Department of the Parliamentary Library

INFORMATION AND RESEARCH SERVICES

Bills Digest

No. 48 2001–02

Cybercrime Bill 2001

ISSN 1328-8091

Inquiries

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2646.

Information and Research Services publications are available on the ParlInfo database.
On the Internet the Department of the Parliamentary Library can be found at:
http://www.aph.gov.au/library/

Published by the Department of the Parliamentary Library, 2001

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 48 2001–02

Cybercrime Bill 2001

Angus Martyn
Law and Bills Digest Group
10 September 2001

Contents

Cybercrime Bill 2001

Date Introduced: 27 June 2001

House: House of Representatives

Portfolio: Justice and Customs

Commencement: On a day to fixed by proclamation or six months after Royal Assent, whichever is the earlier.

Purpose

To update existing Commonwealth provisions on computer-related crime.

Background

Origins of the Cybercrime Bill 2001

The main Commonwealth offence provisions on computer-related crime are currently found in Part VIA of the *Crimes Act 1914*. These are largely based on the recommendations of the 1988 Gibbs report.[1] They have not been substantially amended since coming into force in 1989. Computer-related search and seizure provisions were added in 1994 and again have remained largely unchanged since then.

In January 2000 the Model Criminal Code Officers Committee (MCCOC)[2] released a discussion paper *Chapter 4: Damage and Computer Offences* followed by a report of the same name in January 2001 (the Chapter 4 report)[3]. The Chapter 4 report is one of a series addressing particular aspects of Australian criminal law with the purpose of achieving national consistency of approach along the Criminal Code model. It contains a 'model' Cybercrime Bill, complete with definitions and offences.

According to the second reading speech, the offences contained in Cybercrime Bill 2001 (the Bill) are based on the Chapter 4 report. Interestingly, the report's approach is itself significantly influenced by the UK *Computer Misuse Act 1990*:[4]

> That is a consequence, in the main, of the fact that the Committee was asked by the Standing Committee of Attorneys-General to base its proposals for reform of the law of theft and fraud in Chapter 3, *Theft, Fraud, Bribery and Related Offences* (1995), on

> the provisions of the UK *Theft Act* 1968. The *Theft Ac*t, together with the *Criminal Damage Act* 1971 and the *Computer Misuse Act* 1990 comprise a complementary scheme of legislation, with interlocking parts…in view of the interdependence of these schemes of legislation, the Committee concluded that *Computer Misuse Act* 1990 provided an appropriate basis for the reform of Australian law…[although the] Committee's proposals go beyond the scope of the United Kingdom Act in certain respects [such as in so-called] preparatory offences and the offence of unauthorised access etc with intent to commit a serious offence.

However, in addition to the *Computer Misuse Act 1990*, the Chapter 4 report also takes account of more recent events such as the Council of Europe draft Cybercrime convention.

NSW has already enacted the Chapter 4 report. The *Crimes Amendment (Computer Offences) Act 2001* was passed by the NSW Parliament in April and received Royal Assent in June. That Act corresponds very closely with the proposed offences in the Chapter 4 report. According to a media release by the Commonwealth Minister for Justice and Customs, all Australian jurisdictions 'reconfirmed their commitment to giving priority to developing updated computer offences' at the most recent meeting of Australian Attorneys-General.[5]

The Structure of the Bill

The operative sections of the Bill are grouped into two schedules.

Schedule 1 creates a number of offences to replace those currently under Part VIA of the *Crimes Act 1914*. The main offences are:[6]

- Unauthorised access, modification or impairment to commit a serious offence
- Unauthorised modification of data to cause impairment
- Unauthorised impairment of electronic communication
- Unauthorised access to or modification of restricted data
- Unauthorised impairment of data held in a computer disk, credit card or other data storage device
- Possession of data with intent to commit a computer offence, and
- Production, supply or obtaining of data with intent to commit a computer offence.

Schedule 2 revises existing powers under the *Crimes Act 1914* and *Customs Act 1901* to search and seize electronically stored data.

Commonwealth jurisdiction over cybercrime

The Commonwealth has no direct constitutional power over computer-related offences. It can of course legislate with respect to Commonwealth facilities, property or activities and so actions involving Commonwealth computers and data may be regulated. However, potentially the widest constitutional power is that under section 51(v) - 'postal, telegraphic, telephonic, and other like services'. The High Court has previously ruled that this power extends to post-1900 forms of mass electronic communication such radio and television[7] and there seems no to reason to doubt that it would cover contemporary forms of telecommunications such as the internet. A number of the Bill's offence provisions provide for Commonwealth jurisdiction where a 'telecommunications service' is involved. The Bill defines 'telecommunications services'[8] as:

> A service for carrying communications by means of guided or unguided electromagnetic energy or both.

Some submissions to the Senate committee[9] inquiring into the Bill contended that this would include situations where computers were linked by a simple 'in-house' cable network. The Attorney-General's Department were of a contrary view, apparently because such a network would not constitute a 'service', although they did not provide any legal authority for this other than saying that their position was based on legal advice received. In any case, possible constitutional uncertainty about the prosecution of an alleged offence involving only an in-house network (and no other Commonwealth jurisdictional 'hooks') could be avoided by having the offence prosecuted under the state law. Of course this presupposes the State in whose territory the offence to place has passed the Chapter 4 legislation.[10]

Main Provisions

Schedule 1 - Computer Offences

Item 1 is a consequential amendment to subsection 25A(4) of the *Australian Security Intelligence Organisation Act 1979*. It is required as the computer-related offences currently found in Part VIA of the *Crimes Act 1914* will be replaced by the insertion of new Part 10.7 of the *Criminal Code Act 1995*.

Item 2 repeals Part VIA of the *Crimes Act 1914.*

Item 3 amends the definition of what may constitute a physical element[11] under the subsection 4.1(1) of the *Criminal Code Act 1995* (the criminal code). This clarifies that circumstances that 'arise as a result of conduct'[12] can be considered to be a physical element of an offence.

Item 4 inserts **new Part 10.7 (Divisions 476-478)** into the Criminal Code.

Division 476 - Preliminary

New section 476.1 defines a number of technical terms such 'access to data held in a computer', 'Commonwealth computer' etc. These terms, with some minor changes, reflect the recommendations of the Chapter 4 report. Some submissions expressed concern about the about the breadth of some definitions in **new sections 476.1** and **476.2**. For example, one submission[13] suggested that definitions of the concepts 'access or modify' and 'impairment' could be amended to reduce the possibility that innocuous activity or minor transgressions could fall with the criminal scope of the Bill.[14]

New section 476.2 defines what is meant by the terms 'unauthorised access, modification or impairment'. These terms are key elements of offences under **new sections 477.1-478.2**.

Of particular importance in **new section 476.2** is **subsection 476.2(2)** which provides that any such access, modification or impairment is not unauthorised merely because it is done for a purpose other than that for which a person is entitled. The *Explanatory Memorandum* to the Bill comments that:[15]

> …for example, if a Commonwealth employee is authorised to access certain computer data so he or she can perform her duties but instead accesses that data for the purpose of defrauding the Commonwealth, that access does not become unauthorised [and so does not fall within the meaning of 476.2]

The Chapter 4 report addressed this matter in some detail:[16]

> Should individuals who are authorised for one purpose be guilty of an offence under this Part if they act for another, ulterior purpose? Liability should certainly be imposed if the original authorisation was obtained by deception as to the offender's purposes. It does not follow, however, that liability should be imposed when authorisation was obtained without fraud and the defendant misuses the authorisation[17] [although] the issue is clearly contentious…It should be noted, at the outset, that the issue is unlikely to arise in the offences which prohibit unauthorised modification of data and unauthorised impairment of electronic communications. When breach of those provisions is charged, the issue is whether some particular modification or instance of impairment is authorised…there is an undoubted need for one or more specialised offences which would deal with misuse of authorised access to particular categories of data…[however]… Legislation which imposes criminal penalties for obtaining confidential information, sale or publication of that information cannot be restricted to instances where the offender happened to acquire the information by operating a computer.

New subsection 476.2(3) provides that a person is considered to have caused any unauthorised access, modification or impairment if their conduct 'substantially contributes to' the access, modification or impairment.[18]

New section 476.3 provides that criminal code 'Category A' geographical jurisdiction[19] will apply to the new computer offences created by the Bill. As a result of the application of Category A jurisdiction, the offences would extend to situations where the conduct

constituting the offence occurs wholly or partly in Australia or on board an Australian ship or aircraft, or where the *result* of the conduct constituting the offence occurs wholly or partly in Australia or on board an Australian ship or aircraft, or the person committing the offence is an Australian citizen or an Australian company. Thus an Australian citizen operating in a country where computer hacking is not an offence, who hacks into a computer system in a third country would face potential criminal liability under the Bill.[20]

Further jurisdiction is available under **new section 476.3** for so-called ancillary offences committed outside Australia. For example, this would apply where a persons outside Australia conspire to commit a Part 10.7 offence and subsequently that offence occurs in Australia or on an Australian ship or aircraft.

New section 476.4 provides for the concurrent operation of Commonwealth, State and Territory laws. Thus State or Territory computer law may be used to regulate to computer-related actions in those relatively few instances where they fall beyond the Commonwealth constitutional power. However, State or Territory computer law cannot be used where an action falls under the scope of **new section 476.5.**

New section 476.5 gives immunity from civil and criminal liability for staff or agents of the Australian Secret Intelligence Service (ASIS) and the Defence Signals Directorate (DSD) for computer-related acts which are done 'in the proper performance of a function of the agency'. These acts may be done either inside or outside Australia, although in the former case the act must be directly related to the overseas activities of the agency. What constitutes 'proper performance of a function' is not defined. The concept does appear in the Intelligence Services Bill 2001, although again it is not defined. Both Bills are also silent on how it might be determined whether a person's actions constituted proper performance of an agency function. This is important issue given the severe criminal penalties under the Bill. Readers should refer to the Digest on the Intelligence Services Bill 2001[21] for more discussion on the issue.

Division 477 - Serious computer offences

New section 477.1 deals with unauthorised access, modification or impairment with intent to commit a 'serious offence'. A serious offence is defined as one that is punishable by imprisonment for five years or more, including life sentences. **New section 477.1** actually creates two offences. The first is where the unauthorised access, modification or impairment is by means of a 'telecommunications service' - in this case the serious offence can be either a Commonwealth, State or Territory offence. The second offence applies where no telecommunications service is involved, and in this case the serious offence must be one under Commonwealth law. This latter restriction is because the lack of a telecommunications service element removes the Commonwealth's ability to legislate under section 51(v) of the Constitution.

New 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 relevant fault elements under the Criminal Code for this offence are *intention* to do the act which causes unauthorised access, modification or impairment, but only *recklessness* as to whether the act will cause that access, modification or impairment.

Recklessness is defined by section 5.4 of the Criminal Code as:

> A person is reckless with respect to a result if:
>
> (a) he or she is aware of a substantial risk that the result will occur, and
>
> (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

New section 477.1 also provides that it is not necessary 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 and/or that the offence falls within the definition of serious offence. This approach is consistent with other criminal code offences such as burglary. In addition, the intended serious offence does not have to be committed or completed in order for a new section 477.1 offence to occur, nor is the fact that it was actually impossible for it to have been committed or completed a bar to conviction. However, an *attempt* to commit a new section 477.1 offence is not itself an offence.

The penalty for committing a **new section 477.1** offence is not to exceed the penalty for the serious offence.

New section 477.2 makes it an offence, subject to Commonwealth constitutional power, 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[22], security or operation of, any data held in a computer or is reckless as to any such impairment. One or more of the following circumstances must exist so as to confer Commonwealth constitutional power: the modification or data affected must involve a telecommunications service, or Commonwealth computer, or data held on behalf of the Commonwealth: **new paragraph 477.2(1)(d). New subsection 477.2(2)** applies absolute liability to the circumstances listed in 477.2(1)(d), meaning that the prosecution does not have to show that, for example, the accused knew the data in question was held in a Commonwealth computer. This also means there is no defence of mistake of fact - thus a person could not plead that they thought the data impaired related to a private computer network when in fact it involved Commonwealth computers or data.

In a similar way to 477.1, a person may be guilty of a 477.2 offence if their actions do not actually result in any impairment. According to the Chapter 4 report, there are three broad situations that the offence is likely to cover:[23]

- a person with limited authorisation impairing data by engaging in an unauthorised operation on data
- a hacker who obtains unauthorised access over the Internet and modifies data and causes impairment, and
- a person who circulates[24] a disk containing a computer worm or virus which infects data.

The *Explanatory Memorandum* to the Bill comments:[25]

> The proposed offence is limited to instances where a person modifying computer data intends to impair data or is reckless as to causing impairment. The existing offence contains no such limitation and merely requires that the person modify the data intentionally and without authority or lawful excuse (Crimes Act, paragraphs 76C(a) and 76E(a)). The existing offence is too broad and vague for a maximum 10 year penalty, as it extends to the harmless use of another person's computer without that person's permission.

The penalty for committing a **new section 477.2** offence is up to 10 years imprisonment.

New section 477.3 makes it an offence, subject to Commonwealth constitutional power, for a person to cause any unauthorised impairment of electronic communication to or from a computer, where the person knows the impairment is unauthorised, and either intends to impair electronic communication or is reckless as to any such impairment. In relation to **new section 477.3**, constitutional power would only be conferred where the electronic communication that is impaired occurs by means of a telecommunication service or is to or from a Commonwealth computer. As for 477.2, absolute liability would apply to these Commonwealth jurisdictional connections.

'Impairment of electronic communication to or from a computer' is defined in **new section 476.1** as including:

> (a) the prevention of any such communication; or
>
> (b) the impairment of any such communication on an electronic link or network used by the computer;
>
> but does not include a mere interception of any such communication.

Commenting on **new section 477.3**, the *Explanatory Memorandum* to the Bill states[26]

> 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. The proposed offence would extend to situations where a person impairs a computer 'server', 'router' or other computerised component of the

telecommunications system that relays or directs the passage of electronic communications from one computer to another.

The existing offence of interfering with, interrupting or obstructing the lawful use of a computer (Crimes Act, paragraph 76E(b)) applies to conduct that impairs the ability of a computer to send or receive communications. However, it does not clearly cover actions that interfere with the passage of electronic communications to or from computers, for example, by altering addresses, re-routing messages or interfering with the capacity of the telecommunications system to transmit those communications. The proposed offence would cover this conduct.

The proposed offence would only apply to *unauthorised* impairment. Consequently, the offence would not apply, for example, to a refusal by an Internet Service Provider (ISP) to carry certain types of electronic communications traffic on its network if such a refusal is pursuant to a contractual arrangement or an agreement between the ISP and users of the service. Furthermore, this offence, like the other proposed offences, applies only to acts and not to omissions.[27] Therefore, a strike by telecommunications maintenance workers that resulted in impairment of electronic communication, for instance, would not constitute the commission of this offence.

The penalty for committing a 477.3 offence is up to 10 years imprisonment.

Division 478 - Other computer offences

New section 478.1 makes it an offence, subject to Commonwealth constitutional power, for a person to cause any unauthorised access to, or modification of, restricted data. Restricted data is defined to mean 'data held on a computer to which access is restricted by an access control system associated with a function of the computer' An obvious example is a password. In relation to **new section 478.1**, constitutional power would only be conferred where the access to, or modification of, is caused by a telecommunications service, or the data must be held in a Commonwealth computer, or held elsewhere on behalf of the Commonwealth. As for **new sections 477.1-3** offences, absolute liability applies to these Commonwealth jurisdictional connections.

Recommendation 2 of the Senate committee report suggests the definition of restricted data be amended to clarify that the restricted access applies to the data not the computer system.[28] The recommendation seems a sound one.

The penalty for committing a 478.1 offence is up to 2 years imprisonment.

New 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 Commonwealth computer disk, Commonwealth credit card or other Commonwealth device used to store data by electronic means, where the person intends to cause the impairment and knows that the impairment is unauthorised. It is sufficient that the Commonwealth leases the disk / credit card / devices rather it owning them outright. Again, absolute liability applies to the Commonwealth jurisdictional connections.

The penalty for committing a **new section 478.2** offence is up to 2 years imprisonment.

New section 478.3 makes it an offence for a person to have possession or control of data with the intention of committing or facilitating the commission of a Division 477 offence (ie offences under 477.1-477.3).

The offence provisions of **new sections 478.3** and **478.4** implement Article 6 of the draft Council of Europe Convention on Cybercrime. There is no comparable offence existing under the current *Crimes Act 1914*. Commenting on **new section 478.3**, the *Explanatory Memorandum* to the Bill states:[29]

> This offence is designed to cover persons who possess programs or technology designed to hack into other people's computer systems or impair data or electronic communication. For example, a person will commit the offence if the person possesses a program which will enable him or her to launch a 'denial of service attack' against a Commonwealth Department's computer system and intends to use the program for that purpose. It would also be an offence for a person to possess a disk containing a computer virus that the person intends to release over the Internet in order to impair data in infected computers. In both instances, the person would also commit the offence if he or she intends to provide the program to another person for the purpose of enabling the other person to impair electronic communication or computer data.

It is notable that 'possession or control' is defined as including having control of data in a computer that is in the possession of another person, whether that computer is inside or outside of Australia. The *Explanatory Memorandum* does not provide any information about what situations this would cover. However, it is understood that it would be applicable if a person could remotely access data located say on the hard drive of another computer and this access could be used to manipulate or use the data with the intention of committing or facilitating a Division 477 offence.

The fact that it was actually impossible for a Division 477 offence to have been committed is not a bar to conviction under **new section 478.3**. However, an *attempt* to commit a **new section 478.3** offence is not itself an offence.

The penalty for committing a **new section 478.3** offence is up to 3 years imprisonment.

New section 478.4 makes it an offence for a person to produce, supply or obtain data with the intention that data be used by that person or another person for committing or facilitating a Division 477 offence. Data can either be recorded electronically (eg in a computer or data storage device such as a disc) or can be in the form of a document 'in which the data is recorded'. According to *Explanatory Memorandum* to the Bill 'this offence is primarily targeted at those who devise, propagate or publish programs which are intended for use in the commission of an offence'.[30]

The fact that it was actually impossible for a Division 477 offence to have been committed is not a bar to conviction under **new section 478.4**. However, an *attempt* to commit a **new section 478.4** offence is not itself an offence.

The penalty for committing a **new section 478.4** offence is up to 3 years imprisonment.

Item 5 amends note 2 of subsection 109(5) of the *Education Services for Overseas Students Act 2000.* Section 109 deals with unauthorised access to student information. The amendment simply substitutes a reference to the new Part 10-7 of the *Criminal Code Act 1995* (ie the provisions inserted by **item 4**) for the *Crimes Act 1914* provisions that are proposed to be repealed by **item 2**.

Item 6 amends subsection 5D(5) of the *Telecommunications Act 1997*. Section 5D deals with obtaining warrants authorising interception of telecommunications. The amendment is for a similar purpose as **item 5**.

Schedule 2 - Law enforcement powers relating to electronically stored data

Items 1-13 amend various sections of Part 1AA of the *Crimes Act 1914*. Part 1AA governs the issue and use of search warrants. In general, Part 1AA allows magistrates and authorised Justices of the Peace to issue search warrants if they are satisfied that evidential material may be at a nominated premises at any time within 72 hours of issuing the warrant.[31] Warrants authorise the seizure of things nominated in the warrant, but other evidential material may also be seized if an officer believes that this is necessary to prevent its concealment, loss, destruction etc.

Items 1-4 incorporate a range of definitions into the Part 1AA. With one minor, but curious exception, these match various definitions created by **new section 476.1** in **item 4** of **schedule 1**. The exception is that **item 3** - the definition of data storage device - does not include the words '(for example, a disk or file server)' that its counterpart in Schedule 1 does. The *Explanatory Memorandum* incorrectly states that the two definitions are 'matches'.[32] Presumably the omitted words in **item 3** are a drafting oversight, although of only minor importance.

Item 5 deals with a situation where a search warrant has been issued but it is unclear at first instance whether a thing falls within the scope of the warrant or is otherwise be able to be seized as evidence. **Item 5** provides that a thing (such as a computer or data storage device) may be moved from the search premises to another place for examination or processing, where either it is 'significantly more practicable'[33] than examining or processing the thing at the search premises and where 'there are reasonable grounds to believe…[it]…contains or constitutes evidential material' *or* the occupier consents in writing to the move. As for the existing subsection 3K(3), there is a statutory right for the occupier or their representative to be present during the examining or processing. Under **item 7**, the thing may be removed for up to 72 hours, although this can be extended for an unlimited period by a magistrate or other authorised person if they believe on reasonable

grounds that more time is required to complete the examination / processing.[34] The occupier has a right of being heard in such an extension application. This 'right to be heard' is common in Commonwealth legislation. For example, it is found in subsection 3L(8) of the *Crimes Act 1914*, which relates to securing electronic equipment until an expert is available to examine it.

Item 8 amends existing **subsection 3L(1)** to clarify that electronic equipment on the search premises may be operated by an officer to find data that is present at another location, eg on other computers linked through a network. He or she must believe on reasonable grounds that the data may contain evidential material and that the equipment may be operated without damaging it. Such material may be downloaded on to a data storage device and taken from the premises without the occupier's permission providing that the data storage device was brought to the premises as part of the search exercise. This provision has attracted significant comment during the committee inquiry.[35] However, it is notable that the Attorney-General's Department suggested in evidence before the committee that remote accessing of evidential material was already implicitly permitted under section 3L(1) and that item 8 was intended to 'make the law clearer'.[36] Section 3L(1) states:

> The executing officer or a constable assisting may operate electronic equipment at the premises to see whether evidential material is accessible by doing so if he or she believes on reasonable grounds that the operation of the equipment can be carried out without damage to the equipment.

If Attorney-General's Department view is correct, **item 8** actually incrementally tightens the law by requiring the executing officer must believe on reasonable grounds that data to be remotely accessed might constitute evidential material. However, an executing officer would not be required to notify the operators / owners of computers not on search premises if data held on those computers is accessed under warrant.

Another issue that was raised in relation to **item 8**, but also relevant to **items 12, 24 and 28**, was privacy concerns about the data and other information collected from the operation of computers during searches. This was mainly prompted by the wide range of information that may have been collected but subsequently found not to be evidential material. The submission from the Office of the Federal Privacy Commissioner suggested that, for example, personal information that is not evidential material be destroyed within three months unless this time is extended by a senior officer.[37] In oral evidence to the Senate committee, officials from the Attorney General's Department commented:[38]

> There are various safeguards to protect the privacy of information, which 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 two years imprisonment under the secrecy provisions in the *Australian Federal Police Act 1979* for any improper recording or disclosure of information. The AFP has said that they will review their guidelines on recording, disclosure and storage of information in light of the new offences and investigation powers.

> Consultation about those guidelines is occurring with the Federal Privacy Commissioner. The vigour with which that was being pursued was quite evident immediately after the last hearing. While I do not have anything to give you today, I am very certain that those responsible for considering this legislation will require a progress report or some evidence of progress on that. As soon as we can do that we will give it to you.

In addressing this, recommendation 3 of the Senate committee report stated:

> 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.

Items 9-11 make minor amendments to various parts of section 3L consequential on **item 8**.

Item 12 inserts **new section 3LA** which would enable an officer to apply to a magistrate for an order requiring a specified person to provide any reasonable assistance or information to enable an officer to access, copy or convert data. Before granting the order, the magistrate would have to be satisfied (i) of the existence of reasonable grounds to suspect a computer on search premises contains evidence of an offence, or such evidence is accessible from the computer; (ii) that person(s) named in the order is reasonably suspected of committing the offence specified in the search warrant, or is the owner of the computer or computer system to be accessed, or a current employee of the owner; and (iii) that the person specified in the order has knowledge of the computer or system or measures applied to protect the computer or system.

The maximum penalty for non-compliance with the order would be 6 months imprisonment.

This provision attracted significant criticism on the grounds that a person failing to comply with an order because, for example, they had forgotten the information necessary to grant the access sought by the executing officer, might have to prove that they had truly forgotten it to escape prosecution. It has been suggested that the **new section 3LA** include provisions about how a person could demonstrate that they cannot comply with a **new section 3LA** order for valid reasons and thus not be subject to potential prosecution. Recommendation 4 of the Senate inquiry suggested that paragraph 3LA(2)(c) be amended to ensure that the magistrate issuing the assistance order be satisfied that a person the subject of the order must have 'relevant knowledge' of the computer, its network, or the data security system, rather just 'knowledge' of these matters.[39]

Another issue was whether this assistance order could be seen as possibly compelling a 'form of self-incrimination'. The Attorney-General's Department rejected this view, commenting that:[40]

> I do not think I have ever brought forward a piece of legislation here without someone saying that the right to self-incrimination is being threatened in some way or another. The point is that it 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 grounds that it would incriminate them. An 'assistance order' is different in that it does not require a person to produce particular data; it only requires the person to provide information necessary to enable a law enforcement officer to get access to the computer. Once they have got access to the computer, the officer still has to search for it and find it.

An assistance order typically takes the form where, as part of a search of premises under the power of a warrant, certain persons on the premises are required by the relevant legislation to provide the executing officers 'with all reasonable facilities and assistance for the exercise of their powers'.[41] Again typically this obligation does not extend to providing any documents requested by the officer if this would tend to incriminate the person the subject[42] of the request. Note that the privilege against self-incrimination - which is common law concept - can be nullified if the relevant legislation specifically requires that documents be provided or if there is some reasonably clear intent in the legislation for the privilege not to apply.

Under the common law, it is clear that a person cannot refuse access to premises (so as to prevent search and seizure of documents) by executing officers under the privilege against self-incrimination. The privilege does allow a person to decline to reveal the whereabouts of documents. Unfortunately, there does not seem to be any obvious case law directly on the point of what degree of assistance a person must provide to access documents. **New subsection 201A(2)** provides that an order requiring a person to provide access to computer data can only be granted if the magistrate has reasonable grounds for suspecting that evidential material is held in a computer or accessible from it. Although not absolutely beyond doubt, the best view of **section 201A** orders are that they are not inconsistent with the common law privilege against self-incrimination.

Item 13 is an amendment consequential on **item 12**.

Items 14-30 amend various aspects of the *Customs Act 1901*, particularly the powers of Customs officers acting pursuant to a search warrant under sections 200-202, which are very similar to those of police officers under the Crimes Act. The main amendments mirror those by made by **items 5,7, 8** and **12** of Schedule 2.

Item 21 is identical to that in **item 5**.

Item 23 is identical to that in **item 7**.

Item 24 is identical to that in **item 8**.

Item 28 is identical to that in **item 12**.

Item 31 provides that the changes made by **Schedule 2** only apply to warrants issued after the comment of the schedule.

Concluding Comments

The existing computer-related crime provisions in the *Crimes Act 1914* certainly need updating. The passage of the Bill, if amended by the generally sound recommendations of the Senate committee, will create an appropriate range of offences to match the growth in computer use and crime since Part VIA of the *Crimes Act 1914* came into effect over ten years ago.

Some submissions to the Senate committee raised concerns that some legitimate activities, such as the operations of persons working in the security computer industry who use tools similar to those employed by so-called 'hackers', may face some risk of falling within the technical definitions of some of the Bill's offences.[43] Fairly similar views have been expressed by the Australian Democrats.[44] The ALP has also been critical of what it sees as a lack of consultation with the information technology industry in the development of the Bill, although it appears to concede that this criticism does not apply to the Model Criminal Code Officers Committee process in drafting the Chapter 4 report.[45] While perhaps the majority of the various concerns expressed in the submissions seem to be adequately dealt with by the responses of the Attorney-General's Department, the relative newness of some the Bill's technical provisions would seem to justify the Australian Democrats recommendation in the Senate inquiry report 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.[46]

Endnotes

---

1 *Review of Commonwealth Criminal Law: Interim Report on Computer Crime*, Attorney General's Department, November 1988.

2 The committee members consist of officials from all Commonwealth, State and Territory jurisdictions and is chaired by a justice of the NSW Supreme Court.

3 *Report on Chapter 4 - Damage and computer offences and amendment to chapter 2: jurisdiction,* Model Criminal Code Officers Committee of the standing Committee of Attorney's General. January 2001.

4 Chapter 4 report, p. 89.

5 'United efforts against Cybercrime' *Media release* Senator the Hon Chris Ellison, 25 July 2001

6 This code of prohibitions is supplemented by the sabotage offences of Part 4.3, which impose severe penalties for conduct which is intended to cause major damage or major disruption to government facilities and public infrastructure. These offences, which were developed from international proposals for anti-terrorism legislation, extend across the saboteur's destructive gamut, from bombs to computer viruses.

7 See *Jones v Commonwealth* (1965) 112 CLR 206.

8 The term is not used in the Chapter 4 report.

9 Senate Legal and Constitutional Legislation Committee Report on the Cybercrime Bill tabled 21 August 2001. The report of the committee can be viewed at http://www.aph.gov.au/senate/committee/legcon_ctte/cybercrimebill01/cybercrime_bill01.pdf

10 See new section 476.4, which allows the concurrent operation of State or Territory law.

11 A physical element is one of the things that must be proved in order for a prosecution to be successful. Serious crimes also require a mental element to be proved.

12 Under Part 2.2 of the Criminal Code, conduct is defined as meaning 'an act, an omission to perform an act or a state of affairs'.

13 Alex Steel, Submission no. 17 to the Senate Legal and Constitutional Legislation Committee Inquiry into the Cybercrime Bill.

14 Ibid, p. 2. These and a range of related concerns were addressed by the Attorney-General's Department in submission no. 20A to the Senate committee inquiry. The Committee appeared to be satisfied with the Department's assurances that the offences contained appropriate fault elements and would not apply to innocuous activities: Report on the Cybercrime Bill, pp. 14-15.

15 *Explanatory Memorandum*, p. 6.

16 At pp. 141–47.

17 The committee noted that it had taken a similar position in relation to its 1995 Theft, Fraud Bribery and related Offences report: '[we take] the view that entry pursuant to permission should not be trespassory, even though accompanied by the intention to steal or commit another offence.' Chapter 4 report, p. 141.

18 The concept of 'substantially contributes' is found elsewhere in the Criminal Code, although only a few places such as section 146.2 'causing harm to Commonwealth public officials'.

19 See section 15.1 of the Criminal Code.

20 This example is taken from p 7 of the *Explanatory Memorandum.*

21 *Bills Digest* No.11, 2001–02 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd011.pdf

22 Concerns about the meaning of 'reliability' were also expressed in Senate submissions: submission no. 17, op cit, p. 3.

23 See p. 163.

24 See section 11.3 of the Criminal Code - Innocent agency. Essentially the person circulating the disk to another, knowing that it will result in the unauthorised data modification, is procuring an innocent party to cause the modification and thus themselves guilty of the offence.

25 At p. 9.

26 At p. 10.

27 This is because of the operation of section 4.3 of the Criminal Code, which deals with omissions in the context the Code's Part 2 'principles of criminal responsibility'.

28 Report on the Cybercrime Bill, p. 19.

29 At p. 12.

30 *Explanatory Memorandum*, p. 13.

31 The exact requirements for issuing of a warrant are detailed in section 3E of the *Crimes Act 1914*.

32 *Explanatory Memorandum*, p. 14.

33 Regard must be had to timeliness and cost of processing or examining the thing at another place rather than on site and to the availability of expert assistance.

34 Senate inquiry recommendation 5 and 6 also relate to the issue of extension of examination time.

35 See for example, submission by the Communications Law Centre (submission no. 3), pp. 2–3.

36 Senate inquiry hearing transcripts, p. 25.

37 Submission no.11 p. 1.

38 Senate inquiry hearing transcripts, p. 39.

39 Although in any prosecution against a person for failure to comply with a **new section 3LA** order, if that person claimed that they did not have the necessary knowledge to comply, the prosecution would carry the burden of proving that the person did in fact have the necessary knowledge.

40 Senate inquiry hearing transcripts, p. 40.

41 For example, section 53 of the *Fuel Quality Standards Act 2000.*

42 Note that the common law privilege against self-incrimination does not apply to companies: *Environmental Protection Authority v Caltex Refining* (1993) 178 CLR 477. Thus an employee could not claim the privilege if a document incriminated the company (or indeed another person) rather than themselves.

43 See for example, submission no.4 (2600 Australia), section 4a and 6j.

44 Senator Brian Greig 'A clumsy step in the right direction' *Canberra Times* 30 July 2001

45 Report on the Cybercrime Bill, p. 33.

46 Ibid, p. 43.