Submission No 141

Inquiry into potential reforms of National Security Legislation

Organisation: Queensland Council for Civil Liberties

QUEENSLAND COUNCIL FOR CIVIL LIBERTIES
GPO Box 2281 Brisbane 4001
visit us at www.qccl.org.au

The Secretary
The Joint Committee on Intelligence and Security

pjcis@aph.gov.au

Dear Sir/Madam

Review of the Telecommunications Interception Powers

Thank you for the opportunity to make a submission on this important issue.

About QCCL
The Council for Civil Liberties is a purely voluntary organisation established in 1967 with the objective of implementing the Universal Declaration of Human Rights in Queensland and Australia. For the purposes of this submission we consider the following articles of the Declaration to be relevant:

1. **Article 9**
   No one shall be subjected to arbitrary arrest, detention or exile.

2. **Article 10**
   Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

3. **Article 12**
   No one shall be subjected to arbitrary interference of his privacy, family, home or correspondence...everyone has the right to protection of the law against such interference or attacks.

General Comments

Consultation
The Attorney General's paper says that the department has consulted "the telecommunications industry." There has been no consultation with this organisation. The Committee should instruct the Attorney General's Department to consult with a broad range of civil society organisations prior to taking this matter any further.

Public Report
It is not clear that the report of this Committee will be made available to the public. It is our submission that it should be. The grave interference with the basic rights of Australian citizens which is proposed in this paper should be the subject of intense public consultation and debate.

Sufficient Powers
In our submission this is an unjustifiable grab for power dressed up as a tidying up exercise. Since 9/11 there have been 45 pieces of legislation giving ASIO new powers many of which

it has never used.

Excessive Powers
The current legislation upholds the traditional but now irrelevant distinction between the content of a private communication such as in a telephone call or an e-mail and the associated telecommunications data by adopting a position that it is not necessary to obtain a warrant to have access to that data. The reality is that the telecommunications or traffic data creates an extensive digital trail from which can be created quite detailed portraits of an individual. In our view it is clear that this data should only be accessible via a warrant.[1] Thus ASIO is not required to obtain a warrant from a Judge for its interceptions is in clear violation of Article 12 of the Universal Declaration of Human Rights[2].

Public Interest Monitor
The Public Interest Monitor ("PIM") has existed in Queensland since it was introduced in 1996 by the then Liberal National party government. The PIM is designed to fill a gap in applications for warrants caused by the fact that under the traditional system the Judge only hears from the prosecution. The Public Interest Monitor is empowered to appear before the court on the hearing of listening devices and similar applications. This enables the Supreme Court or other Judge to hear arguments from both sides and then make a ruling. The Judges of the Supreme Court of Queensland have very much welcomed the involvement of the PIM. Any extension of the circumstances in which interception warrants and access warrants can issue should be accompanied by the introduction of a PIM at the Commonwealth level.

Notification Requirement
In its decision in the *R v Duarte* [1990] 1 S.C.R. 30 at 43 the Supreme Court of Canada established it as a constitutional requirement based on the Charter of Rights and Freedoms that notification must be given to the person whose communications have been intercepted in the case of an interception or access warrant.[3]. This is a vital mechanism because more often than not, particularly in a context of ASIO, access to private communications is carried out in secret. The requirement to notify those the subject of such an intrusion of their privacy would be a significant accountability mechanism.

In our view the law should require police and security agencies to notify all individuals whose personal information has been accessed within one year of the information being obtained unless the individual cannot be readily identified or notification would prejudice an ongoing investigation. Notification should be required within five years of the information being obtained unless it is determined that the public interest in nondisclosure outweighs the right to a notification.

Specific Issues
We have found it extremely difficult to identify from the discussion paper the exact proposals of the Attorney General. We set out below those which we have been able to identify with our comments.

1. *A change in the definition of serious offences from its current 7 years to 3 years imprisonment.*

---

[1] See *Rodrick "Accessing Telecommunications Data for National Security and Law Enforcement Purposes* [2009] U Monash LRS 15
[2] In this regard we note the decision of Keith J. in *United States of America v Warshack* - United States Court of Appeal for the Sixth Circuit delivered 14 December 2010
[3] See also *Queen v Six Accused Persons 2008* BCSC 212 at paragraph 214

This proposition is justified by arguing that there are certain offences which carry a term of three years which should be capable of being the subject of investigation by interception. It seems to us that this is an argument for increasing the penalty for those offences not for reducing the general level of criminality which justifies the issuing of a search warrant. We oppose this proposal as an unjustified extension of the powers to issue search warrants. We note that since the original *Telecommunications Interception Act of 1979* there has been a gradual but unmistakable increase in the circumstances in which these warrants can be used.

The latest *Telecommunications (Interception and Access) Act 1979* Annual Report shows that there were 3,488 telephone interception warrants issued in the period to 30 June 2011. In the calendar year 2011 there were 2,372 warrants issued in the United States of America. By the writer's calculation that means there were 17 more warrants issued per head of population in Australia than in the United States. We fail to see how this is justifiable. And yet the Attorney General seeks to broaden the types of offences in which warrants can be issued. Presumably this will result in a significant increase in the number of warrants.

2. *To extend the number of agencies which can have access to the information obtained under a warrant.*
Once again we oppose this proposal. Once again this is yet another step in the increasing level and number of persons and agencies having access to the data collected as a result of warrants. We see no justification for this.

3. *Reduced record keeping.*
Having noted that the current recordkeeping procedures reflect historical concerns about corruption and the abuse of covert powers, the Attorney General proposes to remove them as if there is no longer any prospect of corruption or misuse of covert powers. The proposal seems to be to give each agency the power to determine the best way to record and report on the information they have. This is entirely unacceptable and will lead to corruption and the misuse of power.

4. *Imposition of obligations on ISP's etc.*
We firstly note that this proposal contains a serious lack of detail. We would oppose any proposal to make Internet Service Providers build into their systems and networks the ability of law enforcement agencies to intercept and conduct surveillance. To require telecommunications systems to build their systems to meet technical standards that are designed to enable surveillance will make these private businesses agents of the state. This is inconsistent with a democratic society. Where is the evidence that this type of arrangement will actually assist in the fight against terrorism or organised crime?

5. *Extension of current arrangements to social networks and cloud computing*
Once again full details of what is proposed here are not contained in the discussion paper.

6. *Creation of a single telephone interception warrant.*
The Council has no objection in principle to such a proposal. However, we would like to see the detail of the proposal. It would be our view that the opportunity should be taken to strengthen the privacy protections by making it clear that telecommunication interception and access warrants are a last resort investigative

mechanism only to be issued when there is no real practical alternative.

Furthermore we note that the current regime inappropriately prescribes a lesser standard for a stored communications warrant . In fact, one would imagine that the state could obtain far more information out of stored electronic communications than out of those in transit. This is because e-mails typically say more personal data than phone calls. They often contain prior messages and an analysis may reveal the computer on which the e-mail is composed, what network it passed through, the times the e-mail was opened, deleted or forwarded. People often reveal their political religious or other beliefs in their emails in a way in which they would never have done over the telephone. Stored e-mails contain a vast archive of people's lives. The effect of this is that the same high standard should apply to both stored communication warrants and content warrants.

7. *Amend the legislation to impose an industry wide obligation on ISPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference.*
We query whether this is some attempt to shift costs onto the private sector. If a government wishes to conduct surveillance of its citizens it should pay the full cost of doing so. It should not be entitled to transfer that cost onto the private sector. It should not be entitled to turn every telecommunications or Internet provider into an agency of the State. Will there be some right of review in the Administrative Appeals Tribunal for example in relation to any directions which are made pursuant to this power?

8. *Definition of Computer*
The definition of computer is said not to cover connected servers. We have no objection to an amendment to cover this deficiency.

9. *Renewal of Warrants*
It is our view that warrants should only be renewed on showing of cause and the detailing of the interceptions made prior to the request such as to justify the need for the warrant to be renewed.

10. *Increase the duration of the warrant from 90 days to 6 months.*
We oppose this proposal. Investigations such as this proceed in secrecy and are rarely subject to public scrutiny. Innocent individuals are subject to a surreptitious invasion of their privacy and may never be in a position to learn about it let alone complain about it. For these reasons the time limit of the warrants and the conditions upon which they are renewed need to be tightly a prescribed. This is another reason why a notification procedure is required as discussed above.

11. *Authorising intelligence operations that the break the law.*
The QCCL strongly opposes the authorisation of illegal conduct by police or the security services. The purpose of the police is to suppress criminal activity, not to encourage or create it. There is in our view no justification for any instigation of any serious criminal conduct by the State.

This type of proposal violates two of the fundamental principles of our society: equality before the law and that we live by the rule of law and not the rule of men.

It violates the first principle by creating a group of superior citizens who are immune from and above the law. It violates the second principle by creating such broad immunities that it requires other citizens to place our trust in individuals rather than the system of law itself.

Whilst the QCCL is strenuously opposed to these proposals if they are to proceed then it is our view that a number of significant safeguards need to be in place.

Any exception from criminal liability must be carefully targeted to limited and specified circumstances. The immunity should not extend the beyond the agents to civilian participants in the operations

These operations must be the subject of judicial supervision. In other words, it should be a requirement that these operations can only be authorised by judicial officers. We have consistently opposed the giving of powers to the Administrative Appeals Tribunal to issue warrants since that Tribunal does not in our respectful submission have adequate independence.

Furthermore, the Commonwealth should appoint a Public Interest Monitor ("PIM") which is authorised to appear in relation to applications for warrants authorising controlled operations and to make submissions on the public interest. The PIM should also be authorised to review the conduct of those operations in a similar fashion to the Ombudsman.

12. *Power to add, delete or alter data on a computer.*
This proposal needs to be considerably more detailed before it can be the subject of comment.

13. *Change the law so that ASIO can get a warrant to search a specified person rather than premises.*
We echo the comments of the Law Council of Australia in their submission to the *Telecommunications (Interception and Access) Amendment Bill 2008* dated 12 March 2008.

14. *Give the Director General power to approve classes of persons to execute warrants.* On the face of it, this is not problematic as long as they are all appropriately trained.

15. *A regime where officers can use third party computers while communication is in transit to access a targets computer.*
This is a proposal which in our view has serious implications given the possibility of agents having access to the personal data of a totally innocent unrelated third party. Far more detail of this proposal would be required before it could be commented on any further. This would certainly want to be the subject of specific judicial authorisation and the person whose computer has been accessed would have to be notified.

16. *Evidentiary Certificates.*
The Council opposes this proposal. It is our view that the existing powers referred to in the discussion paper are more than adequate. In fact, those powers are excessive and impede proper access to justice.

17. *Proposals to facilitate cooperation and training together of ASIO and ASIS officers and to allow ASIO officers the power to carry weapons.*
Both these proposals seem to violate two fundamental principles. Firstly, separation of domestic and overseas intelligence agencies and secondly the historical objection to the creation of a secret police force. Throughout the whole period since September 11 there has been a clear drift towards turning ASIO into a secret police service. We are fundamentally opposed to that situation. In fact, it's quite clear that many of the measures proposed in the discussion paper serve simply to accelerate that trend.

Summary

The Council opposes the Attorney General's proposes except where they truly are technical or designed to tidy up the current law. We see no case for vast increases in the powers of ASIO.

Yours faithfully,

Michael Cope
President
For and on behalf the
Queensland Council for Civil Liberties
20 August 2012