GILBERT + TOBIN
CENTRE OF PUBLIC LAW

THE UNIVERSITY OF NEW SOUTH WALES

FACULTY OF LAW

GEORGE WILLIAMS

ANTHONY MASON PROFESSOR

DIRECTOR, GILBERT + TOBIN CENTRE OF PUBLIC LAW

10 March 2006

Committee Secretary
Senate Legal and Constitutional Committee
Department of the Senate
Parliament House
Canberra ACT 2600
Australia

Dear Secretary

Inquiry into the Telecommunications (Interception) Amendment Bill 2006 (Cth)

Thank you for the opportunity to make a submission on this Bill. We have strong concerns that the Bill overreaches in its effect on the right to privacy without clear benefit to our national security. We also note that parts of the Bill may give rise to constitutional issues.

A B-Party Interceptions

Schedule 2 of the Bill authorises intercepting 'B-Party' communications.

The Bill purports to clarify and restrict pre-existing B-Party interception powers under the *Telecommunications (Interception) Act 1979* (Cth). So far as the Act already authorised B-Party interceptions, we support moves to clarify this power and make its exercise less arbitrary.

We believe, however, that the Bill abrogates the right to privacy substantially more than is necessary to achieve the Bill's security purposes. It is important that legislation does not abrogate rights more than is necessary and incidental to achieving the purpose of the legislation. Where legislation does disproportionately abrogate rights, it may have adverse, unintended effects.

We have two specific concerns with Schedule 2.

SYDNEY 2052 AUSTRALIA
Email:george.williams@unsw.edu.au
Telephone: +61 (2) 9385 2259
Mobile: 0414 241 593
Facsimile: +61 (2) 9385 1175
Web: www.gtcentre.unsw.edu.au

1 The Bill allows the interception and use of all B-Party communications

Schedule 2 allows government agencies to intercept not only communications between the B-Party and the person involved in the offence, but also communications between the B-Party and all other people.

We acknowledge that the interception of all B-Party communications may be necessarily incidental to the interception of material relevant to the offence in respect of which the warrant is issued. However, the Bill does not institute safeguards ensuring that government agencies only use the communications which are relevant to the offence which is being investigated. For instance, the Bill does not provide that records of incidental communications must be destroyed (except in limited circumstances) and/or that such material is subject to use and indemnity use privilege or cannot be used as evidence.

The purpose of the Bill is to allow government agencies to collect information relevant to particular offences which they are investigating. The Bill currently allows government agencies to collect and use a far wider range of information than necessary to achieve the Bill's purpose.

Recommendation:
The Bill should restrict the uses to which incidentally-obtained B-Party communications may be put to those uses which achieve the purpose of B-Party warrants.

2 No nexus is required between the nature of the warrant and the investigation of the particular offence

(a) Warrants to ASIO – Schedule 2, item 1

Item 1 of Schedule 2 (amending s 9(1)(a)) authorises the Attorney-General to issue B-Party interception warrants to ASIO. Under that item, there is no requirement that there be evidence of a nexus between B-Party communications and the activities prejudicial to national security which triggered the warrant. All that must be shown is that: (i) the B-Party is likely to communicate with a person who is likely to engage in activities prejudicial to security; and (ii) intercepting the B-Party's communications is likely to assist in obtaining intelligence related to security.

The purpose behind allowing B-Party interceptions is to obtain information assisting the investigation of the particular activities prejudicial to security which triggered the warrant.

The Bill grants far more extensive powers than those necessary to achieve that purpose for the following reasons:

- B-Party warrants may be issued even if there is no evidence that the warrant will assist in obtaining information relevant to the activities which triggered the warrant. It is enough to show that intercepting B-Party communications to or from *anyone* may assist in obtaining *any* intelligence related to security.
- Once it is shown that the person involved in activities prejudicial to security communicates with the B-Party, the Director-General must only discharge the very low burden that the interception will be likely to assist in obtaining intelligence related to security. 'Likely to assist' is a very broad standard. Further, the concept of 'relating to security' is both wide and vague, particularly since 'security' has the same wide meaning as that given in section 4 the *Australian Security Intelligence Organisation Act 1979* (Cth).

Once a warrant is issued, ASIO may exercise incredibly intrusive powers: it may intercept all communications to or from the B-Party and may enter the B-Party's premises without notice.

If the Bill's purpose is to facilitate gathering information about the particular activities which are being investigated, then the Bill clearly abrogates privacy far more than is necessary to achieve that aim. Currently, the Bill allows ASIO to engage in the kind of 'fishing expeditions' which the Blunn Report specifically warned against (Anthony S Blunn, *Report of the Review of the Regulation of the Access to Communications* (2005), 76). Further, the breadth and vagueness of the burden which the Director-General must discharge may create the potential for abuse of the interception power.

Recommendation:
The Bill should require, as a precondition to issuing a warrant under s 9, that there be evidence that the B-Party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

(b) Warrants to Agencies - Schedule 2, items 8 and 9

Under items 8 and 9 of Schedule 2 (amending s 46), the issuing officer must be satisfied that the warrant will assist in obtaining evidence relating to the offence which is being investigated before a warrant may be issued.

The purpose behind these amendments seems to be that intercepting the suspect's communications is sometimes impractical; therefore, it is may be necessary to intercept communications involving the suspect and the B-Party so as to obtain information.

These items do not, however, require that it be established that the evidence will be obtained from communications between the B-Party and the person suspected of being involved in the offence. It would be sufficient, for instance, if: (i) the B-Party sometimes communicated with the suspect; and (ii) intercepting communications between the B-Party and *any* third party would, in some way, assist in investigating the suspect. This is a particularly low burden.

If the Bill's purpose is to intercept communications involving the suspect in circumstances where intercepting the suspect's telecommunications device is impractical, then clearly the Bill grants far greater powers than are necessary to achieve that aim.

Recommendation 3:
The Bill should require, as a precondition to granting a warrant under s 46, that there be evidence that the suspect will, in some way, be causally related to communications involving the B-Party which will assist in investigating the suspect.

B Issuing Officers for Stored Communications Warrants

Item 4 of Schedule 1 (adding s 6DB) provides that the Minister may appoint federal judges, federal magistrates or magistrates as issuing officers for stored communications warrants'. The regime makes it significantly easier to issue stored communications warrants to an agency than it has previously been to issue telecommunications interception warrants.

This use of federal judges and magistrates as issuing officers will be unconstitutional if it offends the incompatibility principle stated in *Grollo v Palmer* (1995) 184 CLR 348. It is unlikely that item 4 will offend that principle since *Grollo* itself upheld the validity of the *Telecommunications (Interception) Act 1979* (Cth) as it applied to judges being issuing officers.

However, we note that item 4 may be more likely to be unconstitutional than the provisions examined in *Grollo*. This is because the preconditions for granting a stored communications warrant are significantly more lenient than for interception warrants (for instance, they are available with respect to significantly less serious offences). Further, reporting requirements are considerably less burdensome for stored communications warrants, reducing public visibility of the process. Consequently, it is easier to view the issuing officer as a mere 'rubber stamp' for the executive, thereby undermining the public perception of judicial independence.

Yours sincerely

Professor George Williams
Anthony Mason Professor and Centre Director

David Hume
Social Justice Intern