Submission No 175

Inquiry into potential reforms of National Security Legislation

Organisation: NSW Council for Civil Liberties

NSW Council for Civil Liberties Inc.

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

JOINT PARLIAMENTARY COMMITTEE ON INTELLIGENCE AND SECURITY
INQUIRY INTO POTENTIAL RFORMS OF THE NATIONAL SECURITY LEGISLATION

NSW COUNCIL FOR CIVIL LIBERTIES SUBMISSION

Part 1 General Comments

The New South Wales Council for Civil Liberties (NSWCCL) welcomes the opportunity to contribute to this important **Inquiry into Potential Reforms of the National Security Legislation** by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

1. Need for Reform of National Security Legislation

NSWCCL accepts the argument that there is a need to update and rework the relevant legislation in light of technological advances and successive amendments. However, neither of these drivers, in themselves, provides justification for an extension of powers or reduction in accountability for intelligence and law enforcement agencies, nor for the further erosion of individual privacy, civil liberties and democratic values.

There are some proposals that we consider to be appropriate and support. However, we will be asking the PJCIS to advise against proceeding with numbers of the proposals as unacceptable and, to advise against some other proposals, until their scope is more clearly defined and/or clear justification for their negative impact on civil liberties is explicitly established.

The proposals before the PJCIS, if broadly implemented, would amount to a very major expansion of the anti-terrorism laws and powers of intelligence agencies and would result in further serious erosion of civil liberties and human rights of Australians. Many of the proposals are unwarranted and dangerous.

The PJCIS has a responsibility to the Parliament and to the community to subject this sweeping package of proposals to rigorous and independent analysis, and to ensure its advice reflects a central concern to protect our civil liberties and democratic values as well as our safety and national security. The challenge is to bring substance to the rhetoric about balancing these often competing priorities with intellectual rigour and evidence based reasoned arguments.

This responsibility on the PJIC is particularly heavy because the Paper, ***Equipping Australia Against Emerging and Evolving Threats*** , emanating from the Attorney-General's Department, so signally fails its responsibility to deliver on this challenge.

2. The Review Process

NSWCCL welcomes the Government's decision to refer these proposals to the PJIS for parliamentary review with provision for supported community input[1]. This is an improvement on some earlier experiences of rushed and inadequately debated passage of anti-terror legislation. The opportunity for public input via submission to the PJIS and later attendance at committee hearings, will allow broader and more considered examination of the proposals. The provision of a discussion paper identifying specific issues, on which the Government is seeking advice, is also a useful idea - although we have considerable criticisms about the paper's adequacy and orientation.

We are appreciative of the PJCIS's extension of time for submissions by two weeks in response to requests from NSWCCL and other groups. It would have been impossible for us to have responded meaningfully within the original time frame.

Having said that, we still consider a longer time frame would have been more appropriate.[2] Given the significance of proposals flagged 'Government wishes to progress' and is 'considering progressing' NSWCCL would have benefited from more time to do a thorough, comparative analysis of relevant international approaches. The full implications of many of the proposals are difficult to grasp, because of the complexity and difficulty of the legal and technical issues involved. A longer time would have allowed more thorough exploration of these and a more detailed response.

The tight timeframe for response to the CJIS does seem a little gratuitous in the light of the reported, and welcome, statement by the Attorney-General that the Government will not be rushing the legislative response to the review.[3] NSWCCL will certainly utilise this post review opportunity to continue to explore the implications of these proposals and may seek opportunity for further input.

3. Related Reviews and their Potential Implications

NSWCCL notes that there are two other review processes relating to anti-terrorism laws underway.

The independent national security legislation monitor (INSLM) - Brett Walker QC- has an ongoing role to 'review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation. This includes considering whether the laws contain appropriate safeguards for protecting the rights of individuals, remain proportionate to any threat of terrorism or threat to national security or both, and remain necessary.'[4] Following his first annual report, which identified a most relevant and useful range of questions to be addressed, the INSLM is now seeking public submissions on the powers relating to questioning warrants and questioning and detention warrants under the *Australian Security Intelligence Organisation Act 1979* (Cth) and control orders and preventative detention orders under the *Criminal Code Act 1995* (Cth). He will report in December 2012. Submissions will be received until 10th September 2012.

---

[1] NSWCCL understands that the initial intention had been to have a much briefer CJIS review. Article by Bernard Keane Crikey.com 10 July 2012

[2] NSWCCL wrote to the PJCIS asking for a time line equivalent to that given for responses to the similar UK legislation (4 months) especially as the UK was under pressure from the pending London Olympics whereas there was no immediate pressure in the Australian context. Letter from Stephen Blanks Secretary NSWCL 16th July 2012.

[3] Quoted in SMH 10/8/2012 article by Phillip Dorling

[4] Independent National Security Legislation Monitor website; http://www.dpmc.gov.au/inslm/

On the 9th August 2012, the Prime Minister announced the long overdue review of federal and state counter-terrorism laws agreed by COAG in 2006[5]. This review, to be chaired by Judge Anthony Whealy QC, will look at 'control orders, preventative detention and certain police emergency stop, question and search powers.' It has been asked to report within 6 months. Submissions will be received until 1 November 2012.

Obviously these two reviews will be covering much common ground. This is acknowledged by the Government and the Prime Minister indicated that: 'While the Monitor's role is separate, the Review Committee will liaise with the Monitor, Mr Bret Walker SC, on this review.'

On the other hand, the Prime Minister, in the same media release, indicated firmly that the COAG review 'has no relationship to the Parliamentary Joint Committee on Intelligence and Security's examination of potential national security reforms.' [6] This is true in a narrow sense. However, all three reviews will have implications for the overall package of anti-terrorism laws in Australia. All three will have implications for the nature of our overall legal system and the extent to which civil liberties are protected.

At a practical level, these three reviews pose a significant resources challenge for NSWCCL, and we are sure, other advocacy groups. Having to respond to three important and complex reviews within a 5 month timeframe is difficult for community organizations and raises the issue of judging which review process might generate the most positive outcomes.

At a more strategic level, the cumulative effect of these three reviews will be significant in determining whether Australia continues to expand the scope and powers of intelligence agencies and executive power with the consequent erosion of core civil rights and democratic values, or whether we pause, and begin the once promised, roll-back of the more extraordinary aspects of the anti-terror laws before they become a permanent and irremovable feature of our legal system.

It seems likely that the Government will be dealing with recommendations from all three reviews during 2013 at the earliest. In addition, the sunset clauses for some of the more contentious aspects of the anti-terror legislation come up in 2016 and must be reviewed no later than six months prior to the expiry date.[7]

While many commentators consider we have already reached the point of no return in terms of roll back, NSWCCL prefers to regard the next two years as a still open determining point. These reviews and the sunset flag should provide our political leaders with an opportunity for a calm, considered and principled reassessment of our directions and an opportunity to reverse the erosion of civil liberties and rights which has been the dominant trend over the post 9/11 decade.

NSWCCL will therefore do its best to influence the review outcomes by providing informed input to each of these reviews.

4. The Elusive Big Picture

Increasingly however, NSWCCL is of the view that a more holistic intervention is necessary. The evidence is that no government over the decade has been inclined to wind back the more dangerous elements of the anti-terror laws even if formal reviews recommend they should. Rather one might

[5] Press Release 9th August 2012. The review was initially scheduled to occur in 2010.
[6] Ibid
[7] This refers to the ASIO Special Powers Regime. Division 3 of Part 3 introduce by the ASIO Legislation Amendment (Terrorism) Act 2002. There are also sunset provisions relating to Control Orders, Preventative Control Orders inserted in the Criminal Code Act 1995 and the Crimes Act 19014 which expire in December 2015. Details of the Sunset Provisions relating to anti-terrorism laws are set out in the Independent National Security Legislation Monitor ANNUAL REPORT 16 December 2011 Appendix 4 ,p 71

expect on prior trends that they are more likely to extend the reach of anti-terror laws and the powers of intelligence and law and security agencies. If governments will not take the lead in protection of civil liberties, the community must become more engaged and exert appropriate pressure.

This will not happen easily - unless there are further major public controversies arising from abuses of terrorist laws and powers by the agencies. The piecemeal and often rushed approach that has resulted in the 54 pieces of anti-terror legislation in Australia since 9/11 has left most of the community with limited knowledge or understanding of the cumulative impact on their rights and liberties.

One of the most authoritative analyses of this cumulative effect emerges from the detailed body of work by George Williams and his colleagues. Williams accepts that it was necessary for Australia to enact anti-terror laws post 9/11[8]to protect the community and to deliver on its international obligations, but he delivers an alarming assessment of the cumulative impact of the anti-terror laws enacted.

The outcome is 'a large and remarkable new body of legislation providing for powers and sanctions that were unthinkable prior to the 2001 attacks'. Williams considers most of this will remain on the statute books for the foreseeable future and will pose 'a long-term challenge for the Australian legal system and Australian democracy.' He suggests the 'overbreadth of the laws':

> … *'may, over the longer term, erode the very democratic freedoms, including the rights to freedom of speech and liberty, that they are designed to protect. The laws bring this about not only through their direct impact, but also by creating new political and legal norms. These norms broaden the extent to which it is acceptable for Australian law to sanction extraordinary powers or outcomes, such as detention without charge or the silencing of speech.*[9]

In conclusion, he points to what is the undoubtedly the fundamental problem we face in halting/reversing the trend to erode our rights and civil liberties:

> *Australia's new anti-terror laws expose structural problems with Australia's system of law. That system is dependent upon an effective parliamentary process and a culture of respect among political leaders when it comes to democratic values, rule of law principles and human rights.*
>
> *Anti-terror laws reveal how many of the bedrock principles of Australian democracy are actually only*
> *assumptions and conventions within the political system rather than hard legal rules that demand compliance. The laws reveal the capacity of politicians and parliaments to readily contravene these values, and in doing so to create new and problematic precedents for the making of other laws. This can happen because of weaknesses in political leadership and the fragile status of important values within Australian democracy.*[10]

There is clearly need for a broad and well informed national discussion of our anti-terror laws, building on the growing body of academic and professional work describing and analyzing the whole body of our anti-terror legislation .

---

[8] Unlike some commentators who argue that existing criminal law provided adequate powers.
[9] George Williams*: A Decade of Australian Anti- Terror Laws.* Melbourne University Law Review Vol 35 http://www.mulr.com.au/issues/35_3/35_3_13.pdf pp1175
[10] Ibid p1176

NSWCCL will increasingly turn its energies to the support of such a national discussion and will seek alliances with those who share our broad concern that a major challenge of our era- to wisely balance the competing priorities of national security and democratic values – has not been managed well by our governments.

USA and UK recent experience provides some optimism that Governments can be persuaded to draw back from early legislative excesses in the so called 'war against terror' and find a more proportionate and less dangerous legislative regime.

Part 2 Comments on National Security Legislation Reform Proposals

NSWCCL accepts the need for national security legislation fit for the times and appropriately responsive to the dramatic advances in technology and the seemingly permanent threat of terrorist activity and espionage. However, we have major problems with many of the specific proposals and with the inadequacy of the arguments and evidence put forward to support these proposed reforms.

This submission only addresses some of the issues and proposals contained in the extended terms of reference and amplified in the accompanying Discussion Paper**:** Equipping Australia Against Emerging and Evolving Threats (the Paper).

There are other proposals and issues we would have like to comment on but pressure of time has precluded this. NSWCCL will seek to expand on this submission, if given the opportunity, at the PJCIS hearings.

5. The Discussion Paper

The provision of a discussion paper to expand on the reform proposals is good process. However, NSWCCL shares the widely expressed frustration with the lack of detail in relation to numbers of seemingly significant proposals. It is particularly strange that one of the most controversial of the proposals, albeit in the 'seeking views' category, – 'tailored data retention for up to 2 years for parts of a data set' - is not referenced at all in the Paper.

This lack of detail or precision makes it difficult, if not impossible to make sensible comment on many individual proposals or on the cumulative effect of the proposals.

For this reason, it is important that this response to the PJCIS is seen only as a preliminary input. Our concern at this lack of detail has been lessened by the recent indication by the Attorney General that the Government will not be responding to the PJCIS review quickly. It is our expectation that there will be a further stage of consultation and a formal review process with more detailed proposals and draft legislation in late 2012 or 2013.

A more disturbing aspect of the Paper is its overall failure to give serious guidance around issues to be analysed in responding to what has to be a central term of reference:

3) The Committee should have regard to whether the proposed responses :

a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector

The rhetoric is there but the substance necessary for a real and principled analysis of these important competing priorities is not. The willingness to cite administrative convenience as a sufficient reason for 'reforms' which extend intelligence agency powers, reduce rights and liberties and weaken accountability frameworks is one depressing manifestation of this. (See 7 below).

NSWCCL proposal: PJCIS should seek a commitment by Government to a further formal review process based on more detailed and justified proposals and draft legislation.

6. Protection of Human Rights

The terms of reference acknowledge that human rights protection will be a significant issue arising from these proposals to significantly reform national security laws. It is, therefore, surprising that the requirements of the Human Rights (Parliamentary Scrutiny) Act 2011 are not explicitly addressed in the Paper.

As it is clear that there will be considerable and widespread concern about the human rights implications of many of the proposals, it would seem appropriate for the Paper to have given a high priority to addressing the compatibility of the proposals with human rights.

NSWCCL proposal: The PJCIS review considers human rights compatibility issues of reform proposals in line with the requirements of the Parliamentary Scrutiny Act and urges the Government to address these compatibility issues formally in the next iteration of its proposed reform of the national security legislation .

7. Balancing privacy against Community Safety

The Paper opens its substantive discussion of the proposed changes to the Telecommunications (Interception and Access) Act 1979 (TIA Act) with the following:

> 'The primary objective of the current legislation governing access to communications is to protect the privacy of users of telecommunications services in Australia by prohibiting covert access to communications recept as authorised by the circumstances set out in the TIA Act.
>
> 'The exceptions to the general prohibition against interception recognise the need for national security and law enforcement agencies to access the information necessary to protect community safety and security. The limited focus of the exceptions reflects *Parliament's concern to balance the competing right of individuals to freely express their thoughts with the right of individuals to live in a society free from threat to personal safety*.'[11] (Emphasis added.)

There is no sign in the Paper of attempts to do any balancing of these rights. Nor is the restriction to matters threatening personal safety adhered to.

[11] Discussion Paper p. 12.

Balancing is not just a matter of averring that one right is more important than another. A sound process for decision making is outlined by Tom L. Beauchamp and James F. Childres:

> i. Better reasons can be given for acting on the overriding norm than on the infringed norm.
> ii. The moral objective justifying the infringement must have a realistic prospect of achievement.
> iii. The infringement is necessary in that no morally preferable alternative actions can be substituted.
> iv. The infringement must be the least possible infringement, commensurate with achieving the primary good of the action.
> v. The agent must seek to minimize any negative effects of the infringement.
> vi. The agent must act impartially in regard to all affected parties; that is, the agent's decision must not be influenced by morally irrelevant information about any party.

A decision, or a piece of legislation which deals with a conflict of basic principles or rights counts as balanced only if it meets these kinds of requirements.[12]

The Paper should demonstrate that each proposed change to legislation meets such conditions. They do not. There is no hint of recognition that all interception is intrusive, whether or not it is legalized.

For example, the Paper proposes that mere administrative convenience should override privacy considerations; it proposes extending the range of crimes covered to many which are do not affect personal safety; no concern is shown for the right of individuals to freely express their thoughts—nor for the possibilities of personal growth and the development of relationships for which privacy is essential. People need to be able to explore ideas, to express feelings—especially endearments—free from scrutiny. They should be able to do so without the risk of scorn and humiliation, of victimization, harassment or discrimination.

It is left to the JPCIS to determine whether the Government's proposals 'contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threats to national security and the security of the Australian private sector'

NSWCCL proposal: The JPCIS requires explicit explanation of what is intended as an appropriate safeguard for the protection of human rights and privacy and explicit demonstration of the need for any legislative change which impinges on privacy or other human rights before it is endorsed

[12] Tom L. Beauchamp and James F. Childres, **Principles of Biomedical Ethics**, Fifth Edition, Oxford University Press 2001

8. Expanding the range of crimes in relation to which warrants may be sought.

Under the TIA Act, law enforcement agencies are able to seek warrants for telecommunications interception to assist with the detection of serious offences, being offences carrying a seven years or more sentence. There are further criteria, excluding a number of offences. These restrictions are important protections of privacy. There is also a long list of other offences.

For stored communications warrants, however, the threshold is a serious contravention—an offence for which the penalty is three years' detention or a fine of 180 penalty units. There are no further restrictions to the kind of offence included.

Under the heading '*Reforming the lawful access regime*'[13], the Paper's authors propose that the threshold should be three years in each case. They argue that there are already a number of offences with three-year penalties are covered under the Act, and that consistency would reduce complexity in the interpretation of what is permitted.[14] It would appear that the full range of offences with maximum penalties of three years or more would be included.

The range of offences which carry three years' penalty is immense and the number of persons convicted of such crimes is large. For example, under the Criminal Code doing anything with the intention of dishonestly obtaining a gain from a Commonwealth entity:5yrs; causing a loss :5 years; giving a corrupting benefit:5 years. There are many more.

The threshold for a serious contravention includes offences under state laws. Here are some examples:

- Malicious damage to property Under section 195 of the NSW Crimes Act there is a five years' penalty for this offence, which includes graffiti. There are just under 10,000 charges for this kind of offence in the Local Court of NSW alone. (That excludes the Children's Court).
- Larceny (section 117 of the same Act) . This includes shoplifting. The maximum penalty is five years' imprisonment. There were 6,000 charges in 2011 in the NSW Local Court for this offence (excluding motor vehicle offences and the Childrens Court cases.) Three thousand of these were from retail premises.
- Assault occasioning actual bodily harm. The maximum penalty is five years' imprisonment. The offence includes anything more than causing momentary discomfort. There were over 10,000 charges for this kind of offence in the NSW Local Court in 2011.[15]

There are dozens of other examples. The list is likely to expand as the competition between political parties to appear tough on crime continues.

If privacy is going to mean anything, the definition would have to be altered, to exclude all but certain specified crimes. And it is likely that the exclusions would have to be added to as new crimes are

[13] Paper, p.23
[14] Paper, pp22-25.
[15] NSW Bureau of Crime Statistics and Research, Report, 2011.

invented or old ones have their penalties increased. There will be no gains of simplicity. But if there are no exclusions, the powers of interception will have no reasonable limits.

The idea is absurd. The threshold for all warrants should be raised to at least 7 years, and in the case of B-Party warrants and the proposed third party computer warrants for ASIO, the threshold should be higher.

In any case, reducing complexity is an administrative convenience, no more. And the inconvenience is slight. It is not very hard to check what is covered by the Act and what is not. A substantial extension of powers is proposed, with a great invasion of privacy, for a minor increase in convenience. Where is the balancing of competing principles here?

The Paper notes that when the penalties were determined for stored communications access, it was believed that since communicants have the opportunity to review or to delete communications before sending them, covert access was less privacy intrusive than real-time listening. Now however, because technology use and availability has changed, the argument, they say, is less compelling.[16]

What has changed is that people communicate a great deal more by emails and text messages, to the point where they carry out conversations by these means. Telephone conversations have not become more like emails. On the contrary, emails have become more like telephone conversations. This is, surely, is a reason for raising the threshold, not lowering it. The reasons for not engaging in interception unless life or safety are at risk remain as they were. Stored communications are now a kind of conversation, so the original reasons apply to them. If there is a case for logical consistency, it is for the threshold for stored communications access to be raised to seven years.

The Paper notes further that there are some offences that can only be investigated by interception or access, but which are excluded by the seven-year threshold.[17] The only reason for not listing these separately in the TIA Act is administrative convenience.

Section 17(1) of the International Covenant on Civil and Political Rights requires that no one 'should be subjected to arbitrary or unlawful interference with his privacy, family home or correspondence.' Because there is no sufficient reason for the changes proposed, lowering the threshold would be an arbitrary interference, disproportionate to the seriousness of the crimes solved or prevented, and so in breach of the Convention.

Indeed, the *present* data retention laws contravene international standards. The German Constitutional Court in March 2010 declared the German data retention laws unconstitutional, because of lack of proportionality in balancing right of privacy against interest in prosecuting crime. One of the aspects which the Court held was disproportional was that it applied to too wide a range of crimes, and should be permitted only for investigation of crimes of the most serious kind. The Court held that:

[16] Ibid. p. 24.
[17] Ibid. p. 24.

> The German legislator must implement stricter conditions to be attached to the use and storage of data, such as the use of separate data storage, encryption techniques, secured access e.g. by requiring dual authorisation for access and tamper-proof documentation of access and deletion of data; the access to the Telecom's data must serve tasks of paramount importance. Telecom's data may only be used for prosecution of crimes if suspicion of a severe criminal act exists, and may only be used for prevention of crimes if there is a concrete danger; and some data may not be retrieved by authorities at all (e.g. telephone calls made to anonymous telephone counselling services).[18]

NSWCCL proposal: The PJCIS opposes increasing the range of offences in connection with which telecommunications warrants are obtainable. Further, the PJCIS calls for the threshold to be raised to include only crimes that set life or safety at risk.

9. Reducing complexity by creating a single warrant under the TIA Act with multiple [telecommunication interception] powers. (Proposal 8a)

In increasing order of intrusion, the three kinds of warrant are the single service 'telecommunications service' warrant, the 'entry on premises' warrant and the 'named person' warrant. In accordance with the balancing principles outlined above, an applicant for a warrant should seek the least intrusive kind which will serve the purpose of the occasion, and the issuing authority should refuse an application for a more intrusive one when a less intrusive one is sufficient.

It is apparent from the annual reports under the TIA Act that in the heavy majority of cases a telecommunications service warrant has been sufficient. The distinction between the three kinds of warrant should be maintained. CCL sees no problem with a single application being made for more than one kind of warrant, provided the distinction is still made. However, the applications should specify and the judicial officer should have to determine still which kind of interception is warranted.

NSWCCL proposal: The PJCIS should advise that if it is to be possible for a single application to be made for more than one kind of warrant under the TIA Act, the distinction between warrants given should be maintained. The applications should specify and the judicial officer should have to determine still which kind of interception is warranted, with priority being given to what will involve the least invasion of privacy. There should be no diminishment of thresholds.

10. Single warrants under the ASIO Act.

Similar arguments apply to the proposal for single warrants under the ASIO Act. CCL seeds no problems with a single application which specifies which powers are being sought, with a warrant specifying which powers are given.

There is however considerable objection to arrangements under which every warrant gives all of the powers. It is essential that proper consideration is given, by ASIO and by the Attorney General, into

[18] http://www.linklaters.com/Publications/Publication1403Newsletter/20100317/Pages/Germany–ConstitutionalCourt.aspx, accessed 15.8.2012

which intrusions are justified by given circumstances—whether searches may be conducted, computers accessed, listening or tracking devices installed, or postal articles or packages for delivery opened—and which are not. Intrusions must be kept to the minimum necessary in the circumstances. This especially true of intelligence and security organisations, whose activities are secret and whose purpose requires that they have suspicions where others would not.

It is also important that the thresholds are not diminished by whatever process is adopted. Just as different penalties for offences reflect and emphasise the seriousness with which the offence should be viewed, so different thresholds for warrants reflect different degrees of gravity of what is to be undertaken. They have an educative as well as a protective function.

NSWCCL proposal: If it is to be possible for a single application to be made under the ASIO Act for obtaining more than one of the powers under that Act, the Attorney General should determine which powers are to be included in each case before granting the warrant. In order to maintain the educative function of the thresholds as well as their role in protecting privacy, different thresholds for different powers should be maintained.

11. Person search warrants.

ASIO is not, and must not be allowed to become, a secret police force. It must not be allowed to act as though it were adjunct to a police force. The proposal to allow it to conduct searches will permit, even encourage it to so act—especially given recent changes and further proposals to link it to the law enforcement agencies. This is a significant danger to Australian democracy.

Searching a person is not like seeking out facts hidden on a computer, listening to what a person does or watching what a person says. It is intrusive in all of these ways. But it is much worse. It can be confronting, humiliating, and if carried out repeatedly, debilitating. It intrudes upon the self—it is an attack upon the self.

It is also likely to involve physical conflict.

For these reasons, the power to search persons is restricted to members of law enforcement agencies, who are subject to conditions upon their powers to search persons—for example, wearing uniforms with identifying numbers, or carrying other identification which they are obliged to show. A person who is harassed by repeated searches or unjustifiable searches or is otherwise aggrieved can then know who was responsible and can find out to whom to complain.

CCL therefore is opposed to this proposal. If anybody is to search a person, it should be a police officer, with warrants obtained subject to the usual conditions.

If, in spite of these reasons, ASIO is given the power, or if police are asked to search on ASIO's behalf, the following problems need to be dealt with:

- A person being searched must have reason to accept it without engaging in physical resistance.

- Fishing expeditions are to be avoided.
- Political motives and prejudice must not influence the issuer of warrants.[19]
- Harassment by repeated searches must be prevented.
- It must be possible to lay complaints and have them dealt with properly.
- Searches must not be unreasonably intrusive.

The following therefore are requirements:

- Warrants should be issued by a judge, not by the Attorney General as at present.
- The grounds on which a warrant is obtainable should include that there is a reasonable suspicion that the person to be searched is in possession of material that is relevant to an offence.
- The person must be informed what agency is conducting the research, and how complaints are to be made. There must be some means identifying the agent to the agency (even if the person searched may not be told who the agent is).
- The warrant must only be valid for a short period of time—less than a week. (Otherwise the reasonable suspicion requirement could not possibly be met.)
- The search must not be unreasonably intrusive; so limited to the purposes for which the warrant is issued.

NSWCCL proposal: PJCIS should advise rejection of the proposal to allow ASIO to conduct person searches outside of the circumstances where they are permitted at present.

If the contrary view is taken by Government, then:

- Warrants should be issued by a judge, not by the Attorney General as at present.
- The grounds on which a warrant is obtainable should include that there is a reasonable suspicion that the person to be searched is in possession of material that is relevant to an offence.
- The person must be informed what agency is conducting the research, and how complaints are to be made. There must be some means identifying the agent to the agency (even if the person searched may not be told who the agent is).
- The warrant must only be valid for a short period of time—less than a week. (Otherwise the reasonable suspicion requirement could not possibly be met.)
- The search must not be unreasonably intrusive; so limited to the purposes for which the warrant is issued.

12. B-party warrants, and third party computers.

The government seeks the views of the PJCIS as to whether ASIO should be permitted to use third party computers and communications in transit to access a target computer.[20] It is not clear precisely

[19] ASIO has an unpleasant history of political bias and misjudgement as to its proper role.
[20] Term of reference 17(a) and Paper p.50.

what is envisaged here, but the Paper itself notes that there are privacy implications, such that appropriate standards and accountability mechanisms would have to be incorporated into such a scheme.

The privacy implications would appear to be similar to those involved in B-party interception under the TIA Act. CCL opposed the introduction of B-Party warrants; and argued that if they were to be made possible, they should be confined to offences that involved threat to life or the taking of life.[21] As we argued, it is not only those who are suspected of criminal activity whose privacy may be invaded in such cases, nor those who choose to communicate with them via a service that is tapped. A service may be tapped of anybody with whom it is thought they are in contact—their doctor, clergyman, lawyer, business partner, teacher, lover...persons who must keep confidences or they will be unable to perform their useful social roles. Every person who contacts the B parties has *their* privacy invaded too.

Though the original argument for B-party warrants was in terms of defences against potential terrorists, it was not long after their introduction that agencies were being encouraged to seek B-party warrants in relation to other crimes. Now the proposal for what might be called B-party computer warrants for ASIO is put in terms of the nation's security. But if the power is granted, it will not be long before it is used to in connection with other crimes. Indeed, given the cooperation that is being proposed between ASIO and other bodies, and if they are given the power to search persons ASIO will increasingly take the role of secret police.

NSWCCL proposal: PJCIS recommends against the introduction of warrants permitting access to third party computers and emails. If instead they are to be introduced, they should be restricted to situations involving a threat to life or where a life has been taken.

13. Protecting ASIO officers from criminal liability.

It is proposed that Director-General of Security should be authorised to issue certificates which will give ASIO officers and their sources immunity from criminal and civil liability for a specified period. This proposal is a. unnecessary, and b. the wrong response to a problem.

It is unnecessary, for the Commonwealth Director of Public Prosecutions is not likely to exercise his/her discretion whether to prosecute a person by deciding to prosecute that person for taking part in an undercover operation.

It is the wrong response, for the problem lies with the anti-terrorism law. ASIO employees are not going to be permitted to build and plant bombs. CCL has repeatedly objected to the breadth of the definition of 'terrorist act' under the Criminal Code, and does so again now. It criminalises and

---

[21] Senate Legal and Constitutional Affairs Committee, Hansard, March 15 2006, p. 79.

punishes severely actions which are well removed from genuine terrorist acts—amongst them, training a terrorist group.

It is also the wrong response because the experience of Australia's police forces in authorising criminal activity is that it creates a risk of corruption.

Should this power be given to the Director-General in spite of the above reasoning, restrictions should be placed on it parallel to the restrictions placed on 'major controlled operations' under the Crimes Act 1914 (Cmth.).

NSWCCL proposal: That PJCIS recommend against giving the Director-General of Security the authority to issue certificates giving immunity from civil and criminal libility to ASIO officers and their contacts.
If the contrary view is taken, restrictions should be placed on the warrants parallel to the restrictions placed on 'major controlled operations' under the Crimes Act 1914 (Cmth.)

14. Infringements to privacy by unfriendly persons.
The Paper shows some concern for the security of computer networks, not only on the ground that the nation's security may be at risk, or that the security of a network may be threatened by unfriendly action, but that the privacy of users may be affected, along with the risk of theft of their identities.

It is then curious that the Government is floating a proposal requiring Internet providers to retain data on all uses of their networks for up to two years.[22] Such data would have high commercial value to ordinary and criminal enterprises alike. Since it is unlikely that there is any encryption system in the world which is proof against determined hackers, presumably the data will have to be kept be kept off line. It will provide a temptation to corruption for all who have access.

CCL does not have access to information about corruption or infiltration of Australia's security and intelligence organisations.[23] We are aware, however, that every police system in Australia has had some problems of corruption over the last two decades and some of the other enforcement agencies also. There have also been problems of incompetence with two high profile cases by ASIO in the cases of Joseph Thomas and Izhar Ul-Haque.

The authors show no concerns about the invasion of privacy through *legal* interception or other forms of spying on what people are doing or saying. Yet the first item the Government says it wishes to progress is to strengthen the safeguards and privacy protection under the TIA Act. This is to include examination of the privacy protection objective, the proportionality tests for issuing warrants, mandatory record keeping standards and oversight arrangements by State and Commonwealth Ombudsmen.

[22] The Attorney General has since the publication of the Paper indicated some uncertainty as to the desirability of this proposal (15c) for reasons associated with both privacy and cost. Ref?
[23] It would be astounding if there were none.

The Government should follow the lead of the Queensland and Victorian State Governments, and provide a public interest monitor. (PIM). The other states and territory governments likewise should appoint such monitors. A PIM would be present at all applications for telecommunication warrants (or, preferably, for all warrants of any kind), with powers like those of the Queensland PIM, including the right to question applicants for warrants, and to argue an alternative case to the judicial officer who is asked to provide the warrant. The presence of a PIM would provide some assurance that warrants are not issued too easily, without proper concern for civil rights.

Applications for warrants should have to be heard by a judge, not by a member of the Administrative Appeals Tribunal. Informal reports and the huge numbers of warrants that are given each year combine to suggest that warrants are issued too easily. Judges moreover have tenure of appointment, and so are genuinely independent of government

A privacy objective should be introduced into the legislation, as the Government proposes. It should be made clear that the privacy objective limits the operations of government agencies as well as those of other persons. This will assist judicial authorities to be tougher in their scrutiny of warrant applications.

The PJCIS should consider whether its own access to information about Australia's security and intelligence services is adequate, and include and account of the limitations of its access in its report.

If providers are required to retain data for two years, safeguards should include logging all views of the data, by the providers as well as the agencies; demonstrated adequate encryption, security protections, certified destruction regimes so data older than 2 years were properly deleted, and at the very least, mandatory notification of any breaches of the data.

The authors give no examples of what agencies should be denied access to telecommunications information, as proposed in term of reference 2 A, except that those whose record shows they do not need them should have their powers of access stripped. (This of course is an invitation to the agencies to make as much use as they can between now and the drafting of legislation.) CCL notes that the TIA Act was introduced largely in order to enable agencies to attack drug crime.[24] But the "war on drugs" has been a failure, and not only costs lives due to overdoses and criminal activity, but raises the price of mind-altering drugs very substantially, providing profits to criminals and terrorist and extremist organisations, and has set at risk the governance of whole countries such as Columbia and Mexico. It is time that drug laws were changed, with addiction being treated as a medical problem and the possession of small quantities of any mind-altering drug decriminalized. When this is done, there will be less need for certain agencies to have access to telecommunications information.

We recognize that the increase in terrorism and in Australia's exposure to it as a result of involvement in the Iraq and Afghanistan wars in particular have created new reasons for legalising interception. It may be, however, that organisations whose principle raison d'être is the war on drugs will be able to be stripped of their interception powers.

[24] Paper, p. 15.

NSWCCL proposal: The JPCIS supports the view that the protection of the individual right to privacy is a central criterion for any amendments to the TIA Act and that deviation from this protection should only be on the basis of demonstrated, clear evidence of threat to personal safety or national security. Specifically the JPCIS should:

- support the proposed reduction in the number of agencies permitted to have access to telecommunications or telecommunication data
- increase or at least maintain the current thresholds
- consider the appointment of a public interest monitor to be present at applications for telecommunications warrants and have the power to question the applicant and argue an alternative case
- require applications for warrants to be heard by judges
- support the proposal to introduce a privacy objective into the TIA Act that captures the operations of government agencies and other persons
- reject the proposal to require data storage for up two years as an unwarranted erosion of individual privacy
- advise Government that if it nonetheless proceeds with the data storage proposal, strong safeguards must enforced including at least logging all views of the data, by the providers as well as the agencies; demonstrated adequate encryption, security protections, certified destruction regimes so data older than 2 years were properly deleted, and mandatory notification of any breaches of the data.

15. Record keeping standards and oversight.

The Paper addresses the issues of accountability by proposing the weakening of the record keeping standards, and thereby crippling the oversight by Commonwealth and State ombudsmen. While substantially increasing the powers of the agencies to invade the privacy of Australians, it proposes to hide from the public gaze how extensive the invasion of privacy is.

As the Paper notes[25], agencies are required to keep records about what warrants were sought and granted, and each time lawfully intercepted information is used, disclosed, communicated entered into evidence and destroyed. Reports are made to the Attorney General, and these are summarized in an annual report to the Parliament and the nation. These records are at present the only means by which Australian citizens may learn how extensive the use of interception powers is. They give rise to very proper suspicions about how easy it is to obtain warrants and to unfavourable comparisons with the regimes in other countries. It is not surprising if the agencies wish to remove their embarrassment.

This conclusion is supported by the extraordinary statement that:

> *'Many requirements reflect historical concerns about corruption and misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate'.* [26]

[25] P. 26.
[26] Ibid.

This is ludicrous. How are the oversight bodies to operate without this information? Given the increased opportunities for corruption it is proposed be created and the demonstrated readiness of some ASIO agents and police at senior levels to exceed their powers, how could such a claim possibly be made.

The claim also supposes that the Ombudsmen, the Inspector General of Intelligence and Security, the Attorney General or State ministers and the PJCIS are the only people who should know what the agencies are doing by way of telecommunications interception.

If there is some better way of ensuring that the public knows what it should—including the absolute numbers—by a different kind of record keeping and reporting, this needs to be put forward and discussed. In the absence of examples, it is hard to see that new forms of record keeping should displace rather than enhance the existing requirements.

Reports by the IGIS and the Ombudsman are not a substitute for this information, but an important supplement. And what other means is here to get an indication of how well those officials are doing their jobs?

NSWCCL proposal: PJCIS should advise against any changes to the record keeping of agencies which will weaken their accountability.

16. Other matters

Brief reference is made to several additional matters of concern.

Renewal of Warrants

The proposal is made that the Attorney General be able to renew warrants rather than issue fresh ones. Since the claim is made that this will reduce costs to administrative resources,[27] we assume that the intention is that a fresh case will not have to be made. But the criteria for issuing a warrant should not be circumvented by this means, nor should the proper checks be omitted.

Evidentiary Certificates

The proposal that evidentiary certificates be introduced to protect the identities and capabilities of ASIO involved in the execution of warrants under the ASIO Act in court proceedings might be acceptable for certificates in respect of computer access warrants, listening devices and tracking warrants, provided that: the certificates cannot be taken to prove the substantive elements of an offence; a judge can exclude the evidence if there is any reason to doubt the content of a certificate or if its inclusion would make a trial unfair.

But it would not be acceptable for certificates to be adopted in respect of search warrants of either kind, nor of those for inspection of postal or delivery items. And it would most certainly not be appropriate where questioning and detention warrants are involved.

Definition of a computer

[27] Paper, p. 42.

A proposal is made to amend the definition of 'computer' in the ASIO Act. (Proposal 5 a)
It is not clear how broad a network might be tapped on the authorisation of a single warrant. A University? A government department? In the absence of more information, it is impossible to evaluate this proposal.

NSW Council for Civil Liberties

21st August 2012

This submission was written by Dr Lesley Lynch and Dr Martin Bibby members of the Executive Committee of the NSWCCL .

NSW Council For Civil Liberties

The New South Wales Council for Civil Liberties (CCL) is committed to protecting and promoting civil liberties and human rights in Australia.

CCL is a Non-Government Organisation (NGO) in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

CCL was established in 1963 and is one of Australia's leading human rights and civil liberties organisations. Our aim is to secure the equal rights of everyone in Australia and oppose any abuse or excessive power by the State against its people.