Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

10 November 2014

Chair
Parliamentary Joint Committee on Intelligence & Security
Parliament House
Canberra ACT 2600

Dear Sir / Madam

Re: Counter-Terrorism Legislation Amendment Bill (No. 1) 2014

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

This Bill poses substantive privacy concerns that should be explored by the Committee.

The very short period allocated for that exploration is deplorable, as is the shorter time for submissions to the Committee by specialist and nonspecialist members of the Australian public. Committees have traditionally allowed significant longer periods for the provision of submissions and for in-person testimony.

Submissions by the Australian Federal Police, the Australian Security Intelligence Organisation and Attorney-General's Department regarding the suite of national security legislation – of which the current Bill forms part – have not demonstrated that there is a compelling need to fast-track passage of the legislation and to curtail appropriate public consultation.

Inadequate consultation fosters suspicion of legitimate national security activity, potentially encouraging disaffection among some groups within Australia and abroad. It also inhibits the identification of drafting errors and administrative problems that are for example in contradictory statements by the Attorney-General, the then head of ASIO, executives of the Australian Federal Police, and the Minister and Department of Communications, regarding pervasive surveillance through mandatory retention and warrantless access to metadata.

I attach the APF's Submission on this matter.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation

Australian Privacy Foundation

Counter-Terrorism Legislation Amendment Bill (No. 1) 2014

The current Bill appears to be predicated on the assumption, which the Government has not substantiated, that the Australian nation faces an ongoing existential threat from terrorism (in particular from criminals and sympathisers located within Australia rather than people engaged in offences offshore).

The Bill also appears to be predicated on the further assumption, also unsubstantiated, that the existing arrangements regarding authorisations are inadequate.

On the basis of those assumptions the Government is proposing to weaken existing law in a process that at least one independent observer has characterised as a drip-feed erosion of privacy protection.

That erosion is inappropriate. It is contrary to the strong regard voiced by ordinary Australians for privacy (for example through surveys by the Office of the Australian Information Commissioner, commercial entities and scholars). It is also contrary to Australia's commitment to human rights through both a range of international agreements (some of which are highlighted in the Attachment to this submission, which quotes the Government's Explanatory Memorandum for the current Bill) and through a very extensive body of law since at least the time of Entick v Carrington (1765).

The erosion reduces official and ministerial accountability, two foundations of legitimacy in any action against terrorists or other criminals. It privileges bureaucratic convenience over what is legally proportionate. Reducing the accountability of ministers and officials is not good law and not good policy. Neither is a Bill that encourages abuses by enabling inadequate or sloppy documentation.

In the absence of strong evidence for why existing law is inadequate the Committee should not endorse the Bill. Neither the Ministers nor the officials have demonstrated that there is a significant structural problem with the current enactments. The need to fast-track a statutory fix for something that is not broken is accordingly unclear. An independent submission to the Committee has indeed suggested that if there is a problem it should be addressed administratively rather than through a change to the law.

Communication problems for example might most appropriately be solved through enhancing the government communication infrastructure and reskilling Australian Federal Police or other officials rather than resorting to law that allows ministers to give oral authorisations, allows authorisations to be made by officials independent of ministers and very substantially weakens documentation requirements (in practice the official only needs to get one point right) in a context where the contestability of decisions will be unavailable or uncertain.

The Government has implicitly asked all Australians to trust in the diligence of the Australian Federal Police and other agencies, whom we are to assume will be rigorous in meeting all requirements. That trust is called into question by a succession of failures on the part of leading agencies, for example the Federal Police 'raid' on Channel 7 this year that was initially defended by senior Police executives and subsequently acknowledged to have been badly executed on the basis of poor advice.

The Foundation reiterates concerns regarding the adequacy of oversight by the national Privacy Commissioner, by the Commonwealth Ombudsman. and other bodies. Inadequate resourcing of key agencies, along with questions about their commitment to actively investigate and independently report on issues on a timely basis raises questions about whether the weakening of human rights protection inherent in the current Bill and associated national security enactments will be addressed.

The Bill refers to circumstances in which no designated Ministers are available to issue an emergency authorisation or provide agreement". Greater clarity regarding "not readily available" is essential and the Foundation suggests that this should be explored by the Committee.

The Foundation expresses concern regarding the abandonment of the current requirement for emergency authorisations to be issued in writing. In the absence of hard evidence of systemic failure there should be no change.

The Committee should be cautious in endorsing any expansion of oral authorisations, irrespective of whether they are retrospectively documented. Law enforcement and national security agencies have the capacity to prepare documentation on a timely basis for signature by the relevant Minister. They should continue to do so rather than seeking the freedom implicit in oral or delegated authorisation.

The Committee should note community concern regarding justification for privacy-erosive amendments on the basis that an existing enactment (potentially one that was complex and received cursory examination) has a similar provision. There is widespread concern that we are seeing a cascade of small amendments that over time will have a significant effect but are disregarded because observers look at changes in isolation and are reassured by the Government of the day that there are no problems.

The Foundation has particular concerns regarding the proposal that officials need not explain all elements of an application for an order but can simply provide an overall justification, with courts correspondingly not needing to consider every ‘obligation, prohibition and restriction’ in an Order. As noted elsewhere, that ‘streamlining’ is bureaucratically convenient but is inappropriate and should not be endorsed by the Committee.

Australian Privacy Foundation

ATTACHMENT: PRIVACY PARAS FROM EXPLANATORY MEMO

40. Article 17 of the ICCPR provides that no one shall be subject to arbitrary or unlawful interference with their privacy. The collection, use and storage of personal information constitutes an interference with privacy. The control order regime limits the right to protection against arbitrary and unlawful interferences with privacy to the extent it can require the person to wear a tracking device (paragraph 104.5(3)(d)), require the person allow himself or herself to be photographed (paragraph 104.5(3)(j)) and allow impressions of a person's fingerprints to be taken (paragraph 104.5(3)(k)). These limitations on the right to privacy are justified on the basis they protect the public from a terrorist act. These obligations assist in advancing Australia's national security and ensure identification and enforcement of the control order. Photographs and impressions of fingerprints obtained under paragraphs 104.5(3)(j) and (k) are collected, stored and disclosed in accordance with the Australian Privacy Principles (noting that there have been no control orders since the enactment of the Australian Privacy Principles) and section 104.22--treatment of photographs and impressions of fingerprints.

41. The procedures by which this restriction on privacy is permitted are authorised by law and not arbitrary. The operation of the control order regime is prescribed clearly in Division 104. The use of the term `arbitrary' suggests that any interference to privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable, necessary and proportionate to achieving that objective.

42. Legislative safeguards within the control order regime in Division 104 operate so as to not limit the right to privacy beyond what is reasonable, necessary and proportionate. These include that the restrictions imposed by a control order must be `reasonably necessary' and `reasonably appropriate and adapted' for the purpose of protecting the public from a terrorist act. Further, a photograph or impression of fingerprints obtained from the subject of a control order must only be used for the purpose for which they were taken - ensuring identification and enforcement of the order (subsection 104.22(1)). Subsection 104.22(3) creates an offence where a person uses the photograph or impression of fingerprints in a manner inconsistent with the purposes of ensuring compliance with the control order. The offence carries a maximum penalty of imprisonment for two years. Furthermore, a photograph or impression of fingerprints obtained from the subject of a control order must be destroyed as soon as practicable after 12 months after the control order ceases to be in force (subsection 104.22(2)). These guarantees seek to minimise the level of interference with privacy and demonstrate an intention to permit interference only to the extent that it is reasonable, necessary and proportionate to achieve a legitimate end. …

51. The Government is of the view that the provisions of Schedule 2 to the Bill do not engage any human rights, on the basis that the provisions are directed to clarifying and streamlining - without reducing safeguards - the procedural arrangements that enable ISA agencies to undertake activities, with appropriate authorisation to do so. …

53. However, the Government acknowledges that contrary arguments may be advanced, on the basis that amendments which streamline authorisation processes might be said to extend the ability of ISA agencies to obtain an authorisation to engage in activities for the purpose of collecting intelligence on, or undertaking other activities in relation to, persons or entities outside Australia. The Statement of Compatibility has been prepared to address such contentions, in the event that the Government's position is not preferred or accepted by those scrutinising the Bill. The following analysis identifies the rights that might be said to be engaged for the above reason, and explains how any limitations thought to be imposed are adapted to a legitimate objective, and are necessary for, and proportionate to, the achievement of that objective. …

55. To the extent that the measures in the Bill extend the ability of ISA agencies to obtain a Ministerial authorisation to undertake activities permitted under the ISA for the purpose of collecting intelligence on, or undertaking other activities in relation to, persons or entities outside Australia, they might be said to engage the right to protection against arbitrary and unlawful interferences with privacy and reputation of persons who may be the subject of, or otherwise affected by, such activities.

56. Any interference with personal privacy as a result of the authorised activities of ISA agencies relevant to the performance by those agencies of their statutory functions is necessary for the achievement of a legitimate objective. In the case of the amendments to the statutory functions of ASIS, this legitimate objective is to ensure that ASIS is able to provide critical support to the ADF in support of military operations, and for the purpose of cooperating with the ADF on intelligence matters, in a timely way (including in circumstances that may enable ASIS to assist in saving lives of Australian soldiers and other personnel deployed to conflict zones).

57. The amendments in Schedule 2 concerning emergency authorisations are further necessary to achieve the legitimate purpose of enabling intelligence agencies to act quickly (by reason of an agile emergency authorisation process) to collect vital intelligence in circumstances of extreme urgency or to take other action in accordance with the ISA, where to follow the normal processes governing Ministerial authorisations would preclude agencies from obtaining such intelligence, or otherwise compromise their ability to do so. (This may arise if, for example, none of the Ministers who are able to grant an authorisation are readily available or contactable, as no contingency arrangements are presently made in the ISA for this. Such an undesirable outcome may also arise if the requirement that emergency Ministerial authorisations must be in writing cannot be satisfied in a particular case - for example, by reason of a Minister's remote location without access to means of instantaneous written communication or because the circumstances are so time-critical that the time taken to reduce an authorisation to writing may cause the relevant intelligence collection opportunity to be lost.)

58. Any such interference with personal privacy as a result of the measures in Schedule 2 is also subject to extensive and appropriate safeguards to ensure that it is necessary, appropriate and adapted to the legitimate objectives to which the amendments are directed as noted above.

59. In particular, any such interference will be limited, because activities may only be authorised if the relevant criteria are satisfied. (These criteria are applied by a Minister, or an agency head in the case of emergency authorisations in the event that a Minister is not readily available or contactable). These include that the Minister (or agency head, in the case of emergency authorisation) must be satisfied, before giving an authorisation, that any activities done in reliance on the authorisation will be necessary for the proper performance of a function by an agency, there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency, and there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purpose for which they are carried out. In addition, authorisations that are issued on an emergency basis are subject to a strictly limited maximum duration of 48 hours and cannot be extended.

60. There are appropriate safeguards and oversight mechanisms in place to ensure the proportionality of activities undertaken by ASIS for the purpose of performing the new statutory functions inserted by Schedule 2 to the Bill, and activities undertaken in reliance on emergency authorisations. In particular, the activities of ISA agencies are subject to the independent oversight of the IGIS in accordance with the Inspector-General of Intelligence & Security Act 1986.

61. In addition, the ability of an ISA agency head to provide an emergency authorisation in place of a Minister (and the Director-General of Security to provide agreement to the making of an emergency authorisation in place of the Attorney-General) are subject to extensive limitations and safeguards. The emergency powers of authorisation are only exercisable if the agency head is satisfied that none of the relevant Ministers are readily available or contactable. The agency head must be satisfied not only that it would have been open to the relevant Minister, on the facts of the case and the statutory authorisation criteria, to issue the authorisation; but further satisfied that the relevant Minister would have made the decision to issue (which requires consideration of how that particular Minister might have weighted different considerations, including based on an awareness of any authorisations issued for previous activities). To ensure it only applies in an extreme emergency, the agency head must also be satisfied that if the activity was not authorised security would be seriously prejudiced or there would be a serious risk to a person's safety. The relevant agency head must also report on the making of any authorisation to the responsible Minister (to whom the agency head is accountable) and to the IGIS (who may conduct oversight of issuing decisions). The

responsible Minister is also under a positive obligation, on receipt of such a report, to consider whether to cancel the authorisation, or to issue a Ministerial authorisation, or to decline to do either of these things and allow the emergency authorisation to run to its 48-hour maximum, after which time it will cease. The relevant agency head must, in reporting to the Minister on the issuing of an emergency authorisation by that agency head, specifically advise the Minister of his or her obligation to make a decision.

62. Further, any intelligence produced can only be retained and communicated in accordance with the rules to protect the privacy of Australians, made in accordance with section 15 of the ISA. In making the rules, the relevant Minister must have regard to the need to ensure the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agency of its functions. The ISA also requires that agencies must not communicate intelligence information, except in accordance with the rules. The IGIS must brief the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the content and effect of the rules if requested or if the rules change.

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 is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

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

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, 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/