Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

28 October 2010

Mr Hamish Hansford
Secretary
Senate Legal and Constitutional Affairs Committee

LegCon.Sen@aph.gov.au

Dear Mr Hansford

Re: Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

Thank you for your invitation to make a submission to the Committee's Inquiry into the above Bill.

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF expresses the most serious concern about this Bill.

Its effect is to destroy the hitherto carefully maintained separation between the roles of national security and law enforcement.

The APF is also very concerned that major changes have been presented in such a manner as to mislead the public into thinking that they are merely fine tuning.

A detailed analysis is provided in the Attachment.

It is vital that the Senate Committee, and the Senate, strongly recommend against passage of this very dangerous proposal.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation
Submission to the Senate Legal and Constitutional Affairs Committee

27 October 2010

Telecommunications Interception and
Intelligence Services Legislation Amendment Bill 2010

General Comments

This Bill should cause the Committee significant concern, as it **makes wholesale changes to the deliberately and carefully constructed walls separating the roles of national security and law enforcement.**

These walls have been erected because of the extraordinary powers granted to some agencies for some specific functions, where the risk to the public interest is particularly great and where some extraordinary derogation from norms of civil liberties and human rights, including privacy, has been justified.

Not for the first time, major changes are presented as minor marginal fine tuning. The Committee, and the Australian community, should instead see the amendments for what they really are – a wholesale demolition of some important barriers that strike an appropriate balance between various public and private interests.

The Bill comes close to giving a very wide range of enforcement agencies (and not just those engaged in criminal law enforcement) access to the same extraordinary powers that have rightly been limited, to date, to a few specialised agencies with narrow and targeted functions.

The Australian Privacy Foundation accepts that some marginal changes may be justified from time to time to recognise new environments and threats, but the changes embodied in these amendments go far beyond that marginal adjustment and should be rejected. The legitimate objectives of greater co-operation can, in our view, be achieved in other ways, in specific cases and investigations.

The Bill dangerously conflates significant distinctions between national security, national intelligence, criminal law enforcement and wider enforcement functions.

While some residual barriers remain or are re-asserted in the Bill, they are seriously weakened – such as the proposed threshold of 'offences carrying a penalty of at least 12 months imprisonment' which in many jurisdictions would widen the range of offences for which the extraordinary powers could be used.

The Bill gives the specialised national security and national intelligence agencies very broad discretion to assist other agencies, with the 'only on request' proviso being a weak safeguard – invitations can and would be easily contrived.

Some of the changes are justified by reference to a 2008 National Security Statement which is said to have redefined the nature of the threat and necessary level of co-operation. However, that Statement is not widely known and has never, to our knowledge, been the subject of parliamentary or wider public debate. This Bill provides a first opportunity for that debate, and the two year old Statement should not therefore be taken as representing a 'given' or acceptable foundation. The same goes for the National Security Information Environment Roadmap: 2020 Vision, published by the Department of Prime Minister and Cabinet earlier this year, which presents a somewhat confused picture of proposed cooperation, with inconsistent definitions, only token acknowledgement of privacy, and none of wider civil liberties, as important values to be protected.

In the Second Reading speech the Minister stated an objective of "shaping and supporting a national security community… ". This community was undefined, but **the goal "to protect our communities from criminal and other activities threatening our national and personal wellbeing" suggests a scope well beyond any traditionally accepted concept of 'national security'.**

The effect of the Bill would be to give statutory authority for radically new, dangerous and unacceptably broad concepts of 'national security' and 'national security community'.

Specific comments on the Explanatory Memorandum

Paragraph 1 uses the term national security communities (plural) compounding the problem of loose and inconsistent definitions.

Paragraph 2 contains a non-sequitur – it is not clear why a specific failed terrorist attack in the US highlighted the need to 'remove legislative barriers to ... intelligence sharing." We can all agree that greater cooperation on specific categories of investigations is desirable (and the lack of cooperation is a much greater problem than a paucity of information), but that does not justify an illogical leap that all deliberately imposed barriers can be swept away.

Paragraph 5 fails to explain why the required interception expertise and assistance cannot and should not be provided by the AFP (which has already an established role in this respect) rather than authorising ASIO to do so (Schedule 1). ASIO's interception powers are deliberately different from those currently available to law enforcement agencies, for good reasons, not least because they are subject to fewer and less transparent safeguards. This distinction should be preserved.

Paragraph 6 asserts that the Bill does not affect the distinction between law enforcement and intelligence functions. This is simply not true, at least without more clearly distinguishing national intelligence – the exclusive preserve of a narrow set of designated national intelligence agencies – from the more routine intelligence functions which are undertaken by most law enforcement agencies.

Paragraph 7 explains that the Bill also implements two changes – in relation to finding missing persons (b) and permitting delegation of the person to be notified (d) which are questionable – see our later comments

Under the heading Financial Impact Statement, the EM asserts that the amendments will have no financial impact. This may be the case for the Commonwealth budget (although it is not clear if ASIO will provide assistance to State and Territory agencies at no cost). But **it is difficult to see how the new requirements for carriers and nominated carriage service providers (C/NCSPs) to regularly inform the government of proposed changes (Schedule 2) will not incur significant extra costs for them**. This may be more appropriately addressed in a Regulatory Impact Statement, but this is not provided.

Specific Comments on clauses

Amendments to the Telecommunications (Interception and Access) Act 1979

Schedule 2, Item 4 – it is not clear if the new definition of 'notifiable equipment' includes software changes – if it does (as one would expect given the objective) then the scope of the requirement is significantly broadened.

Schedule 2, Item 8 – again, the scope of **the new requirement is not clear but it would appear to be an onerous burden on C/NCSPs to, requiring them unreasonably to 'speculate' about the possible effects of changes and whether they might have a 'material adverse effect' on capacity to comply with interception related obligations**. This also goes to the issue of cost already mentioned above.

Schedule 3 – it is not clear how, if the use of relevant information for the purposes of missing person investigations is to be subject to an overriding 'consent' condition, why the amendments are necessary, as consent is already an exception to the non-disclosure provisions of the Telecommunications Act. Item 5 suggests that disclosure of missing persons information will be

authorised without consent where consent is impracticable, but again, **there are existing exceptions in the Telecommunications Act which address situations where safety, life or health are at risk**.

It is also not clear how the new provisions relate to confirmation to third parties of communications activity by a missing person (proof of life?) – as opposed to substantive information e.g. about location or content of communications. Would the former disclosure be authorised without consent, even though this may be contrary to the wishes of the missing person?

Item 7 – **it is not clear whether the authority for police to use missing person information to locate such a person is limited by the ultimate purpose** e.g. is it only where the police are pursuing one of their other functions, or can location of a missing person be an end in itself (whether or not there is any evidence of foul play or wrongdoing)?

Schedule 5 – The justification for allowing notifications relating to interception to be made to carrier representatives authorised by the Managing Director is not convincing. There appears to be no requirement for consent, or positive action, by the recipient of a notification – arrangements are in place to allow interception to proceed – and the notification serves only, but importantly, as an accountability device. **No evidence is given of the inability to contact a Managing Director having delayed interception in practice** – any such effect of interpreting 'after the MD has been notified' as after he or she has become aware of it could readily be addressed by a simpler amendment, to provide only that the notice must have been appropriately 'delivered'. **Allowing notification to be made to more junior staff is unnecessary and would significantly weaken the effect of the requirement as an accountability measure** – notifications could be 'out of sight' of senior management and interception activity become more accepted as commonplace not deserving of executive notice or attention.

Schedule 6 – **the provision for other agencies to be prescribed by Regulation gives an unacceptable level of discretion to the Executive**. As we have consistently argued in many submissions to this and other Committees, Regulations inevitably receive less scrutiny by Parliament than primary legislation. **Major decisions on policy settings, such as in this case the determination of which agencies – including non-law enforcement agencies, can get the benefit of national security and national intelligence agency assistance, should remain the prerogative of Parliament to make in the legislation itself**.

Other Amendments to the ASIO Act 1979

Item 7 – the proposed new definition of 'law enforcement agency' is expressly designed to include 'other bodies that have functions connected to law enforcement, such as Integrity and corruption agencies and also other agencies with investigatory and enforcement powers with respect to Commonwealth and State laws'.

However, definitions of 'law enforcement' or 'enforcement agency' are very different in different statutes – for example in the Surveillance Devices Act 2004 and the Crimes Act 1914, while related definitions of 'enforcement body' in the Privacy Act 1988, and 'designated agency' in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 are different again.

We submit that **there is an urgent need for consistency in the use of the term 'law enforcement agency' across all Commonwealth (and preferably State and Territory) legislation and urge the Committee to call for a review**.

In the context of the proposed amendments to the ASIO Act, the new definition is far too broad, and should be limited to a finite list of specified agencies set out, for these purposes either in the ASIO Act or in the TIA Act – see our comments on the undesirable Regulation power above. **This list should not include the wide range of agencies that may have incidental 'investigatory and enforcement powers' – which would be most government agencies**. It is completely unacceptable to even provide for the possibility of ASIO, ASIS or the DSD providing assistance to the administration of parking fines or fishing licences. However remote this may be from the government's intention, it must not be facilitated by such a

broad definition, particularly in light of the broad range of types of assistance set out in the EM under item 17.

Item 8 – **the proposed definition of 'serious crime' as 'an offence punishable by a period of imprisonment that exceeds 12 months' represents a significant lowering of the threshold in some jurisdictions, where the current threshold is 'indictable offence'**, which can mean one carrying a potential sentence of 2 years or more. Thresholds should not be lowered in the pursuit of uniformity – it this is important they should be raised to the highest common level.

Item 10 – **the proposed deletion of 'and not otherwise' is undesirable in the context of our objection to the extension of ASIO functions to non-security related purposes** (see above).

Item 12 – **the proposed discretion for ASIO to authorise communication of information where there is a 'national interest' is far too broad. For the reasons given in the rest of this submission, it should be rejected**.

Similarly, the provision in 18(4A) for ASIO to be able to provide information to ASIS, DSD and DIGO even where it is NOT cooperating with those agencies appears dangerous and unnecessary.

Item 17 – the re-assurance that cooperation under the proposed new section 19A will be subject to 'any arrangements made or directions ... given by the Minister ' is welcome but is nullified by the fact that there may not be any such directions, as is admitted later – hence **it is false to claim that this will 'ensure that the Minister has appropriate oversight' as he or she may choose not to!**

The re-assurance given in the EM at the end of item 17 that ASIO will be required to comply with the ASIO warrant requirements when assisting other agencies is false, as the other changes to the TIA Act mean that ASIO would now more typically be exercising warrants on behalf of law enforcement agencies under the LE warrant provisions.

Amendments to the Intelligence Services Act 2001

Item 19 – this proposed carve-out from the definition of 'intelligence information' merely compounds the terminological confusion to which we have already referred.

Items 20-27 – these provide for ASIS, DSD and DIGO to assist a wide range of agencies with functions which go well beyond traditional concepts of national intelligence, and with the same broad range of types of assistance (EM re item 27) as is proposed for ASIO.

The same criticism also applies to the re-assurance about Ministerial directions, as these are again optional and may not exist.

For the same reasons already given above, we urge the Committee to reject this major and unacceptable expansion of the role of these agencies.

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90)
  http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-)
  http://www.privacy.org.au/Campaigns/Media/