The Secretary
Joint Committee on Intelligence & Security
Parliament House
Canberra ACT 2600

Inquiry into the *National Security Legislation Amendment Bill (No. 1) 2014* (Cth)

This submission responds to the Committee's call for public comment on the *National Security Legislation Amendment Bill (No. 1) 2014* (Cth).

In summary –

- aspects of the Bill, such as formally renaming the Defence Signals Directorate, are unexceptional and present no concerns
- the potential for inappropriate restriction of legitimate media activity, is highly undesirable. Uncertainty threatens to have a chilling effect that is contrary to the principles of Australia as a liberal democratic state and that will foster distrust of legitimate national security and law enforcement activity
- the need for trust in the national security regime is fundamental. That trust can be fostered by the Committee considering the Bill in a broader privacy context and encouraging stronger resourcing of key accountability mechanisms such as IGIS and the INSLM.

Basis

The submission is made by Assistant Professor Bruce Baer Arnold. I teach law at the University of Canberra, including graduate teaching regarding privacy and national security. My work has appeared in leading Australian and overseas law journals. I was formerly the general editor of *Privacy Law Bulletin*, the Australian privacy and data protection practitioner journal.

The submission does not involve what would be reasonably construed as a conflict of interest. It does not necessarily represent the views of the University of Canberra.

The submission reflects familiarity with relevant Australian law and with overseas regulatory frameworks and jurisprudence, particularly that in Europe and United States. Those frameworks are relevant because they provide benchmarks for activity in Australia and should result in caution about advocacy statements from particular government agencies.

A review of the Australian framework

There is growing acknowledgment within the Australian legal, telecommunications, law enforcement and national security communities of the desirability of conducting a comprehensive principles-based review of Australia's legal and policy framework regarding national security and law enforcement activity in the digital environment.

I refer to 'digital environment' because traditional practice and legislation at the national and state/territory levels is failing to keep pace with developments such as

- the emergence of 'citizen media',
- ready accessibility of a range of multi-function devices such as smartphones,
- anonymisation tools such as TOR,
- increasing use of cloud computing and offshoring
- geolocation capability in vehicles, shipping containers, cameras and other devices,
- consumer uptake of social network services
- public and private sector collection of metadata.

In responding to those developments it is imperative that Australia adopts a principles-based and coherent approach that is founded on proportionate responses to substantive threats.

It is axiomatic that law enforcement and national security activity should be proportionate rather than based on what is bureaucratically convenient. That activity should be subject to meaningful oversight, an oversight that requires resourcing of bodies such as IGIS (and responsiveness by ASIO and other agencies to questions by parliamentary committees) rather than merely formal powers.

It is also axiomatic that we should be wary of treating law enforcement as indistinguishable from national security and for example equipping all national, state/territory and local government agencies (and non-government entities such as the RSPA) with authority to readily collect and/or access personal information. In that respect there are well-founded concerns regarding rhetoric this week that strengthened surveillance powers will be used in a 'war' against 'general crime' rather than national security matters.

How do the above comments relate to the Committee's inquiry into potential implementation through the *National Security Legislation Amendment Bill (No. 1) 2014* (Cth) of its past recommendations? There are several answers.

Considering the Bill in context

The first is that we should be looking beyond the specific recommendations and the Attorney-General's tick list in its submission regarding the Bill. There is a danger of surveillance creep and regulatory myopia, with Governments (reflecting polls and agenda-setting by particular agencies) incrementally weakening legitimate protections of civil liberties – especially privacy, the freedom of political communication and reliance on warrants – and committees losing sight of the forest by concentrating on a clause that deals with the specific branch of a particular tree.

It is time for a well-resourced investigation by the Australian Law Reform Commission regarding Australia's surveillance framework, encompassing both Commonwealth and state/territory law.

That inquiry would foster community understanding of the rationales for surveillance activity and the proportionality – or otherwise – of specific mechanisms such as whole-of-population telecommunications metadata retention and warrantless access

by public/private sector entities (for example local government and the RSPCA) to telecommunication data. It would address perceptions that neither the Coalition nor the ALP dares to articulate a principles-based policy that will be misrepresented as 'soft on terror' or on 'organised crime', misrepresentation that is fostered by uncritical embrace by ministers, officials and the media of claims about the prevalence and impact of organised crime or potential terrorism.

We need an informed national discussion, rather than slow erosion of civil liberties alongside decreasing trust in politicians and agencies such as ASIO and the AFP.

Trust is fundamentally important in law enforcement, in national security and more broadly in public policy-making. Few legal scholars and practitioners consider that every aspect of law enforcement and intelligence collection/analysis should be fully open. Some, such as myself, have referred to principles and practicalities in making strong criticisms of figures such as Julian Assange and Edward Snowden. However, those people – and the broader community – are legitimately wary of over-reaching by bodies such as ASIO and the AFP and of disregard by the Attorney-General's Department and successive Attorney-Generals of expressions of concern by legal and civil society entities such as the Law Institute of Victoria, Australian Privacy Foundation and Law Council of Australia during the past decade in relation to proposed surveillance legislation.

Resourcing the accountability mechanisms

That trust is significantly undermined by the unwillingness of the current and previous national Governments to appropriately resource key agencies such as the Inspector General of Intelligence and Security and the national Privacy Commissioner.

Plans to abolish the Independent National Security Legislation Monitor – to achieve a saving less than the Commonwealth funds allocated to accommodation for a ballet school in Victoria – and the Office of the Australian Information Commissioner (an agency whose incapacity was in part attributable to underfunding under the preceding Government) are unsurprisingly read as signalling that the major political parties are indifferent to questions about trust.

That indifference is especially problematical in the context of statements that erode trust, for example AFP Asst Commissioner Gaughan's 2012 claim that opposition to mandatory data retention in Germany (which he incorrectly attributes to the German government rather than courts) has left the German federal police agency a laughing stock and is "causing all sorts of problems". We might hope that the AFP is made of sterner stuff and is sufficiently resilient to cope with occasional inconvenience. (As far as I am aware law enforcement in Germany has not ceased and respect by Germany's national legislature for privacy as a core value has bipartisan support.)

Indifference is problematical in the face of criticisms by bodies such as the UK Independent Reviewer of Terrorism Legislation, who in his latest report on UK surveillance legislation warned about the criminalisation of legitimate media activity and about ongoing incremental inappropriate expansion of the powers of law enforcement and national security agencies. That report is consistent with a recognition that activity needs to be proportionate rather than merely lawful, given that lawfulness is often simply a matter of securing the required number of votes in the legislature.

Indifference is problematical in the face of research indicating that large-scale official

access to metadata is not a silver bullet for either national security or law enforcement. (I acknowledge that the Committee in the current inquiry is not concerned with mandatory data retention but note that matter as an indication of the need to think holistically rather than on a clause by clause basis.)

Proper oversight – a matter of resourcing and legislation – is essential. In testimony to the Senate Legal & Constitutional Affairs last month ASIO's Director-General referred to integrity being in that institution's DNA and stated that oversight was effective. I assume that the same response would have been made by the chief of the Central Intelligence Agency in the US (whose personnel have this year been revealed to have illegally surveilled a Congressional committee) and the Metropolitan Police in the UK (with official acknowledgment of significant corruption). Historically Australia's national security agencies appear to have been inept rather than corrupt. Presumably the new 'DNA' means that their performance of an often invidious task is more effective than in the past. A succession of inquiries into corruption in the state police forces and questions about the integrity of personnel in the Australian Customs Service mean however that we should be wary about permissiveness in the sharing of surveillance information across jurisdictions.

Malcolm Turnbull's cogent 2012 Alfred Deakin Lecture raised questions about rights and responsibilities regarding public and private surveillance. Those questions have been raised by other politicians, such as Scott Ludlam, irrespective of political affiliation. They are important in terms of principle and because they strongly reflect the concerns of most Australian voters, of lawyers and of business.

We do need a strong and vigorous law enforcement and national security community. That community must however be accountable.

I thus suggest that the Committee looks beyond the specific clauses in the Bill by considering

- the relationship of the proposed legislation with other law, in particular the *Privacy Act 1988* (Cth) and the *Telecommunications Act 1997* (Cth), as the basis for a coherent national regime that respects the dignity of all Australians
- the strengthening of bodies such as IGIS, the INSLM and Privacy Commissioner
- the basis for claims made by the Attorney-General's Department, ASIO and the AFP – claims that are sometimes obfuscated through reference to a need for secrecy because of law enforcement and national security.

Warrants

I suggest that the Committee considers the potential for abuse through weakening of the current warrant system.

It is no doubt inconvenient for law enforcement and national security personnel to have to seek warrants. There have been no indications that such inconvenience is tangibly fostering terrorism or other illegal activity.

As a liberal democratic state we should be very wary of removing the accountability that is provided by warrants. All government agencies must be accountable. Inconvenience is an appropriate cost of law enforcement and national security activity in the same way that having elections (and funding the Australian Electoral Commission) is acceptable.

The Media

I suggest that the Committee consider the potential misuse of the Bill to restrict legitimate investigation and reporting by the media. We may well be disquieted about the culture of particular media organisations, for example the illegality evident in connection with the *News Of The World*, but a free press – to which all major parties are committed – is a foundation of the liberal democratic state.

Governments have on occasion sought to restrict publication of information that would be embarrassing, would undermine law enforcement or cause harm to an individual. Australia's courts have strong record of sensible principled decision-making that has allowed publication in the public interest where appropriate and has restricted publication in the same interest where appropriate.

ASIO's Director-General last month indicated that the proposed legislation would never be misused. I have no reason to doubt his sincerity but I note that ASIO Director-Generals – and Attorney-Generals – come and go. Given my comments about trust it would be best to ensure that the Bill does not embody overreach. There is a need for statutory clarification so that we do not need to rely on the opinion of an office-holder who may not be around when a decision has to be made.

Uncertainty about misuse has the potential to chill legitimate media activity and public discourse. As such it is highly undesirable.