Submission No 184

Inquiry into potential reforms of National Security Legislation

Name: Benedict Bartl
Policy Officer

Organisation: Tasmanian Association of Community Legal Centres

TASMANIAN ASSOCIATION OF COMMUNITY LEGAL CENTRES

Animal Welfare Community Legal Centre • Environmental Defenders Office • Hobart Community Legal Service • Launceston Community Legal Centre • North West Community Legal Centre • Tenants' Union • Women's Legal Service • Worker Assist

27 August 2012

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Secretary,
Re: Inquiry into Potential Reforms of National Security Legislation

We appreciate the opportunity to make a submission to an inquiry initiated by the Parliamentary Joint Committee on Intelligence and Security into potential reforms of national security legislation.

TACLC is an incorporated network representing the eight community legal centres in Tasmania. Our member centres provide accessible advice, representation and legal education services to the community, and advocate for law reform on a range of public interest matters.

The Committee's decision to review Australia's national security legislation at a time of relative calm is welcomed. A climate of fear has historically surrounded terrorism legislation ensuring both a lack of deliberation and scrutiny. The Committee is therefore to be commended for seeking neither the introduction of emergency measures nor acting out of a need for an urgent response.

The Tasmanian Association of Community Legal Centres (TACLC) endorses the recommendations outlined in the Gilbert + Tobin Centre of Public Law submission, particularly the focus on ensuring that any and all reforms are counter balanced through the implementation of appropriate safeguards including protection of human rights. Although the Federal Government has introduced a *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) we do not believe that a legislative 'statement of compatibility' provides adequate human rights protections, particularly when Parliament is called upon to consider the public interest in the protection of national security.

Whilst not the subject of review, we remind the Committee that the United Nations Human Rights Committee has urged the Australian Government to amend national security laws to ensure compatibility with international instruments[1] and that significant human rights breaches remain including the

[1] Human Rights Committee, *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: concluding observations of the Human Rights Committee—Australia* (7 May 2009)

reversal of the onus of proof which undermines the right to be presumed innocent until proven guilty.[2] In our view, the best way to assure the protection of human rights whilst at the same time maintaining national security is through the introduction of a *Human Rights Act* as recommended by the National Human Rights Consultation Committee.

Despite the lack of formal human rights protection in Australian law, if reform of national security legislation is to take place, there are a number of practical safeguards set out in the Gilbert + Tobin Centre of Public Law submission that should be introduced. The implementation of the following safeguards will provide an accountability framework that acts as a brake on Executive powers and ensures that abuses of power remain limited.

Telecommunications (Interceptions and Access) Act 1979 (Cth)

The Discussion Paper proposes a number of reforms to the *Telecommunications (Interceptions and Access) Act 1979 (Cth)* including most significantly standardising the threshold for issuing telecommunications interception and stored communication warrants. Standardisation is sought because of the distinction between a telecommunications interception warrant which may only be sought by a law enforcement agency in relation to a 'serious offence' usually defined as an offence punishable by a maximum period of at least seven years imprisonment[3] and a stored communications warrant which may only be sought for 'serious contraventions' which is defined as an offence punishable by a maximum period of three years.[4]

We endorse the recommendation of the Gilbert + Tobin Centre of Public Law that the threshold should be raised rather than lowered. That is, rather than providing that in future both telecommunication interception warrants and stored communication warrants will be issued for offences subject to a minimum of three years imprisonment we recommend that the threshold be raised to the higher threshold of an offence subject to a minimum of at least seven years imprisonment.

Of the other reforms proposed to the *Telecommunications (Interceptions and Access) Act 1979 (Cth)* we agree that there should be no proposed creation of 'a single warrant with multiple telecommunications interception powers'. In our view the current legislative requirement that law enforcement agencies apply for either a 'telecommunications service' warrant (authorising the interception of only one service, such as a single telephone number)[5] or a 'named person' warrant (authorising the interception of any telecommunication services or devices that are likely to be used by the person named in the warrant)[6] reduces

---

at [11].

[2] See for example the Amnesty International and Gilbert + Tobin Centre of Public Law submissions to the National Human Rights Consultation Committee.

[3] Sections 5D(2)-(3) and 46(1)(d) of the *Telecommunications (Interceptions and Access) Act 1979* (Cth).

[4] Sections 5E and 116(1)(d) of the *Telecommunications (Interceptions and Access) Act 1979* (Cth).

[5] Section 46 of the *Telecommunications (Interceptions and Access) Act 1979* (Cth).

[6] Section 46A of the *Telecommunications (Interceptions and Access) Act 1979* (Cth).

the risk that law enforcement agencies will use all the powers available to them rather than being used for a specific purpose as currently provided in the powers of the two warrants.

Australian Security Intelligence Organisation Act 1979 (Cth)

The *Australian Security Intelligence Organisation Act 1979* (Cth) sets out a number of warrant powers that Australia's Security Intelligence Organisation (ASIO) may apply for including search warrants, computer access warrants, listening devise warrants, tracking device warrants, postal article warrants and delivery service article warrants. As the legislation currently stands, search warrants and computer search warrants require the relevant Minister to be satisfied that there are reasonable grounds for believing that access to either the premises or the contents of the computer will substantially assist Australia's security intelligence.[7] This can be contrasted with the threshold requirement for the grant of a listening devise warrant, tracking device warrant, postal article warrants or delivery service article warrants which requires a significantly higher threshold in which a person must be engaged in, or is reasonably suspected of activities prejudicial to security and; the warrant will assist ASIO to obtain relevant intelligence.[8]

We endorse the Gilbert + Tobin Centre of Public Law recommendation that if it is proposed to create a single category of warrant that the threshold requirement for the grant of the warrant be the higher threshold. We also agree that ASIO should be required to specifically set out which out of the warrant powers it is seeking, for example a power to access a computer or use a listening device, so that it is not (ab)used as "a *carte blanche* for ASIO to exercise any and all of the warrant powers".[9]

- Broadening the definition of Computer

Similarly, we share Gilbert + Tobin Centre of Public Law's concerns that any broadening of the definition of 'computer' to include a network of computers should be accompanied by a corresponding narrowing of the circumstances in which such a warrant may be issued:[10]

> ASIO should not be able to seek a warrant to access the computers on a particular network unless there are reasonable grounds to believe that the person in relation to whom intelligence is being sought had a connection with computers other than his own on the network.

- Search Powers

The Discussion Paper also proposes that ASIO be able to apply for a warrant to search a person, 'regardless of whether a premises search warrant has been

---

[7] Sections 25 and 25A of the *Australian Security Intelligence Organisation Act 1979* (Cth).

[8] Sections 26, 26A, 27 and 27AA of the *Australian Security Intelligence Organisation Act 1979* (Cth).

[9] Gilbert + Tobin Centre of Public Law submission at 11.

[10] Gilbert + Tobin Centre of Public Law submission at 11.

issued and where the person is'. This would amount to a significant expansion of the personal search powers currently provided by section 25(4A) of the *Australian Security Intelligence Organisation Act 1979* (Cth) which limits the powers of ASIO to conduct a person search to circumstances in which (i) it is specified in the warrant; (ii) the person is at or near the premises where the warrant is being executed and; (iii) there is reasonable cause to believe that the person has records relevant to the security matter.

If the Government intends to expand the personal search provisions than we would urge that a number of legislative safeguards be guaranteed as set out in the Gilbert + Tobin Centre of Public Law submission, including that the warrants be issued by an independent judicial officer, a reasonable suspicion requirement be included; the person to whom the warrant is to be applied to is to be informed of the identity of the agency conducting the search and to whom he or she may make any complaint/s; the search must be carried out in public; the warrant should operate for only a short period of time and; the search should be no more intrusive than is reasonably necessary in the circumstances.

- Issuance of Evidentiary Certificates

Evidentiary certificates protect both the identities of ASIO officers and sensitive information and are used in part to protect witnesses from having to give evidence as to how the material was obtained. We agree that whilst it may be appropriate to allow evidentiary certificates to the warrant powers dealing specifically with technology –such as listening devise warrants, computer access warrants and tracking device warrants– it is not appropriate for those warrants defined as 'physically intrusive' by the Gilbert + Tobin Centre of Public Law and including search warrants, inspection of postal and delivery service article warrants and questioning and detention warrants. We therefore recommend that evidentiary certificates be limited to listening devise warrants, computer access warrants and tracking device warrants.

- Authorised Intelligence Operation Certificates

Finally, the Discussion Paper proposes that ASIO officers and persons working in an unofficial capacity for ASIO be protected from criminal liability in circumstances in which criminal activity is engaged in during the course of an undercover operation. The proposal would allow the head of ASIO to issue 'authorised intelligence operation certificates' granting immunity from criminal and civil liability for specified conduct for a specified period. As has been observed, it is unclear why this power is considered necessary with the Commonwealth Director of Public Prosecutions retaining discretion whether or not to prosecute.[11]

Nevertheless, if legislation is to be introduced granting immunity then we would urge that the minimum safeguards set out in the Gilbert + Tobin Centre of Public Law submission be adopted including (i) criteria by which an appropriate level of seriousness is required before unlawful conduct will be authorised; (ii) that time-limits be limited to three months; (iii) that extensions/renewals of the

[11] Gilbert + Tobin Centre of Public Law submission at 15-16.

authorisation be given to an independent body; (iv) that there be appropriate record-keeping and reporting requirements; (v) that a wider range of conduct be prohibited and finally; (vi) that a sunset clause be legislatively mandated unless the Australian Government presents a case for its renewal.

Summary

In summary, TACLC urges the Committee to adopt a human rights approach to national security legislation through an assurance that any interference with the right to privacy and other human rights is 'only permitted to the extent that it is necessary and proportionate to protect Australians from serious criminal offending'.[12] In our view this approach would be in keeping with international human rights instruments to which Australia is a signatory, would provide an appropriate balance between the public interest in the protection of national security and the protection of individual human rights, and finally, would ensure that the risk of abuse of power was limited.

We thank you for your time in considering this submission.

Please do not hesitate to contact us if you have any queries or would like to discuss our submission further.

Yours Faithfully,

Benedict Bartl
Policy Officer
Tasmanian Association of Community Legal Centres

[12] Gilbert + Tobin Centre of Public Law submission at 6.