

## **Introduction:**

This submission has been prepared at short notice and we note that our application to extend time for submissions was refused. It has not been possible to canvas all aspects of this proposed legislation but we make the following observations and are prepared to further discuss our views at a public hearing.

You cannot achieve absolute security in a democracy without substantially limiting people's rights. In the wake of the events of September 11 2001, we recognise that there are legitimate public fears about safety and security but it is imperative that we take time to consider the appropriate response. Our organisation is concerned that many of the measures proposed to address potential threats of terrorism have the capacity to be abused, and used by the government against Australian citizens while providing little tangible benefit in combating acts of terrorism and espionage. Instead of trying to act quickly in providing a response we should be taking time to be sure that our response is the correct one in the long term.

## **Definitions:**

This bill no longer limits acts of espionage to classified information but rather extends it to a wide variety of government held or controlled information. The result is therefore the extending of the reach of espionage offences into areas of dissemination of information which most of the community would not consider to be acts of espionage. It may easily be used against activists and whistleblowers to prevent or control their important role in society.

An area of great concern is the change of definition in this legislation from 'safety & defence' to 'security & defence'.

The widening of this definition means that it will now include in particular, the *operations and methods* of intelligence and security agencies. This could mean that exposure of an illegal action of a security agency or a security bungle could fall within the meaning of an act of espionage. There are many circumstances in which it is in the public interest to discuss the methods and operation of security agencies that will under this legislation become an offence liable to prosecution. We recommend that the definition remain as safety and defence and there be no change.

In particular this definition will now include security agencies of other countries. The exposure of operations and methods of activities of security agencies in other countries could become an offence. It is conceivable that members of a human rights watch organisation could be charged and convicted of an offence for publicising security operations of repressive

regimes in other countries or publicising human rights breaches by Australian authorities.

We recommend a general defence for whistleblowers and activists and those organisations. There is a need for clarification in the legislation so that an intention to publicise in the public interest does not amount to an act of delivering to another country or foreign organisation or disclosure within the meaning of subsections 2 and 4 of the proposed Division 91.1

As it is proposed the definition of information is so wide that information includes opinions and even reports of a conversation. A briefing of a Minister on information that is or later becomes public knowledge could fall within the definition of “information” as it is currently constructed.

### **Division 91.1 Offences relating to espionage and similar activities, subsection 2**

We are concerned that acts of “communicating or making available information that results in or is likely to result in making information available to other countries” will capture acts of whistle blowing. Unless it is more clearly defined, and a defence inserted, publication of information could also make it available to other countries. We recommend a whistle blowing defence, as recommended by the Gibbs committee, is inserted into the bill.

The intention of the provision seems to be to protect our allies from the disclosure of information that prejudices or compromises the operation of their security services by creating an offence of the disclosure of “information concerning the security or defence of another country... that has been in the possession or control of the commonwealth.”

Given the wide definition of information this could include ministerial briefings of many kinds to, for example, the defence or foreign minister and as the information is not limited to classified information could include information that is in the public domain in any event. The information does not have to be obtained from the Commonwealth; it is enough for it to be in its possession or control.

We believe that the wide definition will serve to make liable to prosecution, activities far beyond those envisaged or intended by the attorney general in his second reading speech. As the actual countries are not defined, if someone gave information about the security arrangements of North Korea to the United States, and that information was in the control or had been in the control of the commonwealth they could face prosecution under this section.

#### **Example A:**

The National League for Democracy in Burma has information concerning the operation of Burmese security forces and their intention to execute or

imprison pro democracy campaigners in that country. At the same time the Australian Foreign Minister has been briefed with this information. The national league for democracy, operating in Sydney passes the information to the U.S. Congress and the U.S. State Department so that it might take action against Burma. This could be a clear case of an offence under subsection 4 making the members of the National League for Democracy liable of an offence for which they could be imprisoned for 25 years.

Example B:

It is unclear what constitutes “lawful authority” as referred under the bill. This is absent from the definitions contained in the Bill and subjective in its nature.

ASIO agent X receives information about North Korea’s security arrangements, briefs the attorney general and in an act of goodwill and cooperation, passes the information to the United States. Agent X, if the Attorney General decides to prosecute, could be prosecuted for espionage under this provision. The only defence available to Agent X is that he had lawful authority – which is undefined and its meaning open to debate.

**Division 91.1 Offences relating to espionage and similar activities, subsection 4**

This section is so broad that virtually any information could be described in a way that it comes within paragraph (a) of subsection 4. The requirements of subsection (b) are very vague and do not clarify exactly what is meant by “an advantage to another country’s security and defence”. Presumably, any information of any type passed to another country, that is not already in the possession of that country could be argued to be providing an advantage to their security and defence. We recommend that there is a tighter definition of “information” and that there is a public interest defence for the actions of whistleblowers.

Example A:

The obtaining of the phone card records of the defence minister, information about excessive travel of MP’s, an memo or facsimile about the misuse of Australian helicopters in Papua New Guinea etc. with the intention to publicise that information could amount to an offence under this subsection.

Recommendation: A clear exemption is needed for people acting in the public interest in good faith. We recommend that there is a general defence for whistleblowers as recommended by the Gibbs inquiry.

## **Division 92.1 Offence relating to soundings**

The offence of sounding should provide that the burden of proof is on the prosecution. The section would affect a ship making soundings for safe passage or entry into a harbour if it then noted its soundings or communicated them to its head office overseas. The onus of proof is placed upon the persons taking the soundings to establish that they were taken for a purpose for which the vessel was "lawfully engaged".

It would appear that any sailor who may be a mere employee that takes a sounding at the request of the master of his ship and/or makes a record of it would have to prove his innocence under subsection 2. (b)

Otherwise he could be liable for imprisonment for 2 years for simply carrying out his duties as a sailor. This seems to be an extraordinarily heavy handed approach to any problem that might exist with the taking of soundings.

## **Division 93.2 Hearing in Camera etc.**

This division allows the court to suppress a trial under this legislation "if satisfied that it is in the interest of the security or defence of the Commonwealth". This provision is too wide ranging and allows a great scope to suppress matters that are often in the public interest.

In the past two years our organisation has assisted several people in relation to matters with similar provisions allowing matters to be suppressed in the interest of "the security or defence of the Commonwealth". In these cases the interpretation of this provision is applied so that a mere request is sufficient to exclude members of the public or suppress reporting of the events of the hearing. This type of provision has worked to reduce accountability of security organisations and cover up incompetence. We recommend that there be a much more stringent demonstration of the national security or defence implications of the matter and that the onus of proof is placed upon the organisation making the request.

It is conceivable that every matter involving espionage or related offences could be held to be in the 'interest' of the security or defence of the Commonwealth to suppress. This is the way that these matters are often decided in practice. A better approach would be for the applicant to have to demonstrate that a public hearing would damage the operation of the security or defence of the Commonwealth.

## **Conclusion:**

There may well be well be problems that need to be addressed with legislative changes but it is vital that there is clarity in the legislation. It is appropriate that we have a proper, public debate about the appropriate response to our security needs after the events of September 11 rather than simply making new laws that sound effective but are can be easily targeted against

whistleblowers instead of terrorists. In any attempt to prevent acts of espionage it is most important that we maintain a defence for people who are activists or whistleblowers, and are acting in the public interest. The legislation as it is currently constructed fails to provide adequate protection for whistleblowers and activists.

The legislation also seeks to reduce accountability by creating a system of secrecy in the prosecution of espionage offences. Any attempt to protect the national interest during a prosecution should be more than simply an unsubstantiated claim. Anyone claiming that a prosecution should be suppressed from public scrutiny should have to prove that it will damage national security or defence. It is our view that the national interest is better served by an open and public court process rather than one that is closed and secret, and based on dubious and unsubstantiated claims that it is in the Commonwealth interest to conduct it that way.

David Bernie and Cameron Murphy

New South Wales Council for Civil Liberties Inc.  
30<sup>th</sup> March 2002