

From: Keiran Hardy
Sent: Friday, 1 May 2015 3:58 PM
To: INSLM Submissions
Cc: George Williams
Subject: RE: INSLM section 35P inquiry - follow up from today's public hearing

Dear Christina,

I have reviewed the examples from the UK and US suggested by the Acting INSLM, and we can add the following:

- Part II of the *Regulation of Investigatory Powers Act 2000* (UK) provides for the authorisation of surveillance by public authorities, including through covert human intelligence sources. However, those sections are not comparable to the SIO regime in that they do not allow officers of the intelligence services and other public authorities to engage in unlawful activity (except in the sense that intrusive surveillance measures would be unlawful if not authorised by statute). There is also no offence for disclosing information relating to that surveillance. Part II of RIPA is therefore akin to ASIO's other statutory powers (in both the ASIO Act and the Telecommunications (Interception and Access) Act 1979 (Cth)) for conducting surveillance through the interceptions of communications, planting of tracking devices and the like. The SIO regime goes beyond these typical intelligence powers by authorising potentially any unlawful conduct (except for conduct which would fall within one of the listed exceptions, such as acts causing death, or those amounting to torture or a sexual offence).
- The Attorney-General's Guidelines Regarding the Use of FBI Confidential Human Sources do provide for the authorisation of illegal activity by human sources relied upon by the FBI. However, those guidelines set a higher threshold for authorising illegal activity: such authorisations can only be made where 'essential for the success of an investigation' OR are necessary to prevent death, serious bodily injury or property damage AND the benefits of the operation outweigh the risks (p 32). By contrast, an SIO may be authorised where doing so will 'assist the Organisation in the performance of one or more special intelligence functions (special intelligence functions defined as ASIO's intelligence gathering and analysis functions under s 17). A confidential human source also cannot be authorised to participate in any act of violence or an act that would be unlawful for an FBI officer to perform (p 30), whereas the SIO regime can authorise any unlawful activity (save conduct falling under the relevant exceptions). The higher standards in the FBI guidelines are justifiable in part because they are referring to illegal acts by confidential human sources and not officers of the FBI. However, the FBI's law enforcement functions, and the relevance of these guidelines to criminal investigations, mean that the guidelines are not in any case directly comparable to ASIO's situation.

The closest comparator to the SIO regime is that currently being debated by the Canadian Parliament (Bill C-51). If enacted, that regime will give agents of the Canadian Security Intelligence Service (CSIS) special powers to 'reduce' threats to security. The examples of powers to be authorised include entering premises, seizing things and installing devices – these appear similar to ASIO's ordinary statutory powers to conduct surveillance, although the focus on 'reducing' threats to security suggests that the activities by CSIS agents would be designed to disrupt terrorist activity (rather than collect intelligence). In this sense, the CSIS regime would appear to have a similar operation to SIOs. However, CSIS will be required to seek judicial authorisation for such acts (in contrast to the ministerial warrants for SIOs), and there is no disclosure offence attaching to the regime.

I hope that is of some help, and please let us know if you have any further questions.

Kind regards,

Keiran