SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

INQUIRY INTO ENTRY, SEARCH AND SEIZURE PROVISIONS IN COMMONWEALTH LEGISLATION

SUBMISSION NO : 4

SUBMISSION BY :

Mr Philip N Argy
Vice President
Australian Computer Society, Inc.
PO Box Q534
QVB SYDNEY NSW 1230

DATE : 29 June 2004

CONTACT : Mr Philip Argy

PHONE : (02) 9299 3666

FACSIMILE : (02) 9299 3997

EMAIL : Philip.Argy@mallesons.com

NO. OF PAGES : 7

AUSTRALIAN COMPUTER SOCIETY

Australian Computer Society Inc.
ABN 53 156 305 487

National Secretariat
Level 3
160 Clarence Street
Sydney NSW 2000 Australia

PO Box Q534
QVB Sydney 1230

Telephone: (02) 9299 3666
Facsimile: (02) 9299 3997
Email: info@acs.org.au
Internet: www.acs.org.au

A member of the
Australian Council of Professions

29 June 2004

The Chair
Senate Standing Committee for Scrutiny of Bills
Room SG49
Parliament House
CANBERRA ACT 2600

Dear Sir/Madam

RE: ENTRY AND SEARCH PROVISIONS INQUIRY

Thank you for your invitation of 13 April 2004 to submit our views to the above inquiry.

The Australian Computer Society believes that its views on the relevant issues were sufficiently canvassed in its 18 July 2001 submission to the Senate Legal and Constitutional Legislation Committee's Inquiry into the Provisions of the Cybercrime Bill 2001. The Standing Committee for the Scrutiny of Bills is respectfully invited to consider our submission on that occasion to reflect our current views on the subject matter.

Kind regards

Philip N. Argy
Vice President

AUSTRALIAN COMPUTER SOCIETY

18 July 2001

OUTLINE SUBMISSION BY AUSTRALIAN COMPUTER SOCIETY INC

Senate Legal and Constitutional Legislation Committee

Inquiry into the Provisions of the Cybercrime Bill 2001

Introduction

1 The Australian Computer Society Inc supports the proposed legislation in principle so far as it reflects Parliament's intention to implement the basic recommendations of the January 2001 Model Criminal Code *Damage and Computer Offences Report* (the "**Officers' Report**"). However, the Society has some serious concerns about the specific language used in many of the provisions. The Society also has serious reservations about the powers conferred upon statutory agencies being broadened beyond ensuring that current investigatory powers are available in respect of offences suspected of being committed utilising modern technology.

2 In the same way that the Society would oppose any new offence of murder by laser gun, on the basis that the offence of murder is a crime regardless of the means employed, so too does the Society regard some of the newly proposed offences as unnecessary. The Society would prefer to see a more rigorous review of existing law to enable appropriate 'tweaking' to be effected rather than the creation of a new parallel universe which may or may not overlap existing provisions. This is so despite the Model Code from which the Bill is derived having itself been based to a considerable extent on the UK Computer Misuse Act 1990 and there having been considerable effort expended by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General in preparing the Officers' Report.

3 The approach preferred by the Society is to ensure that definitions of "record" and "data" for example are modified (as is indeed proposed) so that conventional offences, such as *alteration of a record with intent to deceive* or *obtaining property by deception,* are thereby covered without the need for more computer-specific offences. Only where there are activities in relation to computers which have no historical analogue does the Society accept the need for specific provisions, and for the most part the proposed legislation seems to implement that approach where it tracks the provisions of the Model Code.

4 The Society respectfully submits that it is incumbent upon the Explanatory Memorandum for any Bill before Parliament that purports to implement an external report or recommendation to acknowledge, explain and justify any departures from the report or recommendation. In the case of the Cybercrime Bill 2001 **the Society's most serious concerns are directly attributable to unacknowledged and unjustified departures from the Model Code set out in the Officers' Report.**

5 The Society's specific comments relate primarily to the proposed new Part 10.7 of the Criminal Code but comment is also made on the proposed enhanced investigative powers for ASIO and other agencies.

Proposed Part 10.7 Criminal Code

6 A large number of our objections concern definitions that are much wider than appropriate. This is entirely contrary to this passage on page 91 of the Officers' Report, which states in relation to a (rejected) general offence of obstructing lawful use of a computer:

> *"The explosive growth in the number of people using computers, the variety of uses to which they are put, coupled with the intractable problems of defining what is and is not a computer, should preclude blunderbuss prohibitions of this nature. One might just as well argue for offences of impeding the lawful use of a television or record player"*

7 On page 95 of the Officers' Report the following passage also appears:

> *It is important to emphasise, however, that techniques and tactics involving encryption, the use of trademarks in metatags, bulk spam, anonymity and disguised identity are all capable of legitimate use. Legitimate resort to these techniques and tactics may, indeed, be more common than illegitimate use. None of these practices can be banned outright nor do they indicate that the individual is engaged in some nefarious enterprise.*

8 These two passages underlie both the Society's strong support for the intentions of the Bill, and the basis of its serious reservations about the language that is proposed. Unfortunately, by reason of the awesome breadth of the definitional language employed, seemingly reasonable provisions are converted into precisely the blunderbuss prohibitions the Committee was seeking to avoid, and leave legitimate everyday activity vulnerable to prosecution by misguided if not over zealous enforcement authorities. This effect must be guarded against at all costs. The Society fundamentally rejects an approach which in essence sacrifices such concerns for the sake of the broader objectives of the Bill.

9 Whilst the discussion at pages 123 to 131 of the Officers' Report is sensitive to the "overreaching" potential of some of the language proposed, it does not always propose a satisfactory solution. The Bill, therefore, inherits the broad approach of the Model Code in these respects.

10 The definition of telecommunications service is far broader than the public network, and goes well beyond any telecommunications service covered by the Telecommunications Act. It plainly includes private internal networks, and probably even includes two or more computers connected in a private residence. The consequences of such a broad definition are that offences that involve "impairment" of a telecommunications service can encompass activities as trivial as printing a large file which will inevitably slow other traffic on a small network of inadequate capacity. Nowhere in the legislation is any regard paid to the need for the prohibited impairment not to be attributable to any inherent inadequacy of the telecommunications service the operation of which may be impaired. In those circumstances, all persons with knowledge of the inadequacy could be taken to intend to impair the operation of the service if they use it to transmit a large file.

11 Clause 476.2(3) is similarly of concern because the accused need only have "substantially contributed" to any impairment. The Society believes that Parliament needs to make explicit that the offence is not committed where the impairment is substantially attributable to inadequate capacity in the telecommunications service concerned, even if the accused was aware of that fact. The Society does not by this suggestion mean to exclude from any offence the taking advantage of known security inadequacies in any service or system; the suggestion is confined to exempting mere impairment of the communications service by some non-malevolent conduct.

12 Equally concerning is the impact of the broad definition of telecommunications service in those provisions which prohibit alteration of data where that is effected by means of a telecommunications service. Short of altering data held on a single standalone computer, all other connected data storage devices or other computers can only be accessed or operated upon by means of a telecommunications service. The definition thus effects a very significant broadening of reach of the proposed offence provisions.

13 Provisions which are described as "preparatory" (such as clause 477.1) are tolerable only on the basis that an otherwise overreaching provision is constrained by the concurrent requirement of an intention "to commit, or facilitate the commission of, a serious offence". However, offences such as those in clause 477.2 are not so constrained. Taking clause 477.2 as an example, which well illustrates the Society's concerns:

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

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

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

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

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

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

(d) one or more of the following applies:

....

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

....

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

Penalty: 10 years imprisonment

....

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:

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

(b) the reliability, security or operation, of any such data."

14 Although this language reminds one of John Perry Barlow's famous quote about the potential for there to be "government by the clueless, over a place they've never been, using means they don't possess", the humour is short lived. When read in conjunction with the definitions, such as clause 476.1 and 476.2(3), the provision becomes quite dangerous. Its departure from the more circumscribed form of section 4.2.5 of the Model Code is neither acknowledged nor justified by the Explanatory Memorandum.

15 Here are just two examples of innocuous conduct that would become serious criminal offences under the proposed provision:

> An Australian employee modifies before sending an external email composed by her boss by adding a graphic to it without his permission to make a humorous point, knowing full well that the company's policy is that graphics are not to be used because they use up communications bandwidth and may slow other people's emails. *Should this person face 10 years' imprisonment? More critically, what defence is available to the hapless employee under the proposed provision? And the commission of that offence would also constitute a separate offence under clause 477.1 because the offence under clause 477.2 attracts a penalty in excess of five years' imprisonment!*

> A person receives a cookie from a web site and decides to alter it to avoid what the recipient regards as a privacy intrusive practice. Alteration of the cookie is plainly not authorised by the sender of the cookie. Retrieval of the cookie on the next visit to the web site will plainly cause the retriever's computer to behave in some way other than would have been the case had the cookie not been altered. Viewing a web page on someone else's site will always involve use of a telecommunications service. *Should this person also face 10 years' imprisonment? And what defence is available under the proposed provision?*

12 Even under the Model Code's more constrained provisions of section 4.2.5, the Officers' Report notes (at page 165) that the "net is cast more widely here than it is in s3 of the UK *Computer Misuse Act 1990*, which requires proof of intention to impair data". In the Society's view some malevolent intent should be made an express element of all offences under the Bill. There may be situations where recklessness reaches a level of criminality that requires sanction, but in the Society's view it would be rare that criminal recklessness of the kind the proposed clause targets is not accompanied by disingenuity sufficient to establish the requisite level of malevolent intent.

13 Clause 476.2(1) makes "unauthorised" synonymous with "not entitled to cause". It is not easy to discern the rationale for this interpretative provision (which is the same in the Model Code), but in the Society's view it has the potential to deprive an accused of a defence of honest and reasonable belief.

14 In general terms, and subject to the Society's criticisms of the language of some of the substantive offences, the Society is supportive of the "possession with intent" provisions. However the Society recommends the inclusion of an express exculpatory provision entitling a Court to find that "in all the circumstances the accused's conduct ought not be regarded as criminal". Indeed such a provision might usefully be inserted as a more general provision for the whole of Part 10.7.

Schedule 2 - Law Enforcement Powers

15 The Society believes that strong enforcement and, more importantly, strong education of enforcement agencies, is a significant element in fighting computer-related crime. Until there is a perception that there are both strong laws and a strong likelihood of apprehension and conviction, there is likely to be an increasing proliferation of computer related crime. However, the Society is also very concerned to ensure that civil liberties are protected, and that strong legislation is not able to be used by law enforcement agencies for harassment or other ulterior purposes. To ensure this the investigative powers that are conferred need to be subject to proper judicial or similar level of supervision and scrutiny, and provisions which are intended to enhance investigative powers need to be carefully worded to avoid scope for misuse.

16 By way of example of the Society's concerns in this regard, the definition of "*data storage device*" inserted in s.3C(1) of the *Crimes Act 1914* by clause 2 of Schedule 2 differs from the definition of the same term in clause 476.1 of proposed Part 10.7 of the Criminal Code. This difference is the omission in the former case of the words *"(for example, a disk or file server)"*. Whilst at first blush an apparently trivial difference, in the Society's view the omitted example is vital to indicate to both the enforcement agency and any judicial officer approached to approve any investigative action, that "*contain*" means "*embody*". In other words, a plastic case containing diskettes would be within the definition of a *data storage device* under the proposed definition in the *Crimes Act* but plainly not within the definition of the same term in the *Criminal Code*. This criticism applies equally in relation to the same definition inserted by clause 19 in s.183UA(1) of the *Customs Act 1901*.

17 The proposed new s.3LA (inserted by clause 12 of Schedule 2) needs to be confined so that the persons against whom orders can be made are only persons with the knowledge necessary to allow the executing officer to do what he or she is otherwise authorised to do. As presently worded, any employee of an organisation with even the most superficial knowledge of the organisation's computer network (eg, our computers are connected to a network by a cable that runs under my desk) can be the subject of an order to provide whatever assistance an executing officer may require. Unlike provisions of this kind that one sees in other legislation, which include language such as "without lawful excuse", the proposed section makes compliance with an order to assist mandatory. One would have to assume that non-compliance through lack of the required knowledge would be excused, but the legislation does not appear to allow for this.

18 The Society respectfully suggests that "relevant" be inserted before "knowledge" in proposed subsection 3LA(2)(c) and that "without lawful excuse" be inserted after "fails" in proposed subsection 3LA(3).

This outline was prepared by:
Philip N Argy
Vice President
and
Chairman, Economic, Legal and Social Implications Committee
Community Affairs Board
Fax (61 2) 9296 3954
mailto:pargy@acslink.net.au
http://www.acs.org.au/