6 August 2014

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Secretary,

The media organisations that are parties to this correspondence – AAP, ABC, APN, ASTRA, Bauer Media, Commercial Radio Australia, Fairfax Media, FreeTV, MEAA, News Corp Australia, SBS, and The West Australian – welcome the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security regarding the *National Security Amendment Bill (No.1) 2014* (the Bill).

The right to free speech, a free media and access to information are fundamental to Australia's modern democratic society, a society that prides itself on openness, responsibility and accountability.

However, unlike some comparable modern democracies, Australia has no laws enshrining these rights. In the United States of America the right to freedom of communication and freedom of the press are enshrined in the First Amendment of the Constitution and enacted by state and federal laws. In the United Kingdom, they are protected under section 12 of the *Human Rights Act 1998*.

In the absence of such clear protections, there are a number of keystones which are fundamental in Australia to ensure journalists are able to do their jobs. These include:

- The ability for journalists to go about their ordinary business and report in the public interest without the real risk of being jailed;
- Protection of confidential sources;
- Protection for whistle-blowers; and
- An appropriate balance of power between the judiciary, the executive, the legislature and the media.

Limits on the ability of journalists to report on matters of national security must always be carefully considered and minimised. A recent report by Human Rights Watch, regarding the US, notes that:

> *This situation has a direct effect on the public's ability to obtain important information about government activities, and on the ability of the media to serve as a check on government. Many journalists said it is taking them significantly longer to gather information (when they can get it at all), and they are ultimately able to publish fewer stories for public consumption. …[T]hese effects stand out most starkly in the case of reporting on the intelligence community, national security and law enforcement – all areas of legitimate – indeed, extremely important – public concern.*[1]

The media organisations that are parties to this submission do not seek to undermine Australia's national security, nor the safety of the men and women involved in intelligence and national security operations.

[1] Human Rights Watch in conjunction with the American Civil Liberties Union (2014) *With Liberty to Monitor All* at page 4; www hrw.com

Over many years there has been useful dialogue between security officials and producers and editors of media organisations that has led to considered outcomes. Journalists and editors have demonstrated over time that such matters can be approached in a reasoned and responsible manner. We hold that this approach should continue to be preferred over attempts to codify news reporting and criminalise journalists for doing their jobs.

We are concerned that the Bill has been characterised as being similar to the controlled operations regime in Part IAB of the *Crimes Act 1914* (the Crimes Act).[2] There are significant differences between the federal police controlled operation provisions and the new special intelligence operation provisions, particularly the significantly longer jail terms under the Bill. The existence of controlled operation provisions in the Crimes Act does not automatically justify the imposition of similar provisions in the context of special intelligence operations.

We are concerned that the Bill includes provisions that erode freedom of communication and freedom of the press. These concerns are set out in more detail below.

JAILING JOURNALISTS FOR DOING THEIR JOBS

The Bill includes proposed section 35P(1) to the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), which creates an offence for a person disclosing information relating to a special intelligence operation (SIO). A further offence is created (at proposed section 35P(2)) for a person who discloses such information with the intent to endanger the health of a person, or prejudice the conduct of the SIO, or where the information has that effect.

The insertion of proposed section 35P could potentially see journalists jailed for undertaking and discharging their legitimate role in a modern democratic society – reporting in the public interest. Such an approach is untenable, and must not be included in the legislation.

This alone is more than adequate reason to abandon the proposal as the proposed provision significantly curtails freedom of speech and reporting in the public interest.

This is particularly so as the proposed section 35P prohibits any disclosure of information relating to an SIO, not just reporting in the public interest.

In addition, SIOs by their very nature will be undisclosed. This uncertainty will expose journalists to an unacceptable level of risk and consequentially have a chilling effect on the reportage of all intelligence and national security material. A journalist or editor will simply have no way of knowing whether the matter they are reporting may or may not be related to an SIO. We express this as information that 'may or may not be' related to an SIO because:

- It may or may not be known if the information is related to intelligence operations, and whether or not that intelligence operation is an SIO;
- *'relates to'* is not defined and therefore the breadth of relevance is unknowable;
- It is unclear whether SIO status can be conferred on an operation retrospectively – i.e. if information has been 'disclosed,' whether any operation that it may be associated with or related to can be retrospectively allocated SIO status; and
- It is likely that clarity about any of these aspects would only come to light <u>after</u> information is disclosed – particularly in the case of reporting in the public interest.

[2] Explanatory Memorandum to the Bill, para. 463.

To illustrate, the discloser may not be aware that the information relates to an SIO, nor whether the information is core/key/central to an SIO, and even less aware as to where the boundaries may lie for information that may or may not 'relate to' an SIO.

So the discloser – who may be a journalist, doing what they are legitimately entitled to do as part of their job – could be jailed for disclosing information that is related to an SIO, even if they were not aware of it at the time, or it was not an SIO at the time of the report.

This uncertainty is intensified as the proposed criminal offence is based on the disclosure of information that relates to an SIO – regardless of to whom the disclosure was made. For example, a journalist who checks with his/her editor or producer regarding the information and/or the story could be jailed for responsibly doing their job, even if the information is not ultimately broadcast or published.

To illustrate this further, if the producer or editor disclosed the information to anyone in the course of making an editorial decision, then the source, the journalist and the editor could all be jailed. The conversations that are currently able to be had as media outlets make responsible decisions about disclosure in the public interest, would be denied under the proposed legislation, because any disclosure by anyone – to anyone – would be a criminal offence.

Further, the aggravated offence applies wherever the disclosed information has the effect of prejudicing the conduct of an SIO and does not require intent. This means that journalists may find themselves liable for a 10 year jail sentence when they had no idea that the information was the subject of an SIO, and the disclosure had an unintended consequence, unforeseeable to someone who was unaware of the SIO status.

It is also observed that it is the intelligence agency that determines an intelligence operation as an SIO, and would also determine the 'related' nature of the information to the SIO.

We reflect also on the Foreward of the Committee's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*[3] particularly the references to the Boston bombings and the murder of a British Soldier on the streets of London. These incidents are indeed concerning. If these incidents, or incidents such as these, were or became the subject to an SIO, then under the proposed amendments, journalists may be unable to report – including on incidents that may have been witnessed by a small or large number of members of the public, for fear of arrest.

In summary, the introduction of a serious criminal offence, punishable by jail, for journalists doing their job is strongly opposed. This in turn also has a chilling effect on freedom of speech and freedom of the media, hindering news gathering to the detriment of Australia's place amongst modern democracies.

LACK OF PROTECTION FOR WHISTLE-BLOWERS

The parties to this submission note that the insertion of section 35P to the ASIO Act also entrenches the currently inadequate protections for whistle-blowers regarding intelligence information. As a foundation of freedom of communication, we draw attention to this matter and highlight that it further erodes freedom of speech and freedom of the media in Australia.

---

3 http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm at *vii*

Specifically, proposed section 35P makes it a criminal offence punishable by jail, for anyone, including a whistle-blower, to disclose information that relates to an SIO.

The effect of proposed section 35P on potential whistle-blowers will be similar to those raised in relation to journalists, particularly - that a whistle-blower may or may not know if information relates to an SIO. This in turn would likely discourage whistle-blowing – particularly in the absence of protections, and would leave any whistle-blower facing the real risk of jail.

If a whistle-blower were to emerge from the ranks of intelligence personnel, then the Bill now imposes a 10 year jail sentence for disclosing information – up from 2 years – further discouraging whistle-blowing.

Notwithstanding the measures in the Bill, the other legislation that is designed to provide protections to whistle-blowers, the *Public Information Disclosure Act 2013* (PID Act), provides no protection to intelligence personnel if they make an external or public disclosure (sections 26 and 41). Media organisations and experts such as Professor A.J. Brown of Griffith University urged this to be changed when the PID Act was debated as a Bill in 2013. In our submissions to the House Standing Committee on Social Policy and Legal Affairs and the Senate Standing Committee on Legal and Constitutional Affairs on that matter, we said:

> *Again, there is no justification for a broad exclusion regarding disclosable conduct concerning intelligence agencies. There may well be instances where corruption or maladministration occurs in these agencies, the disclosure of which will not affect intelligence or security matters. These agencies, which are responsible for significant matters of public interest, should be subject to the same level of accountability as the rest of government.*

This Bill further impairs the lack of protection for persons, including intelligence agency personnel, driven to resort to whistle-blowing in the public domain. It is now unequivocal that the whistle-blower and the person/s who make the information public – most likely a journalist doing their job and reporting in the public interest – will face time in jail. Such an approach does not serve a free and open society and a modern democracy.

In addition to these two key issues, there are a number of consequences of the Bill which will have the potential to undermine a free media. These are:

UNDERMINING CONFIDENTIALITY OF SOURCES

i. Expanding definition of computer to include networks
The Bill expands the definition of computer under the ASIO Act to extend to 'computer networks' as it applies to search warrants, computer access warrants, identified person warrants and foreign intelligence warrants. We have serious concerns that this could expose the computer networks of media organisations to monitoring, and therefore undermine confidentiality of journalists' sources and therefore news gathering.

ii. Enabling access to third party computers
The current section 25(5)(a) of the ASIO Act provides the power under a search warrant to add, delete, or alter other data (that is not relevant to the security matter) to obtain access to data that is relevant to the security matter. This is being amended to also include the power to copy.

Additionally, the ASIO Act will also be amended (sections 25(6) and 25A(5)) to enable the use of third party computers or 'communication in transit' for the purpose of access data on the target computer.

These amendments, in combination with the extension of the definition of computer to computer network, and the ability to add, delete, alter, and now copy data that is not relevant to the security matter (albeit for the purpose of accessing data that is relevant to the security matter and the target) amplifies the risks to the fundamental building blocks of journalism including undermining confidentiality of sources and therefore news gathering.

EXPANDING THOSE WHO CAN EXECUTE WARRANTS, WARRANTS FOR ACCESS TO THIRD PARTY PREMISES AND USE OF REASONABLE FORCE

The Bill amends sections of the ASIO Act to:

- Authorise a class of persons able to execute warrants rather than listing individuals (section 24);
- Clarify that search warrants, computer access warrants and surveillance device warrants authorise access to third party premises to execute a warrant (sections 25, 25A and new section 26B); and
- Authorise the use of reasonable force at any time during the execution of a warrant, not just on entry (sections 25, 25A, 26A, 26B and 27J).

The expansions of these aspects of the ASIO Act, in aggregate, and in addition to matters raised previously in this submission, are of major concern. These amendments increase the risk to all that media organisations encompass, including all employees, information and intellectual property which in turn curtails freedom of speech.

We urge the Parliament to consider this impact of the proposed amendments before proceeding with the Bill.