Dear Sir

INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION

The purpose of this submission is to express my views on the privacy aspects of these proposals – specifically, the highly intrusive nature and unjustifiably broad range of the present and proposed powers of access to telecommunications data (Terms of Reference (TOR) paras 3.a., A.2.a., and C.15.c.)

Making this submission is hampered by the inadequacy of the Discussion Paper. It is confusingly laid out and does not follow the TOR. For example, some material relevant to Section A of the TOR is at pp 23 et seqq and some is at pp 41 et seqq.

A proper discussion paper should identify issues, provide relevant factual material, suggest changes, and canvass arguments for and against the changes.

This Discussion Paper does not do so. It is, rather, a prospectus for the Government's (for which read "bureaucracy's") proposals, often reassuringly (but dubiously) described as "reforms".

Astonishingly, the Discussion Paper contains no discussion at all of the

proposal to require retention of tele. communications data for up to 2 years (TOR C.15.c) — a feature of the package which has attracted widespread public criticism (see, e.g., Attachment A).

The proposal for a single warrant with multiple TI powers (TOR B.8) — surely a matter of significance — does not appear to be discussed either.

With these deficiencies in the Discussion Paper, I have been unable to prepare a submission which addresses specific proposals in light of my concerns.

However, against TOR 3.a., A.2.a., and C.15.c., I would like to record my strong opposition to the scale of the present and proposed powers of access to telecommunications data. This opposition relates both to the frequency with which the powers are exercised and the large number of agencies which can exercise these powers.

These points are demonstrated by the facts in the article at Attachment B. It is astounding that the access power was exercised 250,000 times in 2010/11. It is equally astounding that such a wide range of agencies have the power — what possible reason is there for Medicare or Australia Post to enjoy this power?

The potential for misuse of the power is shown by the fact that the Victoria Police exercised the power some 65,000 times in 2010/11. The facts that "auto processing" is used in these matters, that authorisation is internal rather than by warrant, and that there is no external scrutiny, are deeply troubling. This, after all, is the Victoria Police whose officers (we have recently learned) did not think it necessary to actually swear the affidavits they submitted in applying for search warrants!

The scope for wholesale intrusion into personal privacy is demonstrated by the Department of Defence leak inquiry which accessed the call records of 14,000 phone services. The intrusion into personal privacy here was totally disproportionate to any conceivable public benefit. Political or bureaucratic embarrassment is not an overarching justification for trampling our civil liberties.

If the power of access to telecommunications data is to continue, it should be limited as follows:

- it should only be used in relation to the investigation of significant security matters or serious crimes;

- it should only be available to security and law enforcement bodies (see the British proposals referred to at Attachment C);
- it should never be used for the purposes of revenue gathering or debt recovery;
- it should require authorisation by an external body;
- the scope of any authorisation should be strictly limited, based on proper cause and proportional to the need.

The Australian people are entitled to be secure in their persons, homes, property and communications against unreasonable search or intrusion by Government agencies or apparatchiks (compare, in this context, Attachment B.).

Failing vigilance in this respect, we slide inexorably into a Stasi State (Attachment E).

Yours sincerely

(MR. STEPHEN BROWN)