18 While we acknowledge that there will be a period between enactment and commencement of the legislation, to develop appropriate guidelines, the Democrats are concerned by the lack of apparent close consideration by agencies, including the NCA, of the new enforcement environment that the Bill enables.

1.19 In our view, the substantial privacy concerns warrant additional public scrutiny thus we recommend that the Minister develop regulations covering access to third party information in conjunction with the Privacy Commissioner that are subject to disallowance.

---

[6] Office of the Federal Privacy Commissioner, *Submission No. 11*, p. 3

[7] Attorney General's Department, *Submission No. 20A*, p. 4

[8] National Crime Authority, *Committee Hansard*, Sydney, 19 July, 2001, p. 4

Recommendation 3: that the Minister develops regulations covering access to third party information in conjunction with the Privacy Commissioner that are subject to disallowance.

5. Additional Items

1.20 A number of submittees argued that the Bill will not be effective because it does not address the substantial problem of inadequate security and protection against viruses, worms and hacking and, in addition, the capacity of the ACCC to investigate 'totally secure' claims of software vendors.[9]

1.21 While outside the provisions of the Bill, the Democrats believe there is an ongoing need for education of all computer users as to the necessity of using and regularly updating appropriate security software.

Senator Brian Greig, Member

Australian Democrats

IT Spokesperson

[9] 2600 Australia, *Submission No. 4*, s.4 (c) and s.5 (b). Ajoy Ghosh, *Submission No. 7*, Silicon Chic Pty Ltd., *Submission No. 18*