DR MATT COLLINS QC

List A Barristers
205 William Street
Melbourne Victoria 3000

E matt.collins@vicbar.com.au
T +61 3 9225 7780
F +61 3 9225 8646

The Hon Roger Gyles AO QC
Acting Independent National Security Legislation Monitor
PO Box 6500
Canberra ACT 2600

14 April 2015

Dear Mr Gyles

Inquiry into section 35P of the ASIO Act

I welcome the opportunity to make a submission in relation to the potential impact upon journalists of section 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**).

Special intelligence operations (**SIOs**) are authorised under Division 4 of Part III of the ASIO Act by the Attorney-General without any judicial or other oversight.[1] The Attorney-General may authorise participants in SIOs to engage in certain criminal and other unlawful conduct[2] in circumstances where they enjoy a broad legislative immunity from civil or criminal liability.[3]

There is an inherent risk of abuse of power in connection with the authorisation and execution of SIOs, because of their covert nature and the exceptional character of the powers authorised by Division 4 of Part III of the ASIO Act.

Section 35P of the ASIO Act, which criminalises the disclosure of information in relation to SIOs, is capable of applying to journalists and media organisations, who are in the business of imparting information to the Australian community. It also has potential application to those who provide information to journalists, such as whistleblowers and other confidential sources.

The media plays a vital role in holding those in power to account, by exposing alleged malfeasance to the glare of public scrutiny. Mere knowledge of the risk that malfeasance might be publicly exposed tends to act as a curb on potential abuses of power.[4]

---

[1] Section 35C.
[2] Section 35C(2)(c), (e).
[3] Section 35K.
[4] cf *Russell v Russell* (1976) 134 CLR 495, 520 (Gibbs J): without being 'fully exposed to public and professional scrutiny and criticism … abuses may flourish undetected.'

Legislation that criminalises the disclosure of information, even where that information reveals malfeasance, thus warrants the closest scrutiny.

Against that backdrop, I have three principal concerns in relation to the potential operation of section 35P.

First, section 35P is likely to have a chilling impact upon freedom of expression and of the press that goes well beyond its intended scope. In the absence of confirmation from ASIO itself, there is no way for any journalist or media organisation to know with any degree of assurance whether information coming into their possession concerns an SIO. The risk of inadvertently disclosing information concerning an SIO is thus significant, and responsible media organisations will necessarily be conscious of that risk. Although the fault element for an unintentional breach of section 35P is recklessness, that threshold may not provide much practical protection to journalists and media organisations.

A 'hotline' has been established, which journalists are supposed to call if they come into possession of information that may relate to an SIO. A journalist who published information suggestive of an SIO without first calling the hotline would, presumably, be likely to have acted recklessly. Equally, however, journalists consulting the hotline will be exposed if there is (as might be expected to be the default position from those staffing the hotline) a refusal either to confirm or deny that particular information relates to an SIO. A journalist who went on to publish information, having received a non-committal response from the hotline might also, depending on the circumstances, be said to have acted recklessly.

A good deal of information that could be disclosed without breaching section 35P, and that ought to be disclosed in the interests of keeping the public informed of matters of legitimate interest, may thus never see the light of day, because journalists and media organisations will self-censor out of fear that the information might relate to an SIO. That risk could be mitigated by those staffing the hotline being given clear guidelines requiring them to provide positive confirmation to journalists and media organisations as to whether particular information does, or does not, relate to an SIO.[5]

[5] Providing that information would, presumably, not itself be a breach of s35P: see s35P(3)(d).

Secondly, there is no time limit attached to the offence in section 35P(1). As a consequence, a journalist or media organisation could commit an offence, carrying a 5 year prison term, by disclosing information relating to an SIO even months or years after the SIO had run its course, expired or been cancelled.

There may be good reason, in some cases, why information concerning stale SIOs ought not to be disclosed, but the legislation provides no mechanism by which information concerning past SIOs can ever be disclosed, whatever the circumstances.

It would be preferable if the offence in section 35P applied only to active SIOs, unless the Attorney-General certified in respect of a particular SIO that he or she was satisfied that continued secrecy was necessary to protect the health or safety of a person or so as not to prejudice the effective conduct of other SIOs.

Thirdly, section 35P does not provide any protection to journalists, media organisations or others who disclose information relating to SIOs, even where the disclosure has not compromised an SIO and is manifestly in the public interest because, for example, it reveals serious malfeasance in connection with their authorisation or execution.

It is true that information concerning alleged wrongdoing in connection with SIOs could be disclosed to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers or performing functions or duties under the *Inspector-General of Intelligence and Security Act 1986* (Cth).[6] There may, however, be good reasons why those with relevant information would not wish to provide it to IGIS officials; and in any event, public confidence in the integrity of processes ultimately depends on transparency and accountability.

While the formulation of a public interest defence would no doubt present difficulties, the absence of any such form of defence means that there is a real risk that, if serious wrongdoing were ever to occur in connection with the authorisation or execution of an SIO, those responsible may be practically unaccountable for their actions.

[6] Section 35P(3)(f).

Thank you for the opportunity to provide this submission.

Yours faithfully

M J Collins QC