The Senate

Environment, Communications, Information Technology and the Arts Legislation Committee

Communications Legislation Amendment Bill (No. 2) 2003

September 2003

ISBN 0 642 71299 9

This document was printed by the Senate Printing Unit, Parliament House, Canberra

Committee membership

Members
Senator Alan Eggleston, Chair (LP, WA)
Senator Sue Mackay, Deputy Chair (ALP, TAS)
Senator Andrew Bartlett (AD, QLD)
Senate Kate Lundy (ALP, ACT)
Senator Santo Santoro (LP, QLD)
Senator Tsebin Tchen (LP, VIC)

Substitute Members
Senator John Cherry (AD, QLD) to replace Senator Bartlett for matters relating to the Communications portfolio
Senator Gary Humphries (LP, ACT) to replace Senator Tchen for the hearing on the Bill held on 5 September 2003

Participating Members
Senator the Hon Eric Abetz (LP, TAS)
Senator the Hon Nick Bolkus (ALP, SA)
Senator the Hon Ron Boswell (NPA, QLD)
Senator Bob Brown (AG, TAS)
Senator George Campbell (ALP, NSW)
Senator Kim Carr (ALP, VIC)
Senator Grant Chapman (LP, SA)
Senator Stephen Conroy (ALP, VIC)
Senator the Hon Helen Coonan (LP, NSW)
Senator Christopher Evans (ALP, WA)
Senator the Hon John Faulkner (ALP, NSW)
Senator Alan Ferguson (LP, SA)
Senator Jeannie Ferris (LP, SA)
Senator Brian Harradine (IND, TAS)
Senator Leonard Harris (PHON, QLD)
Senator Gary Humphries (LP, ACT)
Senator Susan Knowles (LP, WA)
Senator Meg Lees (AD, SA)
Senator Ross Lightfoot (LP, WA)
Senator Jan McLucas (ALP, QLD)
Senator Brett Mason (LP, QLD)
Senator Julian McGauran (NPA, VIC)
Senator Shayne Murphy (IND, TAS)
Senator Kerry Nettle (AG, NSW
Senator Robert Ray (ALP, VIC)
Senator John Watson (LP, TAS)
Senator Penny Wong (ALP, SA)

Committee Secretariat

Mr Michael McLean, Secretary
Mr Frank Nugent, Principal Research Officer
Mrs Sharon Babyack, Executive Assistant

Committee Address

Environment, Communications, Information Technology and the Arts Legislation Committee
S1.57, Parliament House
Canberra ACT 2600

Tel: 02 6277 3526
Fax: 02 6277 5818

Email: ecita.sen@aph.gov.au

Internet: http://www.aph.gov.au/senate/committee/ecita_ctte/index.htm

TABLE OF CONTENTS

Referral and conduct of the inquiry

1.1 On 20 August 2003 the Senate resolved, in accordance with the recommendation of the Selection of Bills Committee, that the Communications Legislation Amendment Bill (No. 2) 2003 (the Bill) be referred to the Environment, Communications, Information Technology and the Arts Legislation Committee for inquiry and report by 9 September 2003.[1] The Senate subsequently agreed to extend the reporting date to 15 September 2003.[2]

1.2 The Committee invited submissions on the Bill in an advertisement in *The Australian* on Wednesday, 27 August 2003. It also wrote direct to a number of relevant organisations inviting submissions. The Committee received two submissions on the Bill which are listed at Appendix 1. It also held a public hearing in Canberra on Friday, 5 September 2003, details of which are shown in Appendix 2. Following the hearing the Committee received a submission from the Department of Commutations, Information Technology and the Arts clarifying evidence it had given at the hearing.

1.3 The Committee thanks all those who contributed to its inquiry by preparing submissions and by appearing at the hearings.

Summary of the Bill

1.4 The Bill was introduced into the House of Representatives on 26 June 2003 and into the Senate on 19 August 2003.

1.5 In his second reading speech Senator Ian Campbell, Parliamentary Secretary to the Treasurer, stated that the Bill amends the *Telecommunications Act 1997* (Telecommunications Act), the *Australian Security Intelligence Organisation Act 1979* (ASIO Act*)* and the *Administrative Decisions (Judicial Review) Act 1977* (AD(JR) Act) to enhance the security of Australia's telecommunications services and networks and to improve existing arrangements relating to call data disclosure and interception services.[3]

Carrier licensing

1.6 The Bill proposes to insert new section 56A in the Telecommunications Act requiring the Australian Communications Authority (ACA) to consult with the 'agency co-ordinator' (a senior official in the Attorney-General's Department who liaises with national security and law enforcement agencies) before issuing a carrier licence. The agency co-ordinator may then issue a notice to the ACA that it does not require any further consultation about the application or give a written notice to the

---

1 Selection of Bills Committee, Report No. 9 of 2003, 20 August 2003.

2 *Journals of the Senate*, 9 September 2003, p. 2317

3 Senator Ian Campbell, Senate Hansard, 19 August 2003, p 13594.

ACA directing it not to issue a licence. Notices have effect for a maximum of three months, but can be renewed to allow a consultation period of up to 12 months as part of the carrier licensing process.

1.7 Proposed section 58A gives the Attorney-General specific power to direct the ACA not to issue a carrier licence on national security grounds. An amendment to paragraph 1(a) of schedule 4 of the Telecommunications Act will exclude these new provisions from review by the ACA, and also from review by the Administrative Appeals Tribunal.

1.8 The Bill does not propose that telecommunications providers with current licences retrospectively undergo a similar procedure. However, new sub-section 581(3) will allow the Attorney-General to order a telecommunications carrier to stop using or providing telecommunications services.

Direction not to supply a service

1.9 The proposed amendments to section 581 will also allow the Attorney-General to give a direction to a carrier or carriage service provider to cease supplying service to particular persons if the Attorney-General considers that the particular use or supply of services is 'prejudicial to security'.

1.10 The Government envisages that the Attorney-General would only use the proposed new powers 'in extreme circumstances' if security issues could not be resolved through consultation and contractual mechanisms. [4]

1.11 During the Committee's hearing clarification was sought about the extent to which this power would also allow the Attorney-General to issue a direction that a service no longer be supplied to a particular individual. It was explained that this power was intended to deal with the introduction of new services which may have security vulnerabilities and was not intended to apply to individuals, although it does do so.[5]

> The draft as it stands certainly appears to do that but the intention was to turn off an actual carriage service of itself, so a carrier or carriage service provider could not provide to itself or any other person or particular service to a group of people out there in the community at large. It was not the intention that it would be targeting an individual service. It was about protecting the telecommunications infrastructure itself and the protection of being able to execute a warrant on a particular carriage service provider.[6]

---

4 Senator Ian Campbell, Senate Hansard, 19 August 2003, p 13594.

5 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 7-8.

6 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 7.

Security assessments

1.12 The Bill does not require a security assessment to be prepared before the Attorney-General uses the proposed new powers to direct that a carrier licence not be issued or that a service not be supplied. The Explanatory Memorandum states only that it is "expected" that the Attorney-General will receive a security assessment from the Australian Security Intelligence Organisation (ASIO) before taking that action.

1.13 The Bill contains amendments to the ASIO Act to bring a security assessment issued for these purposes into line with the existing provisions dealing with security assessments.

1.14 The Bill amends the Act to include the new powers within the definition of a 'prescribed administrative action' under section 35 of the Act. It inserts a new section 38A in the Act which provides that the Attorney-General must notify a person of an adverse or qualified security assessment within 14 days unless it is essential to the security of the nation to withhold such notification. The notice, if issued, must attach a copy of the assessment but any matters the disclosure of which would be prejudicial to the security of the nation may be removed from the notification. The amendments in the Bill also enable appeals to the Administrative Appeals Tribunal by people who receive an adverse or qualified security assessment in connection with the Attorney-General's use of the new powers.

Review of the direction powers

1.15 The Bill proposes to exclude the Attorney-General's new powers in proposed section 58A and subsection 581(3) of the Telecommunications Act from judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (AD(JR) Act). In his Second Reading Speech Senator Campbell said that this 'is consistent with existing exclusions under the AD(JR) Act for similar decisions based on national security considerations.'[7] This will also have the effect of relieving the Attorney-General of the requirement in the AD(JR) Act to provide on request a statement of reasons for the decision.

1.16 The Explanatory Memorandum notes that 'judicial review will still be available in the Federal Court under section 39B of the Judiciary Act 1903 and in the High Court under section 75(v) of the Constitution.'[8]

Interception warrants

1.17 The Telecommunications Act already requires carriers and carriage service providers to give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for safeguarding national security.

---

7 Senator Ian Campbell, Senate Hansard, 19 August 2003, p 13594.

8 Explanatory Memorandum, p 9 and pp 28-9.

The current definition of senior officer contained in section 282 refers, inter alia, to commissioned officers and officers of the senior executive service. The Bill inserts a new definition which takes into account the changes in structure of some law enforcement agencies and requires that the person issuing the certificate has been nominated in writing by the Commissioner of Police or other chief executive officer.

1.18 A new sub-section 313(8) will be inserted into the *Telecommunications Act 1997* to specify that when executing an interception warrant, telecommunications providers are required not only to supply the content of intercepted communications but also all 'relevant information about any communication'. According to the Explanatory Memorandum, this provision aims at ensuring that 'relevant technical data and contextual information about each communication is provided to law enforcement agencies.'[9]

Principal issues raised in evidence

Grounds for exercising the power

1.19 Both major submissions received by the Committee raised concerns about the scope of the discretion provided to the Attorney-General under the Bill. Vodafone was concerned about the subjective nature of proposed section 581(3) which only requires that the Attorney-General, after consulting with the Prime Minister and the Minister administering the Act, consider that the proposed use or supply of a service be prejudicial to security:

> ….. Vodafone submits that it is essential for parliament to ensure that the potential harm to the legitimate business interests of carriers and carriage service providers by a direction under section 581(3) is not disproportionate to relevant risk to national security.
>
> In order to ensure this, Vodafone submits that section 581(3) needs to be amended so that there is an express legislative requirement that the power to is issue a direction under section 581(3) may only be exercised where:
>
> - there are demonstrated grounds that this is necessary to protect national security; and
> - the risk to national security cannot be managed effectively through other mechanisms.
>
> On its current drafting, section 581(3) does not require either of these conditions to be satisfied …..[10]

9 Explanatory Memorandum, p 23.

10 Vodafone, Submission 1, page 5.

1.20 Vodafone attached an annexure to its submission which set out an alternative wording for section 581 which would address its concerns. This issue was raised with Departmental representatives who said that:

> I think what they have said is the actual intention of what exactly will be done. We will need to demonstrate to the Attorney-General, the Prime Minister and the Minister for Communications, Information Technology and the Arts that these risks do apply.[11]

> ….. Certainly, Vodafone were not sure, in relation to this bill, what the level of consultation would be. They will know about it if we have concerns that there is vulnerability within a particular service that they are providing or a particular group that they are providing it to. There certainly would never be any surprises and that is where we would endeavour to consult and talk about perhaps removing the visibility of a particular area to particular parts within their organisation and that sort of thing. There is a determination under part 15 of the Telecommunications Act whereby the agency coordinator can require a particular carrier to describe how they will protect the national security and law enforcement information that is provided to them. It is that kind of process we would envisage that will highlight to them that we have a concern. We will look at what they have to say and try to address it and only in rare and extreme circumstances go to the point of having the Attorney-General make a direction.[12]

1.21 The New South Wales Council for Civil Liberties also raised concerns about the scope of the Attorney-General's power under the proposed amendment. It was concerned that political protest, industrial action and consumer boycotts could all fall within the definition of national security. It referred the Committee to other legislation, such as the *Defence Legislation Amendment (Aid To Civilian Authorities) Act 2000*, which contain exemptions for these types of activities. In response to these concerns Ms Tearne of the Attorney-General's Department advised the Committee that:

> ….. both of the provisions that are contained in the bill with regard to directions on security matters make reference to the fact that security in the context of those provisions has the meaning given in the ASIO Act, and that act defines the concept of security. It defines it by reference to a couple of topics, amongst which are politically motivated violence, attacks on Australia's defence systems et cetera, but it certainly defines the concept and those terms are each further defined within the definitions contained in the ASIO Act. So there is a concept of security. It is defined in the ASIO Act and that definition is picked up in the bill we have before us. I think

---

11 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 24.

12 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 25.

> Cameron Murphy [of NSWCCL] raised concerns in relation to environmental protests, trade union activity and the like.[13]

> ….. the ASIO Act in itself sets out that the act is constrained by the fact that matters of lawful advocacy, protest or dissent and exercise of those rights shall not be regarded in and of themselves as being prejudicial to security, and the functions of the organisation - which include the provision of security assessments - are construed accordingly. So there is some protection by the fact of picking up the definition of security contained in the ASIO Act.[14]

1.22 The relevant provisions of the ASIO Act are reproduced in Appendix 3.

Review mechanisms

1.23 Both Vodafone and the New South Wales Council for Civil Liberties expressed concern that the mechanisms for reviewing a decision by the Attorney-General are inadequate. Vodafone said that there must be a strengthening of the ability of affected parties to have a direction under section 581(3) reviewed if they believed it to be baseless, unsubstantiated or unreasonable:

> A meaningful right to merits and/or judicial review of a decision to issue such a direction is an essential check and balance on the exercise of that power.[15]

1.24 In evidence to the Committee Vodafone expanded on its view of the extent to which judicial review was necessary:

> Our statement is that the requirement for more meaningful judicial review rights is less relevant if the power and the extent to which the power could be relied upon and exercised is clearly defined, whereas at the moment it is quite broadly drafted and quite discretionary in nature. The flip side of that is that you would require more meaningful judicial review rights so as to challenge the boundaries to which that power might be exercised or relied upon.[16]

1.25 The New South Wales Council for Civil Liberties noted that other areas that involve national security issues such as adverse security findings by ASIO are provided with a (limited) process of administrative review through the Administrative Appeals Tribunal or courts utilising the AD(JR) Act. It stated that:

---

13 Anastasia Tearne, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 23.

14 Anastasia Tearne, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 23.

15 Vodafone, Submission 1, page 7.

16 Brian McDonnell, Vodafone, Committee Hansard, Canberra, 5 September 2003, p 15.

> It is beyond the reach of most telecommunications users to take alternative action to restore their services.[17]

1.26 The question of the availability of review mechanisms was raised with Departmental representatives during the Committee's public hearing. In response Ms Tearne, from the Attorney-General's Department, said that:

> ….. To start by reference to the review that is available, the bill does exclude the decisions made under proposed sections 58A and 581(3) from the review mechanisms that are set out in the Administrative Decisions (Judicial Review) Act. It then substitutes, in place of that mechanism, the mechanism that is available in respect of the review of security assessments under the ASIO Act, which is a tailor-made statutory framework for the review of decisions in which there are security aspects. The very simple reason for that is that the Administrative Decisions (Judicial Review) Act framework is not one that is designed to cater for security type issues, whereas the Security Appeals Division has some very specific provisions in the AAT Act that allow for protection of sensitive information and make that forum a much more appropriate one for review of these types of decisions.[18]

1.27 On the issue of the accessibility of the AAT process, Ms Tearne noted that her general understanding was that the process was quite accessible and low cost.[19] In response to concerns raised by the Scrutiny of Bills Committee the Minister identified the other avenues of review which would be available as described in paragraph 1.16.

> There will, however, be a number of avenues for independent review. Judicial review of decisions made by the Attorney-General under the proposed amendments would be available in the Federal Court under section 39B of the Judiciary Act 1903 and in the High Court under section 75(v) of the Constitution.[20]

Security clearance for new carriers

1.28 The Bills Digest suggests that the changes to the carrier licensing provisions amount to the introduction of mandatory security clearances for organisations wishing to provide telecommunications services in Australia.[21] Similarly the New South

---

17 New South Wales Council For Civil Liberties, Submission 2, p 1.

18 Anastasia Tearne, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 28-29.

19 Anastasia Tearne, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 29.

20 Senate Standing Committee for the Scrutiny of Bills, Eighth Report of 2003, 20 August 2003, p 185.

21 Communications Legislation Amendment Bill (No. 2) 2003, Bills Digest No. 21 2003-04, p 2, 8.

Wales Council for Civil Liberties submitted that the amendments will require this step for new licences and questions why there should be any distinction in this regard between existing and new carriers.[22]

1.29 Representatives of the Attorney-General's Department informed the Committee that:

> No, essentially the bill is allowing us to get in under the legislation at an earlier point. The current practice is, in fact, that the Australian Communications Authority advises us when a carrier's licence has been lodged and then gives an opportunity to make contact at that point. All of those processes that are currently in place with the carriers - and I suppose this gets to a standards question - we do actually have some standards in relation to telecommunications interception. We provide technical standards for what we require - auditing standards and access standards - and we apply the Commonwealth Protective Security Manual.
>
> In our negotiations with the current carriers, we require them to meet all of those objectives when they provide interception capability. Probably 99 per cent of the consultation before issuing a carriers licence is to get in early and make them aware of obligations, and we can be aware of any concerns and that sort of thing. Then, with that one per cent, if there are any concerns on national security grounds we can try and manage those. We already have management processes in place with some existing carriers that have licences, where we have asked them to protect national security information and law enforcement security information away from their general management structure when we have been concerned that there may be national security concerns. Of course, there is a distinction because this legislation - if it comes in - will only apply to new carriers licences, and there are already about 90 out there. But the way that we deal with them on a daily basis will be identical.[23]
>
> ….. A security assessment will only be done when we have got to the point where we think that there is potentially a risk to national security. There may be information that has come to light - from ASIO doing their everyday work - that has identified a particular individual, a particular organisation or something like that. In that case, the security assessment will progress. But, on a general basis, I think it is fair to say that 99 per cent will just go through without any security assessment[24]

---

22 New South Wales Council for Civil Liberties, Submission 2, p 2.

23 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 25.

24 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 26.

Interception warrants

1.30 In its submission the New South Wales Council for Civil Liberties expressed concern that the bill would greatly expand the scope of information available under interception warrants. It said that:

> ….. The proposed amendments to Section 313 will radically expand the scope of interception warrants to include all *relevant information about* any communication. This terminology requires clarification, and in its current form will extend far beyond related technical data. This expanded definition could easily allow interception warrants to be used as a 'back door' to gathering substantially more information than under existing warrants to the detriment of the privacy of individuals. National security could become a convenient excuse to increase surveillance or conduct privacy invasive criminal investigation with less accountability.[25]

1.31 In response to these concerns representatives of the Attorney-General's Department stressed that there is no increase in power, but that the provision is intended to assist industry in meeting its obligations. The new provision will make it clear in a different provision within the Telecommunications Act that the information should be provided as subject to a telecommunications interception warrant rather than the current provisions, which are in section 280, which allows information to be provided under warrant.[26]

> Essentially, what these amendments are doing is purely making it beyond doubt that the current reasonable and necessary assistance that is provided under the Telecommunications Act extends to providing that call associated data, call charge records or billing information that everyone has been talking about this morning when a warrant is executed. A far higher standard is required to get an interception warrant than anything like you need to get information currently under the Telecommunications Act. There is a provision within the Telecommunications Act ….. which allows a carrier or carrier service provider to provide this sort of information under full warrant. It has been on that basis that this information has always been provided. However, we are not just dealing with the big carriers; we are dealing with small Internet service providers when the law enforcement and national security execute warrants. Often they are not quite clear on their obligations. The purpose of this is to make it beyond doubt that they are required to provide it.[27]

---

25 New South Wales Council for Civil Liberties, Submission 2, p 1-2. Emphasis in original.

26 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 22.

27 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p 21.

Compensation and protection from liability

1.32 Vodafone submitted that the proposed section 581(3) should be amended so that carriers and carriage service providers are appropriately compensated for any costs they incur and loss or damage that they suffer as a result of complying with a direction issued under that section.

> Vodafone notes that it is presently expressly provided in the Act that carriers, carriage service providers and their officers, employees and agents are not liable to actions or proceedings for damages in respect of an act done or omitted in good faith in the performance of duties under sections 313 or 315 of the Act (see sections 313(5)-(6) and 315(3A)-(3B)).
>
> Vodafone submits that the Bill must be amended to provide similar express statutory immunity to carriers, carriage service providers and their officers, employees and agents in respect of acts done or omitted in good faith in relation to a direction under section 581(3). Carriers and carriage service providers could potentially be exposed to very significant claims in damages and on other bases for ceasing or refusing to supply telecommunications services to their customers in compliance with a direction under section 581(3). It is clearly essential to afford them such bare minimum statutory protection against such claims.[28]

1.33 Departmental officials were invited to comment on this issue although, as noted by the Chairman, it is primarily a policy issue. In response a representative of the Attorney-General's Department said that:

> I think the only comment I would make is that the doctrine of frustration will apply in relation to any carrier's direction to cease to provide a carriage service. There needs to be a distinction made between the provisions under 313 and 315 that Vodafone talked about. In those cases, they have discretion to do certain things; in this case, they will not have discretion. I assume on that basis that their contracts would be frustrated but, in the other cases, they are certainly making decisions based on their own interpretation.[29]

Scrutiny of Bills report

1.34 In its Report on the Bill, the Scrutiny of Bills Committee noted that the proposals are based on a policy relating to the judicial review of decisions based on sensitive material.[30] The Committee said that 'this amendment may make rights or liberties dependent upon non-reviewable decisions but whether it does so unduly is a

---

28 Vodafone, Submission 1, p 7.

29 Catherine Smith, Attorney-General's Department, Committee Hansard, Canberra, 5 September 2003, p. 29.

30 Senate Standing Committee for the Scrutiny of Bills, Eighth Report of 2003, 20 August 2003, p 184-187.

matter for the Senate as a whole.' The relevant extract of the Committee's Report appears at Appendix 4.

Summary and recommendation

1.35 There appears to be little opposition to the objectives of the Bill. The Committee received only two submissions one of which, from Vodafone, expressly supported the objects of the Bill while expressing concerns about some of the provisions.

1.36 The submissions from Vodafone and the New South Wales Council for Civil Liberties raised some important concerns about the scope and operation of the Bill. During the Committee's public hearing, Departmental representatives responded to those concerns and provided the Committee with valuable information about the background to the Bill and the manner in which it relates to existing provisions in the Telecommunications Act and the ASIO Act. Mr Chris Cheah from the Department of Communications, Information Technology and the Arts, noted that the Bill essentially buttresses some of the provisions in existing policy and provides a way of dealing with specific problems when they arise. Similarly, Ms Smith from the Attorney-General's Department explained that the Bill in some ways tightened up the procedures which would be followed in that Department rather than representing any tightening of procedures to be followed by industry.

1.37 Nevertheless the Bill does contain provisions which, as noted by the report of the Scrutiny of Bills Committee, may be considered to trespass unduly on personal rights and liberties. Given this, the Government might care to give consideration to clarifying whether or not the Bill is intended to apply to carriers and carriage service providers, as well as individual persons or only to carriers and carriage service providers, and not to individual persons. If the latter is the case, then an amendment to exclude individual persons from the provisions of the Bill might be appropriate. Against this the Senate must weigh the fact that the provisions of the Bill will make an important contribution to protecting national security and that the powers in the Bill, and the review provisions, are consistent with other legislation dealing with security issues which have been passed by the Senate in recent months.

1.38 The Committee recognises that a fine line must always be drawn between ensuring effective security and protecting longstanding civil liberties. However, the fact that terrorists may use telecommunications services to further their goals demands that the Government must be able to quickly take remedial action. The Committee supports the intention of the Bill to provide an appropriate and effective mechanism to achieve this outcome.

1.39 Accordingly, the Committee recommends:

That the Communications Legislation Amendment Bill (No. 2) 2003 be agreed to without amendment unless the Government chooses to act on the recommendation in clause 1.37 of this Report.

Senator Alan Eggleston
Chair

Australian Labor Party Minority Report

Introduction

1.1 The *Communications Legislation Amendment Bill (No. 2) 2003* makes amendments to the *Telecommunications Act 1997,* the *Australian Security Intelligence Organisation Act 1979*, and the *Administrative Decisions (Judicial Review) Act 1977* seeking to strengthen the national security arrangements for Australia's telecommunications industry.

1.2 A call for submissions was made on 27 August with a closing date of 1 September. Not surprisingly perhaps, given the six day timeline for submissions, only two submissions were received. Mr Cameron Murphy, of the New South Wales Council for Civil Liberties expressed concern in his cover letter to the Committee that several non-government organisations had expressed concerns about the Bill but were unable to make submissions to the Inquiry in the short time frame available. All Senators should reflect on the need to ensure adequate time frames are provided for in Committee inquiries.

1.3 The Bill includes provisions to:

- strengthen national security checks on applicants for carrier licences
- direct carriers not to supply carriage services on national security grounds
- exclude from judicial review under the ADJR Act decisions made by the Attorney General on the national security decisions contained in this Bill
- improve existing call data disclosure and interception arrangements
- change the lodgement date for interception capability plans
- change and arguably loosen the definition of senior officers to certify the disclosure of Carriers and Carriage Service Providers of call data.

1.4 Labor supports the provisions in the Bill which strengthen the national security checking process on applicants for carrier licences. In the current national security environment it is not unreasonable that telecommunications carriers who provide critical infrastructure should face stringent national security checks. While the grounds for refusing carrier licenses are not limited under the Telecommunications Act, this provision expressly provides for a process whereby carrier licence applicants undergo appropriate national security checks.

1.5 Provisions in the Bill to improve existing call data disclosure and interception arrangements and change the lodgement date for interception capability plans are technical amendments that Labor also supports.

1.6 Labor's key concerns with the Bill relate to:

- the power to direct carriers not to supply carriage services on national security grounds;
- the exclusion of judicial review under the ADJR Act for decisions made by the Attorney General on national security grounds under this Bill; and
- the changes to and arguably loosening of the definition of senior officers to certify the disclosure of Carriers and Carriage Service Providers of call data.

This report will now consider these provisions in detail.

Direction not to Supply a Service

1.7 The proposed amendments to section 581 of the *Telecommunications Act 1997* will allow the Attorney General, again in consultation with the Prime Minister and the Minister administering the Telecommunications Act, to direct a person not to use or supply, or to cease using or supplying a carriage service or all carriage services to itself or any other person on national security grounds. This direction may be issued with respect to individuals, groups or telecommunications industry participants, whose activities are deemed to pose a risk to national security.

1.8 Telecommunications services are essential services for all Australians. The new powers in this Bill would theoretically permit, on national security grounds, the Attorney General to cut off a citizen's telephone or Internet service, with limited appeal or compensation rights for affected parties. It is for these reasons that Labor initially expressed some reservations about aspects of these proposed new laws.

1.9 Under this amendment services can be cut off if their use is deemed to be prejudicial to security as defined under the *Australian Security Intelligence Organisation Act 1979*. Under that Act:

security means:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
(i) espionage;
(ii) sabotage;
(iii) politically motivated violence;
(iv) promotion of communal violence;
(v) attacks on Australia's defence system; or
(vi) acts of foreign interference;
whether directed from, or committed within, Australia or not; and
(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph(a).[31]

1.10 It is not inconceivable that organisations such as trade unions or community protest groups could inadvertently fall foul of the security definition provided for in the ASIO Act, and have their telephone or Internet service cut off. Labor does not assume that the Government's purpose is to cut off the phone lines of political activists, but this potential exists in the Bill as it is currently drafted and it cannot be assumed that future administrations will not misuse this power.

1.11 The NSW Council for Civil Liberties described the Attorney General's powers here as "extraordinary" with limited rights of redress or compensation for persons adversely affected by such decisions.[32]

1.12 Under questioning from Senator Lundy, as to whether the provisions of this Bill in regards to ceasing supply of telecommunications services could apply to individuals, the

[31] Australian Security Intelligence Organisation Act 1979.

[32] New South Wales Council for Civil Liberties, Submission, p.2.

Attorney General's Department made the following somewhat extraordinary observation, "it was not the intention that it would be targeting an individual service".[33]

1.13 When further pressed on whether it would be advantageous to cut off the telephone service of a potential security threat, the Department again said it was not the intention of the Bill to cut off an individual's phone service.[34] This contradicts our understanding of the provisions of Section 581, which clearly extend to individuals. This is confirmed by the Explanatory Memorandum of the Bill.

1.14 The Chair's Majority Report agrees that this is a contradiction (1.11).

1.15 The Chair's Report also suggests that these provisions would only be used in 'extreme circumstances'. While the explanatory memorandum states that these powers would only be used in 'extreme cases', this limitation is not expressed in the Bill itself.

1.16 Labor recommends that the Bill be further amended so that it is clear that the proposed amendments to Section 581 do not apply to individuals, in regards to services such as home phone accounts. If the Government's intention is that the Bill does not apply to individuals the Bill should be amended to reflect that.

1.17 If the Government cannot amend the Bill accordingly, Labor believes it should at the very least ensure that adequate administrative appeals mechanisms exist in the Bill so that individuals adversely affected by any decisions under these provisions have adequate and affordable avenues for redress and compensation.

1.18 Labor takes a similar view to Cameron Murphy, when he stated in evidence, "it is all well and good to say that there are these avenues through the federal court and the High Court that allow for judicial review…[but]… the ordinary punter in the street has virtually no capacity to take a matter to the Federal Court or High Court."[35]

1.19 Labor notes the concerns expressed by Vodafone Australia over the proposed new Section 581(3). Although these concerns were not raised by any other carrier, given the short timeframe allowed for submissions, it cannot be assumed that this is not a widespread concern.

1.20 Vodafone similarly submitted, "a meaningful right to merits and/or judicial review of a decision to issue such a direction is an essential check and balance on the exercise of that power". Clearly if the Government persists with proposed Section 581 (3), the appeals process for parties affected by the use of those powers should be improved.

Exclusion of Judicial Review for National Security Decisions

1.21 Proposed amendments to the *Administrative Decisions (Judicial Review) Act 1977* exclude from judicial review under the ADJR Act decisions made by the Attorney General under the proposed amendments on national security grounds. Such national security

---

[33] Catherine Smith, Committee Hansard, Canberra 5 September 2003, p.7.

[34] Catherine Smith, Committee Hansard, Canberra 5 September 2003, p.28.

[35] Cameron Murphy, Committee Hansard, Canberra 5 September 2003, p.17.

decisions are not usually open to judicial review under the ADJR Act as with the ASIO Act, the Intelligence Act, and the Telecommunications Interception Act. Judicial review will still be available in the Federal Court and High Court.

1.22 Again, assuming that the Government persists with the proposed new Subsection 581 (3) applying to individuals, Labor is concerned that this provision may make it even more difficult for individuals or groups to appeal executive decision making under this Bill. If section 581 (3) is not amended to exclude individual services Labor would have difficulty supporting this provision.

Changes to Definition of Senior Officer

1.23 Proposed amendments to subsection 282 of the *Telecommunications Act 1997* arguably loosen the definition of 'senior officers' who can certify the disclosure by carriers and Carriage Service Providers of call data. This amendment is purportedly designed to accommodate current law enforcement agency structures and classifications and reduce delays in the issuing of authorising certificates. The Commissioners, Deputy Commissioners or chief executive officers of relevant agencies will be able to nominate most categories of senior officers.

1.24 According to the Bill's explanatory memorandum, "the proposed amendments will allow greater flexibility in the range of persons that may be specified as senior officers". Further, the Commissioners, Deputy Commissioners or chief executive officers when nominating senior officers will be required to assess the designation of senior officers in an appropriate manner[36]. While some of the change to subsection 282 relate to changes in nomenclature, the provisions mentioned above appear to allow for much greater flexibility in the appointment of senior officers for the purposes of call data disclosure or interception.

1.25 Recent media reports have highlighted the massive expansion of telephone surveillance and interception in Australia. In June this year it was reported that Australian police forces are using telephone taps at 27 times the rate of their US counterparts and that Australia issued 2514 court warrants for telephone taps last financial year, almost double the number in the US.[37] Judging by these statistics the need for broadening and updating laws to expedite related processes is perhaps overstated. There has also been increasing concern in media reports that rogue officers at relatively junior levels within law enforcement agencies may be using telephone interception warrants to tap phones inappropriately.

1.26 The proposed new subsection 282 (10) (c) allows for the definition of officer to include, "a person whose services have been made available to the agency." This extraordinary clause would allow security contractors at law enforcement agencies, not actually employed by those agencies, to become involved in the call data disclosure system. This amendment should be reconsidered by the Government.

1.27 The extension of the definition of 'senior officer' for the purposes of certifying disclosure of call data and the ability of Commissioners, Deputy Commissioners or chief executive officers to nominate 'senior officers' should be carefully reconsidered by the Government. The widespread accessing of call data by inappropriate persons acting under the

---

[36] Explanatory Memorandum, p.22-23.

[37] 'Surveillance Fears on Rise', *The Sunday Tasmanian,* 29 June, 2003.

guise of law enforcement has recently been exposed in the media. We need to ensure that these provisions do not allow for inappropriate access to call data by relatively junior officers who may seek to use such information for non-law enforcement related purposes. These provisions should be tightened to prevent any possible abuses.

Summary and Recommendation

1.28 Labor accepts that under the current security environment measures protecting national security need to be strengthened. But there is an important balance to be struck. Communication networks are vital to our freedom of speech, they are vital to our democracy, they are essential to our standard of living.

1.29 Labor would therefore like to see the *Communications Legislation Amendment Bill no 2* made law as soon as is practically possible so as to ensure that our laws respond appropriately to the changed national security arrangements. Labor has suggested reasonable amendments which we hope the Government will consider in good faith as it is in the interests of all Australians that this Bill is passed forthwith.

1.30 Labor would prefer to see the Bill amended to ensure individuals are not denied access to essential telecommunications services such as the home telephone or home Internet. If the Government insists on these provisions amendments should be made to ensure that citizens are not denied access arbitrarily and that appropriate appeals mechanisms exist including full access to judicial review in regards to private individuals.

1.31 Labor would also like to see the changes to the definition and nomination processes for senior officers tightened considerably. We need to ensure that law enforcement agency personnel do not inappropriately access persons call data. The ability of Commissioners, Deputy Commissioners or chief executive officers to nominate senior officers for these purposes should be strictly regulated and the Government should amend the Bill appropriately.

1.32 Finally, the Government should consider a sunset clause for the Bill of five years, with a review period after four years, so that these matters may be reconsidered in the light of experience.

Senator Sue Mackay
Senator for Tasmania

Senator Kate Lundy
Senator for the ACT

Australian Democrats Supplementary Report

Communications Legislation Amendment Bill (No 2) 2003

The Australian Democrats submit this supplementary report in order to highlight the serious concerns that we have in relation to the Communications Amendment Bill (No 2) 2003.

This Bill contains a range of measures designed to protect the security of Australia's telecommunications services and networks and to prevent their use in the commission of terrorist offences. To this end, the Bill invests the Attorney-General with wide-reaching powers, however there is concern that it goes much further than what is necessary or justified to achieve this purpose. Accordingly, the Bill was referred to the Committee so that its provisions could be considered in detail and to enable interested organisations and individuals to participate in this process and have their views placed on the public record.

Yet, despite the very significant proposals contained in the Bill and the potential for it to affect the rights and liberties of individuals and the interests of businesses, the timeframe for the Inquiry was extremely short. An invitation for submissions was advertised in *The Australian* on Wednesday 27 August 2003, with submissions due only 3 working days later on Monday 1 September 2003.

The New South Wales Council for Civil Liberties (NSWCCL) submission noted that short timeframe for the Inquiry had resulted in the "inability of many interested groups to prepare submissions for the Inquiry". In particular, the NSWCCL made reference to "a number of other non-government organisations including other councils for civil liberties, privacy advocates, and electronic communications groups" that had indicated an intention to provide submissions.

The Democrats question why this bill needs to be so rushed, in the absence of clear evidence of a "threat" needing to be addressed, particularly given the nature at the ministerial powers it proposes.

Turning to the substance of the Bill, the Democrats maintain our serious concerns regarding its provisions as currently drafted. Accordingly, we have concluded that the Bill should be redrafted to provide greater clarity and certainty. In particular, we are concerned that:

- The legislation will allow the Attorney-General to issue a direction that a telecommunications service can no longer be supplied to an individual.
- The grounds upon which the Attorney-General can exercise his or her powers under the Bill are not adequately defined.
- The definition of "security" is too broad for the purposes of the Bill and creates the potential for telecommunications services to be cut off for reasons that extend well beyond the threat of terrorism.

- There is little scope for a meaningful review of an adverse decision.
- The Bill does not provide full statutory immunity for carriers, carriage service providers and their officers, employees and agents in relation to compliance with some provisions.

Direction not to supply a service to an individual

The Democrats are concerned that the legislation will allow the Attorney-General to issue a direction that a service can no longer be supplied to an individual.

While senior Departmental Officials informed the Committee that the legislation was not intended to target individuals, they nevertheless confirmed that it could be used to do so. Acting Assistant Secretary for the Security Law Branch of the Attorney-General's Department, Ms Smith, explained that the intention/policy behind the Bill was to address the risk to the telecommunications industry in executing warrants, and not about individuals, saying "normally that person is not posing that risk to national security in the way envisaged by this legislation". Ms Smith went on to suggest that, because of the way an individual is defined, an individual could be a company, an internet service provider or a person.

It seems clear, therefore, that the powers conferred by this Bill could be used to prevent an individual's access to telecommunications systems and services. Yet the Department expressly states that this is not how the powers are intended to operate.

If the Bill does intend to cover individual persons, the Democrats are concerned that there is no practical process to find out why a service has been terminated or to enable the individual to take steps to restore access where the powers have been exercised in error. This was also one of the key concerns of the Scrutiny of Bills Committee and is subject to further discussion below.

No requirement for ASIO Security Assessment

As highlighted on page 3 of the Committee's report, "the Bill does not require a security assessment to be prepared before the Attorney-General uses the proposed new powers to direct that a carrier licence not be issued or that a service not be supplied". This seems extraordinary that the Attorney-General can make a decision regarding national security without a security assessment, especially given there the lack of adequate review processes.

The Democrats agree with Vodaphone's submission, which calls for an express legislative requirement that there is evidence or demonstrated grounds before the Attorney General uses the power. The Democrats believe that such a requirement for demonstrated grounds could specifically incorporate a requirement for a security assessment from ASIO.

Given the intrusive nature of the powers contained in the legislation, the Democrats firmly believe that the threshold for exercising them must be set sufficiently high.

Obtaining a security assessment from ASIO is rendered even more imperative, given the severely limited rights of review. In the Bill's present form, the only right to review under the *Administrative Decisions (Judicial Review) Act 1977* (AD(JR) Act) is in relation to the ASIO security assessment, itself. No such opportunity for review exists in relation to the decision of the Attorney-General (although it would still be possible to seek a review of that decision in the Federal Court under section 39B of the *Judiciary Act 1903* and in the High Court under section 75(v) of the Constitution).

Given that the more accessible and cheaper option for review under the AD(JR) Act is restricted to the ASIO security assessment, the Democrats believe that such an assessment should be a prerequisite condition for the exercise of the Attorney-General's power.

Should there be any concern as to the ability of the Attorney-General to exercise his or her powers under the Act in urgent circumstances where no formal assessment from ASIO is available, this could be provided for by way of a limited exemption. However, any such exemption should only be included if the grounds upon which the Attorney-General exercises his or her powers are also set out in more detail, as discussed below.

Grounds for exercising power

The Bill provides that the Attorney-General may exercise his or her power under section 581(3) if, after consulting with the Prime Minister and the Minister administering the Act, the Attorney-General considers that the proposed use or supply of a service would be prejudicial to security.

Given the significant and intrusive nature of the Attorney-General's powers under this section, the Democrats believe that the grounds for their exercise need to be more clearly defined. Firstly, the Attorney-General is only required to "consider" that the proposed use or supply would be prejudicial to security. There is no requirement that the Attorney-General's view be based on reasonable grounds, or "demonstrated grounds", as in the amendment proposed by Vodafone.

Secondly, the Democrats believe that the phrase "prejudicial to security" is ambiguous. We believe that this phrase should be replaced with an alternative form of words which imply a more specific threshold. For example, the requirement could be that the Attorney-General believes on reasonable grounds that the proposed use or supply would seriously threaten Australia's security. Alternatively, Vodafone proposes that the Attorney-General's power only be exercised if:

- There are demonstrated grounds to show that this is necessary to protect national security; and
- The risk to national security cannot be managed effectively through other mechanisms.

The problems associated with the current grounds for an exercise of the Attorney-General's power are compounded by the reference to "security", as it is defined in the *Australian Security Intelligence Organisation Act* 1979 (the "ASIO Act"), as discussed below.

The ambiguity of the grounds in section 581(3), not only gives the Attorney-General a broad discretion to exercise a very significant power, but would also have the effect of frustrating and hindering the ability of those affected by a section 581(3) direction to seek a review. It would be extremely difficult, if not impossible, for an interested party to prove that an exercise of the Attorney-General's power was invalid if such broad and ambiguous grounds are the basis for the power.

Definition of Security

For the purposes of proposed section 581(3), "security" has the same meaning as in the ASIO Act. Section 4 of the ASIO Act defines "security" as meaning:

> (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
>
> (i) espionage;
>
> (ii) sabotage;
>
> (iii) politically motivated violence;
>
> (iv) promotion of communal violence;
>
> (v) attacks on Australia's defence system; or
>
> (vi) acts of foreign interference;
>
> whether directed from, or committed within, Australia or not; and
>
> (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a).

On the basis of this definition, the Democrats share the concerns of the NSWCCL that the Attorney-General could exercise his or her powers in relation to political protests, industrial action and consumer boycotts.

We note that section 17A of the ASIO Act provides that:

> This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

Accordingly, ASIO would be constrained by this provision in preparing security assessments for the Attorney-General. However, this constraint would not extend to the actual decision of the Attorney-General, which is particularly concerning given that security assessments are not currently a mandatory prerequisite to that decision.

The Democrats agree with the NSWCCL, that the Bill should be amended to incorporate an express exemption for such activities, such as that which appears in the *Defence Legislation Amendment (Aid to Civilian Authorities) Act 2000*.

Practical implementation

The Democrats are concerned that the Bill does not spell out in any detail the process and steps taken to initiate and implement the directive for a carrier to cease supply of a service. The NSWCCL questioned, for example, how a customer would be notified of the termination, the liability of telecommunications service providers, and how a customer could seek information about the termination. Vodaphone also expressed a desire for greater articulation of rights, roles and responsibilities with regard to terminating an individual's service.

As was pointed out during the Inquiry, the *Telecommunications (Interception) Act* specifies the process with respect to interceptions in quite a degree of detail. However, this Bill fails implies a much greater degree of ambiguity. The Department indicated at the hearing that it was developing guidelines and protocols, separate from the legislation, to address these details. The Democrats would prefer to see more clarity and certainty in the legislation as is provided in the Telecommunications (Interception) Act.

Review Mechanisms

The Scrutiny of Bills Committee in the Alert Digest No. 8 of 2003 states in relation to proposed sections 58A and 581(3) that:

> Such a decision [directing the ACA to refuse to grant a carrier license to a person/direct a carriage services to a particular person] by the Attorney-General can only be made if he or she considers that the grant of that license would be 'prejudicial to security', but there is no means by which that basis for a decision can be tested before any independent body.

The Government notes that this provision is consistent with existing policy and also argues that judicial review of decisions would be available in the Federal and High court, and that carrier/carriage service providers would be able to seek a merits review of the ASIO security assessment in the Security Appeals Division of the Administrative Appeals Tribunal.

There are two important concerns. First, the fact that Attorney-General's decision is not reviewable, coupled with the ambiguous grounds on which that decision can be made, leaves the Attorney-General with a broad discretion and no accountability. The second concern, also raised by NSWCCL, is that "the ordinary punter on the street"

has even fewer avenues for redress than telecommunications corporations, given the potential cost of legal proceedings in the Federal Court or High Court.

Carrier Immunity

Currently, the Bill does not provide statutory immunity for carriers, carriage service providers and their officers, employees and agents in respect of acts done or omitted in good faith in relation to a direction under 581(3), despite the fact that such immunity attaches to sections 313 and 315 of the Act. In its submission, Vodafone argues:

> Carriers and carriage service providers could potentially be exposed to very significant claims in damages and on other bases for ceasing or refusing to supply telecommunications services to their customers in compliance with a direction under section 581 (3). It is clearly essential to afford them such bare minimum statutory protection against such claims.

In response, the Department argued that compliance with a direction under section 581(3) would frustrate the contracts of carriers and carriage service providers, so that they would not attract any liability. While this may be the case, the Democrats believe that it immunity from liability should be expressly included in the Bill, in order to avoid any doubt. This is a matter that should be determined by the Parliament and not left to the courts.

Even if they are granted immunity from liability, there is still some potential for service providers to suffer loss as a result of their compliance with a direction under section 581(3). The Democrats believe that a requirement for the Commonwealth to provide compensation for any such loss would help to ensure that the Attorney-General's powers are only exercised in circumstances where there is a genuine threat to national security.

Summary and recommendation

While the majority report highlights many of the Democrats' concerns, it does not recommend that the Government address all of these concerns.

The Democrats believe that the issues raised in the submissions, at the hearings, in the Bills Digest and through the Scrutiny of Bills Committee raise valid concerns. The mechanisms to increase security in this Bill are ambiguous, unclear and are without effective review processes. The Democrats recommend that the Bill be redrafted to provide greater clarity and certainty.

Senator John Cherry
Democrat Member

Appendix 1

Submissions Received

1 Vodafone

2 New South Wales Council for Civil Liberties

3 Department of Communications, Information Technology and the Arts

Appendix 2

Hearing Program

Friday, 5 September 2003
Parliament House, Canberra

10.30 **Introduction to the Bill:**

Department of Communications, Information Technology and the Arts (DCITA)

Chris Cheah, Chief General Manager, Telecommunications

Brenton Thomas, General Manager, Enterprise and Infrastructure Branch

Don Williams, Director

Attorney-General's Department (A-G's)

Peter Ford, Acting Deputy Secretary, Criminal Justice and Security

Catherine Smith, Acting Assistant Secretary, Security Law Branch

Anna Tearne, Principal Legal Officer, Security Law Branch

11:00 **Vodafone (Submission 1)**

Spencer Maddrell, Manager, Regulatory Compliance

Brian McDonnell, Policy Analyst, Public Policy

11.45 ***Short Break***

12.00 **New South Wales Council for Civil Liberties (Submission No. 2)**

Cameron Murphy, President (By telephone.)

12.30 **Response to matters raised:**

Panel of officers from DCITA and A-G's

1.00 ***Adjournment***

Appendix 3

Australian Security Intelligence Organisation Act 1979

Act No. 113 of 1979 as amended

4 Definitions

security means:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
  (i) espionage;
  (ii) sabotage;
  (iii) politically motivated violence;
  (iv) promotion of communal violence;
  (v) attacks on Australia's defence system; or
  (vi) acts of foreign interference;
  whether directed from, or committed within, Australia or not; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a).

17A Act not concerned with lawful dissent etc.

This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

Appendix 4

SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

EIGHTH REPORT OF 2003

20 August 2003

Communications Legislation Amendment Bill (No. 2) 2003

Introduction

The Committee dealt with this bill in *Alert Digest No. 8 of 2003*, in which it made various comments. The Minister for Communications, Information Technology and the Arts has responded to those comments in a letter dated 19 August 2003. A copy of the letter is attached to this report. An extract from the *Alert Digest* and relevant parts of the Minister's response are discussed below.

Extract from Alert Digest No. 8 of 2003

[Introduced into the House of Representatives on 26 June 2003. Portfolio: Communications, Information Technology and the Arts]

The bill amends the *Telecommunications Act 1997*, the *Australian Security Intelligence Organisation Act 1979* and the *Administrative Decisions (Judicial Review) Act 1977* to enhance the security of Australia's telecommunication services and networks and to improve existing arrangements in relation to call data disclosure and interception services.

Non-reviewable decisions
Schedule 1, item 10

Proposed new section 58A of the *Telecommunications Act 1997*, to be inserted by item 10 of Schedule 1 to this bill, would give to the Attorney-General, after consulting the Prime Minister and the Minister administering the Telecommunications Act, a

discretion to direct the Australian Communications Authority to refuse to grant a carrier licence to a person. Such a decision by the Attorney-General can only be made if he or she considers that the grant of a licence would be 'prejudicial to security', but there is no means by which that basis for a decision can be tested before any independent body. The *Telecommunications Act 1997* does not provide for a review on the merits of such a decision before the Administrative Appeals Tribunal, and item 1 of Schedule 1 to this bill proposes to amend the *Administrative Decisions (Judicial Review) Act 1977* to remove from the possibility of review under that Act a decision made under the new section 58A.

The Committee **seeks the Minister's advice** as to whether this is the effect of the provision and, if so, the reason for excluding review of such a decision.

Pending the Minister's advice, the Committee draws Senators' attention to the provision, as it may be considered to make rights, liberties or obligations unduly dependent upon non-reviewable decisions, in breach of principle 1(a)(iii) of the Committee's terms of reference.

Relevant extract from the response from the Minister

I note the Committee has raised concerns that the Bill will exclude decisions of the Attorney-General under the proposed new section 58A and subsection 581(3) of the *Telecommunications Act 1997* from review by an independent body and may be in breach of principle 1(a)(iii) of the Committee's terms of reference.

The proposals to exempt decisions by the Attorney-General, either to direct the Australian Communications Authority to refuse to grant a carrier licence, or to direct a carrier or carriage service provider not to use or supply, or to cease using or supplying a carriage service on the basis that it would be prejudicial to security, from review under the *Administrative Decisions (Judicial Review) Act 1997* (AD(JR) Act), are consistent with existing policy. While the AD(JR) Act provides a streamlined form of judicial review, it is not designed to deal effectively with the review of sensitive material.

Decisions made on grounds of security, or which have security implications, under for example, the *Intelligence Services Act 2001; Telecommunications (Interception) Act 1979; Foreign Acquisitions and Takeovers Act 1975;* and *Australian Security Intelligence Organisation Act 1979,* are currently exempt from review under the AD(JR) Act.

There will, however, be a number of avenues for independent review. Judicial review of decisions made by the Attorney-General under the proposed amendments would be available in the Federal Court under section 39B of the *Judiciary Act 1903* and in the High Court under section 75(v) of the Constitution.

In addition, the proposed new sections 35 and 38A of the *Australian Security Intelligence Organisation Act 1979* will enable a carrier licence applicant or a carrier/carriage service provider who is the subject of an adverse or qualified security

assessment provided by ASIO to the Attorney-General to seek merits review of that assessment in the Security Appeals Division of the Administrative Appeals Tribunal.

I trust this information is of assistance.

The Committee thanks the Minister for this response. The Committee notes that the proposal is based on a policy relating to the judicial review of decisions based on sensitive material. The Committee considers that this amendment may make rights or liberties dependent upon non-reviewable decisions, but whether it does so *unduly* is a matter for the Senate as a whole.

The Committee draws Senators' attention to the provision, as it may be considered to make rights, liberties or obligations unduly dependent upon non-reviewable decisions, in breach of principle 1(a)(iii) of the Committee's terms of reference.

Non-reviewable decisions
Schedule 1, item 27

Proposed new subsection 581(3) of the *Telecommunications Act 1997*, to be inserted by item 27 of Schedule 1 to this bill, would give to the Attorney-General, after consulting the Prime Minister and the Minister administering the Telecommunications Act, a discretion to direct a carriage service provider to deny carriage services to a particular person. As with proposed new section 58A, such a decision by the Attorney-General can only be made if he or she considers that the use of carriage services would be 'prejudicial to security', but there is no means by which that basis for a decision can be tested before any independent body.

The Committee **seeks the Minister's advice** as to whether this is the effect of the provision and, if so, the reason for excluding review of such a decision.

Pending the Minister's advice, the Committee draws Senators' attention to the provision, as it may be considered to make rights, liberties or obligations unduly dependent upon non-reviewable decisions, in breach of principle 1(a)(iii) of the Committee's terms of reference.

Relevant extract from the response from the Minister

Response same as for Schedule 1, item 10 above.

The Committee thanks the Minister for this response. The Committee again notes that the proposal is based on a policy relating to the judicial review of decisions based on sensitive material. The Committee considers that this amendment may make rights or liberties dependent upon non-reviewable decisions, but whether it does so *unduly* is a matter for the Senate as a whole.

The Committee draws Senators' attention to the provision, as it may be considered to make rights, liberties or obligations unduly dependent upon non-reviewable decisions, in breach of principle 1(a)(iii) of the Committee's terms of reference.