SEVEN WEST MEDIA

22 May 2015

The Hon Roger Gyles QC
Independent National Security Legislation Monitor
Department of the Prime Minister and Cabinet
1 National Circuit
Barton ACT 2600

Dear Mr Gyles

Thank you for the opportunity to appear before you at the public hearings on section 35P of the ASIO Act.

Seven has been asked to provide supplementary comments on a number of issues, which are set out below.

1. ALRC Recommendations in Report 112 (Secrecy Laws and Open Government in Australia)

Section 35P(1) (as distinct from s 35P(2)) makes it an offence to disclose information related to an SIO without any requirement that the disclosure causes harm or that the person disclosing the information intends to cause harm.

AGD/ASIO explain the policy rationale for this as follows in their submission to the INSLM (p.10):

> *"the very disclosure of the existence and conduct of an SIO creates an unacceptable risk that the operation may be compromised, and that the safety of the participants (and potentially their family or associates) may be jeopardised".*

AGD/ASIO go on to suggest that support for this policy rationale is found in the ALRC *Report on Secrecy Laws and Open Government in Australia* (2009) and the 1976 and 1984 Reports of the Hope Royal Commission on Intelligence and Security (p.11). They later call this a *"body of opinion arising from independent reviews"* (p.29).

In particular, AGD/ASIO submit that

> *"The ALRC concluded that secrecy offences in respect of intelligence-related information did not need to include an element requiring proof of harm or intent to cause harm in making a disclosure, on the basis that the harm is implicit"* (p.11 and fn 11; see also p.25 and p.29).

In our view, the full context of the ALRC Report does not support this approach to s 35P.

Seven West Media Limited, ABN 91 053 480 845
38-42 Pirrama Road, Pyrmont NSW 2009 Australia, Postal Address: PO Box 777, Pyrmont NSW 2009 Australia
T +61 2 8777 7777 **F** +61 2 8777 7180

Section 35P criminalises disclosures ***by any person***. The ALRC Report, in the respect identified by AGD/ASIO, was dealing expressly with offences for disclosure ***by intelligence officers***:

> [8.62] *The ALRC considers that a prohibition on the disclosure of information obtained or generated by intelligence agencies is justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies. The existing [Australian Intelligence Community (**AIC**)] secrecy offences cover a limited range of people who handle intelligence information, namely officers and employees, and people with whom the agency has an agreement or arrangement. The ALRC considers that it is appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive intelligence information.*
>
> ...
>
> [8.65] *... the ALRC accepts that specific secrecy offences covering the disclosure of information obtained or generated by or on behalf of the AIC by officers in AIC agencies, or people subject to an agreement or arrangement with the AIC, do not necessarily need an express requirement of harm ...*

When the ALRC considered different secrecy provisions (applicable to law enforcement agencies) which reached ***all*** persons, it was prepared to accept offence provisions that were ***narrowly tailored***. With reference to examples in the *Witness Protection Act 1994* (Cth) and the *Crimes Act 1914* (Cth), the ALRC said:

> [8.76] *... While these offences cover disclosures by 'any person', they are limited to particular information the disclosure of which causes, or is likely to cause, harm.*

These aspects of the ALRC's consideration ultimately found expression in Recommendation 8–2:

> *Specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused or was likely or intended to cause, harm to an identified essential public interest, except where:*
>
> *(a) the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit; or*
>
> *(b) the harm is to the relationship of trust between individuals and the Australian government integral to the regulatory functions of government.*

Section 35P(1) is a specific secrecy offence. It lacks any element of harm to an identified essential public interest. And yet it does not fall within either of the exceptions that the ALRC considered appropriate. It is not narrowly tailored to particular information (such as identifying persons or methods), but rather sweeps up all information that 'relates to' an SIO, which is extraordinarily broad in its reach. Equally, it is not confined to disclosure by

intelligence officers, but rather sweeps up 'any person'. It is the *combination* of those two broad-reaching mechanisms that takes s 35P beyond what the ALRC considered appropriate.

Put another way: if one takes the ALRC report as the point of reference, as the AGD/ASIO submission seeks to do, then if s 35P(1) is not to include a 'harm' requirement, it should apply only to disclosures by intelligence officers, employees or others with whom ASIO has an agreement or arrangement; or it should be narrowly tailored to specific information about identities of undercover officers and intelligence methods. Alternatively, if s 35P is not to be limited to intelligence officers and is not to be limited to specific information, then it should include a 'harm requirement'.

This point carries through to AGD/ASIO comments on stakeholder suggestions. At p.23, AGD/ASIO say that "*[i]t is appropriate that all members of the community are expected to adhere to non-disclosure obligations, which should apply equally to all persons*". The difficulty with that submission is that not all persons stand in the same relationship to information that 'relates to' an SIO. Plainly enough, intelligence officers (and certain others) have greater access to that information and should have greater responsibilities in respect of its non-disclosure. As the ALRC noted in its report:

> [9.129] ... *officers in the AIC should know that the information they handle is inherently sensitive, and that any disclosure has the potential to harm national security ... However, a person outside the AIC cannot be expected to have a similar level of knowledge or responsibility.*

Indeed, journalists and others who do not have a relationship with ASIO are, in practice, likely to be caught by s 35P by making a *subsequent* disclosure of information that relates to an SIO. That is to say, it is difficult to see how a journalist could be in possession of information relating to an SIO unless it had already been disclosed. It is instructive, therefore, to observe what the ALRC recommended in relation to such *subsequent* disclosures (Recommendation 9–7):

> *Offences for the subsequent unauthorised disclosure of information should require that:*
>
> *(a) the information has been disclosed in breach of a specific secrecy offence;*
>
> *(b) the person knows, or is reckless as to whether, the information has been disclosed in breach of a specific secrecy offence; and*
>
> *(c) the person knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—a specified essential public interest.*

This recommendation was specifically informed by the ALRC's view that subsequent disclosure offences '*impact adversely on freedom of expression*' and '*could unreasonably*

curtail the media's ability to discuss matters of public interest' and therefore requires '*several safeguards*':

> [9.127] ... *subsequent disclosure offences have the potential to impact adversely on freedom of expression and could unreasonably curtail the media's ability to discuss matters of public interest. In order to avoid placing a disproportionate restriction on freedom of expression, the ALRC considers that, where a criminal offence regulates disclosure by a third party who has received Commonwealth information by way of unlawful disclosure, several safeguards should be put in place.*

Section 35P criminalises subsequent unauthorised disclosure by journalists of information that relates to an SIO without *any* of the safeguard elements, in particular any 'harm requirement', that the ALRC recommended.

AGD/ASIO also say (at p.23) that the absence of exemptions for journalists is "*consistent with the policy intention that the offences are directed to the risks posed to security as a result of the disclosure ... irrespective of the motives or identity of the discloser*". That, it might be said, is to ignore that the information covered by s 35P is very broadly cast as information that 'relates to' an SIO, rather than information that might actually cause harm.

In summary, the ALRC Report that AGD/ASIO rely on does not provide support for the breadth of s 35P. If anything, the ALRC report suggests that consideration might be given to confining s 35P to disclosures by intelligence officers or persons who have entered an arrangement or agreement with ASIO.

Seven strongly supports the concept of a defence for reporting on matters of public interest.

2. Any comments on the chilling effect of disclosure offences applying to controlled operations by the AFP and law enforcement agencies

AGD/ASIO repeat what the Attorney-General said in the second reading speech to the effect that the absence of any prosecutions since the enactment of ss 15HK and 15HL of the Crimes Act indicates that those offences "*are not operating as an undue limitation on reporting of national security matters and that section 35P is not likely to operate as such a limitation*" (p.15).

This reasoning is somewhat elusive. An absence of prosecutions indicates, if anything, an absence of disclosures, which is precisely what one would expect to be the consequence of criminalising those disclosures. The absence of prosecutions says nothing about what matters are *not* being reported. The difficulty of assessing empirically what matters are *not* being reported is part of the chilling effect of, and vice in, broadly framed criminal prohibitions of this kind.

3. The distinction between section 35P and the more limited disclosure offences applying to ASIO's questioning and detention warrants (section 34ZS of the ASIO Act)

In the alternative to limiting s 35P to disclosures by intelligence officers, Seven welcomes consideration being given to harmonising s 35P with s 34ZS to the extent that limits can be placed on:

- the type of information that cannot be disclosed; and
- the time period in which disclosure is prohibited,

In particular, AGD/ASIO's suggestion that s 35P might be limited to disclosure of the "existence of an SIO, or the content of an SIO authority ... or the conduct of an SIO in accordance with an authority" (p.31) would be a meaningful improvement of the current provision's broad prohibition on disclosing information that simply 'relates to' an SIO. Seven would not, however, support a simple copying of the language of 'operational information' that appears in s 34ZS. 'Operational information' suffers from the same problems of breadth and vagueness as 'relates to'.

In relation to limiting the time period in which disclosure is prohibited, Seven agrees that an SIO may be "directed to collecting intelligence ... over a sustained period of time" and that this distinguishes it from a warrant of the kind dealt with in s 34ZS (p.32). Although an SIO may run for a longer period of time than a s 34ZS warrant (although never more than 12 months unless renewed), the question of how much longer *after cessation* of the SIO/warrant disclosure should be prohibited is not obviously different for s 35P than for s 34ZS. At present there is *no* time limit under s 35P and that is inconsistent with the position under s 34ZS.

An appropriate time limit under s 35P will depend upon the nature of the information. For example, identifying the mere existence of an SIO and perhaps its general subject matter could well become benign shortly after the SIO has ceased and served its authorised purpose. On the other hand, revealing the identity of an officer, or the particular covert techniques used in an SIO could well cause harm long after the SIO ceased. This only serves to highlight the fact that the broad reach of s 35P, which does not differentiate between different kinds of information, or direct itself to disclosures causing harm, is inappropriate. It is difficult to make a meaningful submission about an appropriate time limit when the provision itself is so broad. Nonetheless, Seven submits that there should be *some* time limit, consistent with the approach taken in s 34ZS.

Thank you again for the opportunity to provide you with these further comments.

Yours sincerely

Bridget Fair
Group Chief – Corporate and Regulatory Affairs