Submission No 142

Inquiry into potential reforms of National Security Legislation

Organisation: Castan Centre for Human Rights Law

Castan Centre for Human Rights Law
Monash University
Melbourne

Submission to the Parliamentary Joint Committee on Intelligence and Security

Inquiry into potential reforms of National Security Legislation

Prepared by Dr Patrick Emerton

This submission addresses a number of the matters raised in the inquiry Terms of Reference and the associated Discussion Paper (DP).

1. Telecommunications Interception

1.1 Privacy and proportionality

The Discussion Paper observes that "Telecommunications data is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest" (p 14). This is undoubtedly true. However, on its own it shows only that telecommunications interception is a useful investigative tool. It does not resolve the question of the extent to which agencies should be permitted to intercept communications. This submission therefore supports the emphasis placed on the need for the telecommunications interception regime to ensure proper respect for the privacy of telecommunications (DP p 23). This submission would support the introduction of a privacy-focused objects clause (DP p 23), but would also strongly urge that the protection of the privacy of those whose communications may be intercepted remain the first-mentioned consideration to which regard must be given prior to the issuing of a warrant, as is currently the case.[1]

The Discussion Paper canvasses the standardisation of the threshold for the issuing of warrants (p 24). As it points out, the policy rationale behind the inclusion of particular offences within the scope of the warrant regime is not always clear (DP p 24). The risk of standardisation, however, is a reduction of the threshold requirements for warrants to the lowest existing threshold (namely, those "serious contraventions"[2] that trigger the availability of a stored communications warrant). Although the current approach is perhaps more ad hoc, it is arguable that it also provides a greater limit on the issuing of interception warrants, and thereby helps to preserve a balance in favour of the privacy of telecommunications.

The Terms of Reference raise the possibility of a single warrant with multiple interception powers (item 8). This submission does not support such a proposal to the extent that it would permit a wider range of interceptions to be undertaken on the

[1] *Telecommunications (Interception and Access) Act 1979* ss 46, 46A, 116.
[2] Ibid s 5E.

basis of a single warrant. The current warrant provisions, for example, impose a higher threshold for issue when the basis for interception is that the person whose communication is being intercepted is not a person of interest, but is likely to communicate with such a person, or where the warrant applies to a range of services and/or devices by means of which a particular named person may communicate.[3]

This higher threshold for those forms of interception serves the interests of privacy. Although the Discussion Paper notes that, in the contemporary era, persons of interest are apt to use multiple services or devices, either out of convenience or in order to evade interception (pp 17–21), it also needs to be recognised that many devices (eg shared computers or shared portable devices) may be used by multiple persons, not all of whom are of interest in an investigation. Different forms of interception therefore seem to warrant different thresholds for the issuing of a warrant – as is currently the case – in order to reflect these differing privacy concerns.

The Discussion Paper also contains the suggestion, however, that a simplified warrant regime might be able to *enhance* the protection of privacy by focusing on the identifying characteristics of communications, enabling those of interest to be more easily isolated (p 25). That would seem to be a desirable way in which to develop the current "named person warrant" regime, but without more detail as to the way in which privacy would be guaranteed, it is not clear that it would warrant lowering the threshold for the issue of named person warrants to that of traditional service interception warrants.

The Discussion Paper raises the prospect of extending the interception regime to cover a wider range of information technology service providers (DP p 27). Such extensions have obvious privacy implications. As ordinary citizens increase their reliance upon such services to undertake everyday activities (for example, the storing of photographs or other data) that might in an earlier time not have fallen within the scope of telecommunications, the capacity of telecommunications interception to intrude upon privacy previously taken for granted increases. The

[3] Ibid ss 46(3), 46A(3).

Discussion Paper notes that the rationale for a lower threshold for stored communication warrants was that "communicants often have the opportunity to review or to delete these communications before sending them, meaning covert access can be less privacy intrusive than real-time listening" (p 24). However, as it goes on to note, "this logic, while valid several years ago, has become less compelling as technology use and availability has changed" (DP p 24). This suggests that any extension of the scope of the warrant regime should be based at least on the higher thresholds of the other forms of warrant. In addition, where access to communications – such as social networking – is likely to reveal the communications of those persons who are not of interest, the higher thresholds currently imposed on the issue of B-party warrants.[4]

Similar concerns apply to the suggestion that the industry be obliged to retain information for up to a 2 year period (Terms of Reference item 15c; DP p 28) and to assist agencies in decryption (Terms of Reference item 15a; DP p 28). It is no doubt true that this "would greatly enhance agencies' abilities to detect and disrupt criminal and other behaviours" (DP p 28), but that leaves issues of privacy unaccounted for. The long-term storage of sensitive data by private telecommunications providers, for example, in circumstances where those providers are expected to have the capacity to participate in decrypting that data, has the potential to create new risks of breaches of privacy which any regulatory framework would need to carefully address.

1.2 Agencies and accountability

This submission does not express a view on whether the range of agencies with access to telecommunications interception powers should be reduced. It does not that any improvement in privacy protection achieved via such means might be undone by increase facilitation of data-sharing across agencies (as canvassed at DP p 25).

What is important is accountability of those agencies for their interception activities. This submission would welcome any new proposals to increase such accountability

[4] Ibid s 46(3).

(DP p 26), but would object to any dilution of the current reporting and record-keeping requirements (as canvassed at DP p 26). If the inspection of records is proving overly burdensome for the Ombudsman (as suggested at DP p 26) the obligation on the Ombudsman to perform inspections could be amended to a *permission* to inspect within a broader statement of oversight obligations, without reducing the requirements of agencies themselves to maintain records and make them available when required.

2. Intelligence Agencies

2.1 Variation, duration and renewal of ASIO warrants

This submission does not support the proposals relating to the variation, duration and renewal of ASIO warrants. Surveillance by a covert intelligence organisation is one of the most intrusive violations of privacy in which a government can engage, particularly where its own citizens are concerned, and any steps that would potentially reduce the oversight and accountability of surveillance operations increases the risk that such surveillance poses to the proper relationship, in a pluralist democracy, between a government and its people. A modest additional administrative burden is a small price to pay in return for avoiding any implication, for example, that certain person are, by default, subject to covert intelligence surveillance (as might become the case were a streamlined renewal process adopted along the lines suggested at DP p 42).

2.2 ASIO "named person" warrants and person search warrants

For the same reasons as were stated above, this submission does not support the proposal to create a new category of "named person" warrant to authorise ASIO surveillance, nor a new category of "person search" warrants. Administrative burden is a small price to pay in order to preserve a regime which creates a strong presumption against the permissibility of covert intelligence intrusion into people's affairs.

Personal searches in particular are inherently coercive, and the granting of coercive powers to a covert intelligence agency raise particular concerns about privacy, the integrity of the individual, and the proper relationship between government and citizen. The granting to ASIO of powers of personal search was itself highly

controversial, and this submission strongly opposes its further extension. If individuals are suspected of committing criminal offences there is already ample provision under state and Commonwealth law for police officers to exercise powers of arrest and/or search. Steps should not be taken which would give ASIO even the hint of the character of a secret police force.

2.3 ASIO computer access and surveillance devices warrants

This submission does not oppose the amendment of ASIO's powers in relation to the investigation of computers, and the collection of intelligence via surveillance devices, to bring them into line with contemporary technical realities. In the case of computer access warrants defined in terms of "networks" or "computers connected to a particular person", however (DP p 41), similar concerns to those expressed above about the collection of information pertaining to persons of no interest would arise. "Computers on a particular premises" seems therefore to be the most narrow way of framing an appropriate expansion of computer access warrants.

This submission also doubts the appropriateness of ASIO warrants permitting disruption of data on computers, or access to third party communications and/or computers. As the DP notes (p 50), safeguards for privacy would be essential, but it is not clear how accountability mechanisms of this sort would work in practice for a covert intelligence agency.

2.4 ASIO authorised intelligence operations and evidentiary warrants

This submission does not support the proposal that a regime be established to permit authorised intelligence operations along the model already existing for controlled operations by law enforcement agencies. The Discussion Paper correctly notes some of the mechanisms that would be necessary to ensure propriety and accountability (pp 46–47) but the difficulties nevertheless seem very great.

These difficulties inherent in the notion are illustrated by the Discussion Paper itself, which gives *training with a terrorist organisation* as an example of the sort of offence that might be authorised under such a scheme (p 46), while at the same time suggesting that conduct that is likely to cause the death of or serious injury of a person might be precluded from authorisation (p 47). Of course, the likelihood of

death or serious injury is (notoriously) not an element of many offences established under Part 5.3 of the *Criminal Code*, but the Discussion Paper itself refers to the prevention of "mass casualty" terrorist acts as an important rationale for the ongoing work of law enforcement and intelligence agencies (p 15). It is not at all clear, therefore, how authorisation to join in the activities of those terrorist organisations actually under investigation would be reconciled with the appropriate limitations on any such scheme.

A more general concern is that, of necessity, a covert intelligence agency is not subject to the same degree of oversight and accountability in its operations as is a police force. The concerns of ASIO are necessarily very different from those of a police force or a public prosecution service. Australian police forces and prosecutors are obliged to act in an apolitical fashion. They are independent of the political Executive. They ought not to be motivated by foreign policy or similar political concerns. ASIO, on the other hand, is tightly integrated into the political Executive, being subject to ministerial direction in several respects.[5] ASIO is also statutorily obliged to have regard to foreign policy considerations, as its functions include carrying out Australia's responsibilities to foreign countries in respect of their security, and obtaining, within Australia, intelligence concerning the capabilities, intentions and activities of foreign governments.[6]: And ASIO is not subject to the discipline of collecting evidence that will be admissible in a criminal trial. The notion of authorised intelligence operations ought therefore not to be taken up.

For similar reasons, this submission also does not support an evidentiary certificate regime that would increase the degree of covertness of ASIO intelligence operations.

2.5 Ministerial authorisation under the Intelligence Services Act

This submission does not support an expanded scope of ministerial authorisations under section 9 of the *Intelligence Services Act 2001*. Of particular concern is the reliance, in the Discussion Paper, on amendments made in 2011 to the *Telecommunications (Interception and Access) Act 1979*. In its submission to the

[5] *ASIO Act* ss 8(2), 8A, 19(1). The Minister also plays a key role in approving the issue of warrants under Divisions 2 and 3 of Part III of the Act.
[6] *ASIO Act* s 17(1)(a),(e) read together with the definitions of "security" and "foreign intelligence" in s 4.

Senate Legal and Constitutional Committee inquiry into that piece of legislation,[7] the Castan Centre expressed concern that

> these intelligence agencies, which hitherto have had as their function collection of intelligence about the capabilities, intentions or activities of people or organisations outside Australia, [taking] on a significant domestic operation.

For the sorts of reasons already stated at 2.1 above, it would be inappropriate for these extremely covert agencies to have a further-increased role in spying upon Australians.

[7] Available at <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/telecommuinication_interception_intelligence_services_43/submissions.htm>