Communications Legislation Amendment Bill (No. 2) 2003
Communications Legislation Amendment Bill (No. 2) 2003

Peter Prince
Law and Bills Digest Group
25 August 2003
Communications Legislation Amendment
Bill (No. 2) 2003

Date Introduced: 26 June 2003
House: House of Representatives
Portfolio: Communications, Information Technology and the Arts
Commencement: The day after Royal Assent

Purpose
To amend:

- the Telecommunications Act 1997 to ensure that national security and law enforcement interests are considered before telecommunications carriers are granted an operating licence, and to allow the Attorney-General to prevent a person whose activities threaten national security from using or supplying a telecommunications service

- the Australian Security Intelligence Organisation Act 1979 ('ASIO Act') to enable telecommunications carriers to appeal to the Administrative Appeals Tribunal against an adverse security assessment, and

- the Administrative Decisions (Judicial Review) Act 1977 ('ADJR Act') to exclude from judicial review under that Act the Attorney-General's use of new powers under proposed amendments to the Telecommunications Act.

Background
The primary purpose of this Bill is to ensure that telecommunications providers operating in Australia are security cleared. There appear to be two main motives: to protect sensitive communications at both an inter and intra-governmental level, and to ensure that official telecommunications interception activities are not compromised.

The Bill must, of course, be seen in the context of the heightened focus on national security in the post-September 11 world. Coincidentally, with increasing competition in the Australian telecommunications market, there is a growth in the number of providers in

Warning:
This Digest was prepared for debate. It reflects the legislation as introduced and does not canvass subsequent amendments.
This Digest does not have any official legal status. Other sources should be consulted to determine the subsequent official status of the Bill.
this market. As the Second Reading Speech observes, 'the telecommunications industry is attracting significant new investment which increases the potential for national security and law enforcement issues to arise.'

At present, there is no procedure mandated by legislation requiring formal security clearance of telecommunications providers. As the Government noted in introducing the Bill:

The [Australian Communications Authority] is not required to consult with the relevant national security and law enforcement agencies prior to issuing a [telecommunications] carrier licence to an applicant and, whilst the grounds for refusing to grant a carrier licence are not limited under the Telecommunications Act, the ability to refuse to grant a carrier licence on national security grounds is not provided for expressly.

Telecommunications Interception

The Telecommunications Act 1997 requires telecommunications carriers to give the Commonwealth 'such help as is reasonably necessary' to enforce Australian laws and safeguard national security. Giving help is specifically defined to include 'provision of interception services'.

Telecommunications carriers must maintain an ability to supply an 'interception capability' in accordance with warrants issued under the Telecommunications (Interception) Act 1979. Providers must lodge an 'interception capability plan' with the Australian Communications Authority ('ACA') and the Attorney-General's Department each year, and maintain the ability to implement the plan. Exemptions from the requirement to maintain an interception capability can be granted.

The Telecommunications (Interception) Act allows the Attorney-General to issue an interception warrant on the request of the Director-General of the Australian Security and Intelligence Organisation ('ASIO'). Interception warrants can be issued in various forms. The Attorney-General must be satisfied that a telecommunications service is being or is likely to be used 'for purposes prejudicial to security'. In an emergency the Director-General can issue an interception warrant, providing a copy to the Attorney-General, who can revoke it.

Interception warrants can also be obtained for law enforcement purposes by Federal and State police and other government crime investigation bodies. Applications for such warrants must be made to an 'eligible judge' or nominated member of the Administrative Appeals Tribunal. Warrants can only be obtained for the investigation of serious criminal offences, including – following amendments in 2002 – acts of terrorism.

The latest annual report on the Telecommunications (Interception) Act states that 2514 interception warrants were issued to law enforcement agencies during 2001-02,
representing an increase of 17 per cent over the previous year. These figures do not include interception warrants requested by ASIO.

The annual report noted that there was a 48 per cent increase in the number of prosecutions commenced and a 50 per cent increase in the number of convictions obtained on the basis of lawfully obtained information.

Commenting on these figures, the Attorney-General, the Hon. Daryl Williams MP, stated in June 2003 that:

The report shows that the use of telecommunications interception continues to be an important investigative tool which is demonstrating proven results. The figures contained in the report show that access to this tool is vital for law enforcement particular at a time of such rapid technological change and advancement.

In contrast, the Sunday Tasmanian remarked that:

Australians are fast becoming the most spied-on people in the Western world. Mail interceptions and telephone taps have soared…The 2514 court warrants for phone taps last financial year – almost double the number issued in the US – represent a tenfold increase in the past decade…The warrants apply to hundreds of thousands of individual phone calls and eavesdropping on thousands of people.

In relation to the previous annual report on the Telecommunications (Interception) Act, the then Shadow Minister for Justice and Customs, Daryl Melham MP, stated in September 2002 that 'It is a striking fact that Australian law enforcement agencies are resorting to telecommunications interception much more than their American counterparts'. Given the disparity in population between the two countries, 'this amounts to a per capita rate of telephone interception in Australia more than 20 times that in the United States.'

### Media Commentary on the Bill

There has been little media commentary on the Bill itself.

In one of the few articles to date, Simon Hayes from news.com.au reported on 31 July 2003 that 'civil libertarians are up in arms'. According to the President of the NSW Council for Civil Liberties, the Bill's proposal to allow the Attorney-General to order the disconnection of a telecommunications service where the use or supply is 'prejudicial to security' is 'absolutely outrageous':

This is a subjective decision of the Attorney-General, and we have already seen subjective decisions leading to raids, with no follow up action…It has become a pattern that under the guise of national security, people are being harassed. This will just provide more opportunities to harass people.
Main Provisions

Telecommunications Act

Under existing section 42 of the Telecommunications Act, it is an offence to provide telecommunications services without a 'carrier licence'. An application for a carrier licence must be made in the approved form to the ACA.19

Schedule 1 Item 9 of the Bill proposes to insert new section 56A in the Telecommunications Act requiring the 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.

An application for a carrier licence will be deemed not to be received by the ACA until a copy is given to the agency co-ordinator (Item 6).

Within 15 business days after an application is received, the agency co-ordinator may issue one of two types of notices to the ACA.

Under proposed sub-section 56A(2), the agency co-ordinator may notify the ACA that it does not require any further consultation about the application. This notice cannot be revoked.

Alternatively, under proposed sub-section 56A(3), the agency co-ordinator may give a written notice to the ACA directing it not to issue a licence while the notice remains in force. The ACA must give a copy of the notice to the applicant. Notices have effect for a maximum of three months, but under proposed sub-section 56A(4) can be renewed to allow a consultation period of up to 12 months as part of the carrier licensing process.

Item 10 inserts proposed section 58A in the Act giving the Attorney-General (acting in consultation with the Prime Minister and the Minister for Communications, Information Technology and the Arts) specific power to direct the ACA not to issue a carrier licence on national security grounds.

Item 28 proposes to amend Schedule 4 of the Act to provide that an applicant will not be able to apply to the ACA for review of decisions made under proposed sections 56A and 58A. Under existing section 562 of the Act, this in turn prevents review of such decisions by the Administrative Appeals Tribunal.

The Bill does not propose that telecommunications providers with current licences should be security cleared. Instead, Item 27 proposes to insert new sub-section 581(3) in the Telecommunications Act allowing the Attorney-General to order a telecommunications carrier to stop using or providing telecommunications services or to cease supplying such services to particular persons.

Warning:

This Digest was prepared for debate. It reflects the legislation as introduced and does not canvass subsequent amendments.

This Digest does not have any official legal status. Other sources should be consulted to determine the subsequent official status of the Bill.
As with the proposed section 58A, an order under proposed section 581(3) can be made if the Attorney-General considers that the particular use or supply of telecommunications services is or would be 'prejudicial to security'. Again, the Attorney-General can only make such an order after consulting the Prime Minister and the Minister for Communications, Information Technology and the Arts.

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.20

Schedule 1 provides for other amendments to the Telecommunications Act, including:

- **Item 11** replaces the existing section 59 with a new section providing revised time limits for ACA consideration of a carrier licence application, after which the application is deemed to have been refused. The proposed time limits are similar to the existing periods but allow both for information requests under the current Act and notices requiring consultation under the proposed legislation.

- **Item 19** adds new sub-section 313(8) which specifies 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, the aim of this provision is to ensure that 'relevant technical data and contextual information about each communication is provided to law enforcement agencies.'21

- **Item 21** inserts new sub-section 326(4) which imposes a 60 day time limit on consideration by the agency co-ordinator of an application from a telecommunications carrier to be exempt from the requirement to maintain an interception capability. If the agency co-ordinator does not respond within this time, the exemption is deemed to have been granted. However, an exemption obtained in this way only has effect until a formal decision has been communicated to the applicant.

- **Item 22** amends sub-section 329(1) by requiring interception capability plans submitted to the ACA and the agency co-ordinator to be signed by the chief executive officer of a telecommunications carrier or another person authorised to sign the document. Item 23 requires such plans to include strategies for complying with obligations to provide interception capabilities in relation to each carriage service supplied by the telecommunications provider.

ASIO Act

According to the Explanatory Memorandum, 'it is expected' (but it will not be required) that the Attorney-General will receive a security assessment from ASIO before using the proposed new powers under the Telecommunications Act to direct that a carrier licence
Communications Legislation Amendment Bill (No. 2) 2003

was not to be issued or that a person must cease using or supplying a telecommunications service.²²

**Existing section 54** of the ASIO Act allows applications to the Administrative Appeals Tribunal for review of an 'adverse or qualified security assessment' that has been provided by ASIO to a Commonwealth agency, a State or a State authority. Under **existing section 38**, a person must be notified of an adverse or qualified security assessment except where the Attorney-General provides written certification to the Director-General of ASIO that withholding notification 'is essential to the security of the nation'.

Alternatively, a person can be informed of an adverse or qualified security assessment but the reasons for the assessment can be withheld if the Attorney-General certifies that disclosure of these reasons 'would be prejudicial to the interests of security'.

**Schedule 1 Items 2 to 4** of the Bill amend the ASIO Act to enable appeals to the Administrative Appeals Tribunal by persons who receive an 'adverse or qualified security assessment' in connection with use by the Attorney-General of the new powers in proposed section 58A and subsection 581(3) of the Telecommunications Act.

**Item 2** will include use of the proposed new powers within the definition of 'prescribed administrative action' in **existing section 35** of the ASIO Act. This means that a security assessment recommending use of the new powers will come within the definitions of 'adverse security assessment' or 'qualified security assessment' under section 35. Under **existing section 54** of the ASIO Act, this in turn will allow an appeal against such an assessment to the Administrative Appeals Tribunal.

The Explanatory Memorandum notes that if the Administrative Appeals Tribunal were to overturn such an assessment:

subsection 61(1) of the ASIO Act would require the Attorney-General to treat the AAT's finding in respect of the assessment as superseding the assessment to the extent that the finding does not confirm the assessment. As a consequence, in circumstances in which the Attorney-General's direction [ordering a person to cease using or supplying a telecommunications service or preventing the ACA issuing a carrier licence] under proposed section 58A or proposed subsection 581(3) [of the Telecommunications Act] was based upon an assessment that was not wholly confirmed by the AAT, the basis for the direction would have changed and a reconsideration of the decision to issue the direction would necessarily arise. This might result in the Attorney-General deciding to revoke a direction or deciding that there are other national security concerns that mean that the direction should not be revoked in the circumstances.²³

**Items 3 and 4** establish a specific regime for notification of adverse and qualified security assessments connected with the Attorney-General's use of the proposed new powers.

---

**Warning:**

This Digest was prepared for debate. It reflects the legislation as introduced and does not canvass subsequent amendments. This Digest does not have any official legal status. Other sources should be consulted to determine the subsequent official status of the Bill.
Item 3 inserts **new sub-section 38(1A)** in the ASIO Act providing that the notification procedures in existing section 38 do not apply where an assessment is made in connection with the new powers.

Item 4 inserts **new section 38A** in the ASIO Act which provides that within 14 days of receiving an adverse or qualified security assessment in connection with the proposed new powers in section 58A or subsection 581(3) of the Telecommunications Act, the Attorney-General must notify the person concerned of the assessment. The notice must attach a copy of the assessment and inform the person of the right to apply to the Administrative Appeals Tribunal to have the assessment reviewed.

As with existing section 38, the Attorney-General can withhold notification of an adverse or qualified security assessment if this 'is essential to the security of the nation', or remove from a notification any matters 'the disclosure of which would be prejudicial to the security of the nation'.

Unlike current section 38, however, under **proposed section 38A** the Attorney-General need not provide written certification to the Director-General of ASIO that a person should not be informed of an adverse or qualified security assessment or that supporting reasons or other material should be omitted from a notification.

**ADJR Act**

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 ADJR Act. According to the Second Reading Speech, this 'is consistent with existing exclusions under the AD(JR) Act for similar decisions based on national security considerations.\(^{24}\)

**Schedule 1 of the ADJR Act** lists various pieces of legislation in the national security field to which the ADJR Act does not apply, including the ASIO Act, the Telecommunications (Interception) Act, the Intelligence Services Act 2001, and the Inspector-General of Intelligence and Security Act 1986.

**Schedule 1 Item 1** of the Bill proposes to add **new paragraph (daa)** to **Schedule 1 of the ADJR Act** providing that the Act will not apply to decisions of the Attorney-General under **proposed section 58A or subsection 581(3)** of the Telecommunications Act. Most significantly, this means that telecommunications carriers and others affected by such decisions will not get the benefit of **section 13** of the **ADJR Act** which confers a statutory right to obtain a statement of reasons.

As the Explanatory Memorandum notes, however, '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.\(^{25}\)
Concluding Comments

Security clearances

Introducing mandatory security clearances for organisations wishing to provide telecommunications services in Australia is not an insignificant step. Companies applying for a telecommunications carrier licence will now need to allow for a consultation period which could last for up to 12 months while any security issues are resolved.

In the current security climate, however, it is not surprising that the Government should seek 'more secure telecommunications networks and services', especially in relation to its interception capabilities.

Indeed it seems anomalous in such a climate that security clearances will be required for new telecommunications carriers but not for companies with existing carrier licenses.

Restricting Merits Review

The Bill will prevent any 'merits review' of the Government's use of the proposed new powers under the Telecommunications Act. The Bill specifically rules out any application to the Administrative Appeals Tribunal in relation to proposed section 56A (requirement for consultation before carrier licence issued) or section 58A (direction to refuse a carrier licence). This is not specified for proposed sub-section 581(3) (preventing use or supply of a telecommunications service). But under the terms of the Telecommunications Act and the Administrative Appeals Tribunal Act 1975, an application to the Tribunal in relation to sub-section 581(3) would in any case not be available.

The Bill will instead allow merits review of an adverse or qualified security assessment that may be the basis for the Government's use of the proposed new powers.

Review of an adverse security assessment

As with current security assessments under the ASIO Act, an obvious difficulty in seeking review by the Administrative Appeals Tribunal is that the assessed person or telecommunications carrier might not be told of an adverse or qualified security assessment. This is more than a theoretical possibility. The power to withhold a carrier licence or to ban a person from using or supplying a telecommunications service can be invoked where the Attorney-General considers that it would be 'prejudicial to security' not to intervene. In such circumstances it would be consistent for the Attorney-General to also decide, in accordance with proposed section 38A of the ASIO Act, that withholding notification of an adverse or qualified assessment is 'essential to the security of the nation'.

In practice, the ability to withhold notification of an adverse or qualified security assessment is a power to prevent appeals to the Administrative Appeals Tribunal against

Warning:
This Digest was prepared for debate. It reflects the legislation as introduced and does not canvass subsequent amendments.
This Digest does not have any official legal status. Other sources should be consulted to determine the subsequent official status of the Bill.
such an assessment. It is difficult to see how people can appeal against assessments about which they cannot officially be told. Parliament may wish to consider whether such an approach is appropriate in the case of the telecommunications industry.

Parliament might also note, however, that in this respect the Bill is not proposing anything different from current legislation.

What is different is that in relation to security assessments carried out for the purpose of the Government's proposed new powers under the Telecommunications Act, the Attorney-General will not be required to provide written certification to the Director-General of ASIO that a person or company should not be told of an adverse or qualified security assessment. The Explanatory Memorandum provides no explanation for this difference.

New Powers and Security Assessments

Parliament might also note that, as the Explanatory Memorandum pointed out, even if a person is notified of an adverse security assessment and successfully applies to the Administrative Appeals Tribunal to overturn that assessment, the Government will not be required to revoke a decision to refuse a carrier licence or to stop a person using or supplying a telecommunications service. This is because the Attorney-General's ability to use the proposed new powers is not tied to the outcome of an official security assessment.

Even with a formal security clearance from ASIO or a successful application to the Tribunal against a negative security assessment, the Attorney-General will be able – as the Explanatory Memorandum notes – to invoke the proposed powers because of 'other national security concerns'.

Indeed, Parliament might note that there is no requirement in the Bill for the Attorney-General to obtain any formal security assessment or even to consult ASIO or other security agencies before using the proposed new powers.

Restricted Judicial Review

The Bill will only allow (restricted) judicial review of the Government's use of the proposed new powers. The advantage for the Government of judicial review is that unlike merits review it is not concerned with whether a decision was the correct or preferable one, but only with the legality of an administrative decision. A court 'must affirm a legally impeccable decision even if it thinks that the decision is a substantively poor one'.

In the case of the proposed new powers, the legal requirements on the Attorney-General are not onerous. After consulting the Prime Minister and the Minister for Communications, Information Technology and the Arts, the Attorney-General need only 'consider that the grant of a carrier licence…or the use or supply' of a telecommunications service 'would be prejudicial to security'.

Warning:
This Digest was prepared for debate. It reflects the legislation as introduced and does not canvass subsequent amendments.
This Digest does not have any official legal status. Other sources should be consulted to determine the subsequent official status of the Bill.
In other words, the Attorney-General needs merely to honestly form the impression that allowing such action would be prejudicial to national security. There is no requirement on the Attorney-General to establish that there are national security grounds that are reasonable in all the circumstances before using the proposed powers.

This means the prospects are slim for any successful application for judicial review of the proposed new powers. This is even more so because of the lack of access to a statement of reasons under the ADJR Act.

As with other security related legislation, exclusion of the Government's proposed new Telecommunications Act powers from review under the ADJR Act may be justified on national security grounds. According to the Explanatory Memorandum, the ADJR Act mechanism 'is an expedited judicial review process that is not designed to deal effectively with the review of classified material.'\(^{29}\)

It may still be possible in particular cases to gain access to the Government's reasons for use of these powers as part of the common law judicial review process. As the Government has said, judicial review of the Attorney-General's new powers will still be available through the 'prerogative writ' process under the Constitution and the Judiciary Act. An affected person or company, however, would first need to argue for access to the Government's reasons, adding to the difficulty of challenging a decision to disconnect their telecommunications service or exclude them from the industry.

Moreover, it might be noted that under the common law, the Attorney-General may not need to provide any reasons for use of the proposed powers. According to Professor Zines:

> The prerogative writs...are not completely adequate tools for the purpose of constitutional control. Their usefulness is further reduced if the authority concerned does not give any reasons for the decision. The High Court has confirmed the orthodox view that, in general, an authority who has a discretion is not under an obligation to give any reason for the exercise of that discretion.\(^{30}\)

**The Proposed Legal Regime**

The key issue for Parliament is whether the legal regime proposed in the Bill is justified given the national security outlook facing Australia.

As the Government claims, it may be that in most cases any security concerns raised by an application for a telecommunications carrier licence or by a particular use or supply of a telecommunications service could be dealt with through consultation and other mechanisms.\(^{31}\)

Nevertheless, on a strict reading of the amendments proposed in the Bill, the Attorney-General need not refer to an official security assessment before banning a person or
company from participation in the Australian telecommunications industry; even if an official security assessment exists, the person or company affected may be unaware of it and therefore unable to appeal against it; and decisions by the Attorney-General affecting the business and livelihood of people in the telecommunications industry can be based on subjective judgements of the national security situation with little prospect of any successful review by the courts.

Most significantly, the proposed new powers can be used in respect of individuals, who can be prohibited from having access to any form of telecommunications. Different considerations appear to be involved when the Bill moves from requiring security clearances for telecommunications companies or giving the Attorney-General power to ban such companies from operating in Australia to allowing the Attorney-General to prohibit people altogether from communicating by telephone or similar means.

In this context, the Parliament might note the recognition by the High Court of an implied constitutional freedom of political communication. This may be relevant to the Government's use of the new powers. While there may be a security rationale for preventing individuals from using modern means to communicate, such a prohibition would obviously prevent people communicating on political as well as other issues.

The implied freedom of political communication is not absolute. However, as Harris notes:

> In cases where the limitation relates to a mode of communication, the validity of the restrictions on political communication would depend upon a balancing of the public interest served by the legislation and the degree of limitation of the freedom. The balancing process used to determine whether restrictions on political communication are unconstitutional involves the application of a proportionality test – the interest served by the legislation would have to be proportionate to the inroad on the freedom, and the freedom could only be limited to an extent that is reasonably necessary to serve the interest.

---

### Endnotes

2. ibid.
3. Telecommunications Act sections 313 and 314.
4. Telecommunications Act section 324.
5. Telecommunications Act sections 330 and 331.
A 'telecommunications service' warrant (section 9) or a 'named person' warrant (section 9A), both of which can authorise entry onto premises (section 9B).


Telecommunications (Interception) Act section 10.

Telecommunications (Interception) Act sections 6D and 6DA.


The Telecommunications (Interception) Act does not require information on ASIO interception warrants to be provided in the annual report on the Act. Instead, the Director-General of ASIO is required to report to the Attorney-General on the extent to which interception warrants assisted ASIO in performing its functions within three months after the expiry or revocation of each warrant (section 17).


Sunday Tasmanian, 29 June 2003, p. 2.


Sections 52 and 53.


Explanatory Memorandum, p. 23.

Explanatory Memorandum, p. 1.


Explanatory Memorandum, p. 1. Judicial review would also be available in the High Court under section 75 (iii) of the Constitution.


Section 25(1) Administrative Appeals Tribunal Act, section 562 Telecommunications Act.


Explanatory Memorandum, p. 6.


32 Three High Court cases in the 1990s – *Australian Capital Television* (1992), *Nationwide News* (1992) and *Lange* (1997) established an implied constitutional right of political communication. The cases established that:

- Limits on the Commonwealth’s law making powers may be implied in and from the text of the Constitution

- The key principle of the Constitution is representative democracy - expressed and constitutionally entrenched in sections 7 and 24

- A necessary condition of representative democracy is the freedom to discuss and communicate information regarding political and economic matters

- This freedom extends beyond election periods to all political discussions generally.