Castan Centre for Human Rights Law
Monash University
Melbourne

Submission to the Senate Standing Committee on Legal and Constitutional Affairs

Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008

Prepared by Dr Patrick Emerton,

Ms Stephanie Cheligoy, Ms Meagan Grose, Ms Hannah Pearson, Ms Fiona Ransom, and Ms Philippa Ross

This Submission concerns the Telecommunications (Interception and Access) Amendment Bill 2008 (Cth) (hereafter, the Bill). It is particularly concerned with Items 3–14, 20–25, 35 and 37 of Schedule 1 of the Bill. These would broaden the scope of interception that may be authorised by a particular category of warrant, and make consequential amendments to reflect that broadened scope.

The Current Law

Currently, interception warrants can be issued in relation to

(1) Specific telecommunications services; and

(2) Specific named persons, either in relation to

a. Telecommunications *services* being used by a particular person; or

b. A particular telecommunications *device*.[1]

The following bodies may apply for the issue a named person warrant:

- The Director-General of Security (on behalf of ASIO);[2]
- The Australian Federal Police;
- The Australian Commission for Law Enforcement Integrity;
- The Australian Crime Commission; and
- Eligible State agencies.[3]

With the exception of the Director-General of Security, who applies to the Attorney-General for the issue of a warrant, the application must be made to an eligible judge or nominated AAT member.

As the law stands currently under sections 9A, 11B and 46A of the Act, a named person warrant can be issued in relation to *any* telecommunications services being used by a particular person, or in relation to a *specified* telecommunications device being used by a particular person.[4]

---

[1] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 9A, 11B, 46A.
[2] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 9A(1), 11B(1).
[3] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5, 46A.
[4] The requirement for specification is stated at sections 9A(2)(ba), 11B(2)(ba), 42(4A)(ba).

The Proposed Amendments

The Bill proposes to amend sections 9A, 11B and 46A so that a named person warrant, issued in respect of *devices* rather than *services*, will authorise interception of communications on any telecommunications device that the person uses or is likely to use.

Furthermore, instead of being obliged to identify a particular device in the warrant as one which the named person is using or likely to use,[5] the officer applying for the warrant would need only to specify the details of devices that the named person is using, or is likely to use, to the extent that they are known at the time of applying for the warrant.[6]

Submissions on the Proposed Amendments

1. Broadening of powers of interception

The Attorney-General's second reading speech describes the proposed amendments as 'technical amendments' that 'clarify and align' certain processes but 'do not provide any new powers for law enforcement or security agencies.'[7] The amendments are not merely technical, however. They effect a broadening of powers of ASIO and other agencies, including the AFP, to intercept communications made via '*any* telecommunications device that the person is using or is likely to use', whereas currently this power is limited to 'a *particular* telecommunications device' (emphasis added) that must be identified in the application for a warrant.[8]

The Explanatory Memorandum states that these amendments will make device-based named person warrants '[c]onsistent with service-based named person warrants.'[9] In the case of warrants issued to ASIO, the Explanatory Memorandum

[5] Ibid.
[6] Telecommunications (Interception and Access) Amendment Bill 2008 (Cth) Schedule 1, Items 6, 11, 20.
[7] Hansard, House of Representatives, Wednesday 20 Feb 2008 p. 836-7.
[8] Above n 4.
[9] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2008 (Cth) pp. 4, 6.

states that the amendments 'clarify that a device-based named person warrant … gives the authority to intercept multiple telecommunications devices.'[10] In relation to warrants issued to other agencies, it states that the amendments 'would allow for multiple telecommunications devices to be included.'[11] The second of the two quoted characterisations is the more accurate, as it makes clear that the amendments would allow what is currently not allowed.

It is true that the Act as it currently stands does contain some suggestion that communications from additional devices might be intercepted under the authority granted by such a warrant,[12] but these somewhat obscure suggestions must be taken to be outweighed by the clear wording of the act, that a device-based named person warrant 'authorises interception of communications made by means of a telecommunications device identified in the warrant.'[13] Amendments which remove this requirement of specificity, and would permit interception of communications from any device that the named person uses or is likely to use, are not merely clarificatory.

2. Violations of the privacy rights of third parties

One significant consequence of this broadening of the range of telecommunications devices from which communications may be intercepted would be to permit further incidental monitoring of people who are themselves of no relevance to a particular investigation, but who happen to use a telecommunications device that is 'likely' to be used by a person named in an interception warrant. This may be particularly so in relation to personal computers that are open for public use (eg in public libraries or internet cafes). By way of contrast, a service-based named person warrant may well not authorise interception of all communications from such a device, as many of the users of such a device may not be using it to communicate via a service that the

[10] Ibid p. 4.
[11] Ibid p. 6.
[12] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 16(1A)(d), 60(4A)(d); see also the remark in the Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth) pp. 37, 38, that these particular provisions of the Act recognize that 'named person warrants may authorise interception of multiple telecommunications devices.' Even if this is so, it does not follow that such a warrant authorizes interception of communications from a device not identified in the warrant.
[13] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 9A(3), 11B(3), 46(3)

person named in the warrant is using or likely to use. Therefore, these amendments would increase the power of interception, and not merely establish an equivalence between device and service-based warrants.

In the absence of an express right to privacy under Australian law, legislation such as the Act plays an important role in safeguarding the privacy of individuals. Australia is a party to international agreements which recognise the right to privacy, and which oblige Australia, at international law, to respect that right and ensure it to all individuals within Australia.[14] In particular, Article 17 of the *International Covenant on Civil and Political Rights* states that

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

In its General Comment 16, the Human Rights Committee[15] says in relation to Article 17 that

> In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances…
>
> [R]elevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.[16]

[14] *International Covenant on Civil and Political Rights* Articles 2, 17.
[15] Established under Part IV of the *International Covenant on Civil and Political Rights*.
[16] Human Rights Committee, General Comment 16 [8]. Available at <http://www1.umn.edu/humanrts/gencomm/hrcom16.htm>.

Australia's constitutional arrangements are such that Australia's international human rights obligations do not automatically become incorporated into Australian domestic law. As a consequence, it falls to the Parliament to ensure that Australian legislation does not infringe human rights. The Act ought not to be amended in such a way as to increase the likelihood of violations of the right to privacy of innocent parties. The proposed amendments, in particular, seem likely to increase the interception of communications by third parties whose circumstances and right to privacy has not been taken account of by the authority issuing the warrant. This would be quite contrary to the right to be free of arbitrary interference with one's privacy, as interpreted by the Human Rights Committee in the passage quoted above.

3. Accountability of agencies

A second consequence of this broadening of the range of telecommunications devices from which communications may be intercepted would be to dilute the statutory obligation of ASIO, the AFP and other interception agencies to justify their interception of telecommunications which, but for authorisation via a warrant, would be prohibited.[17] The removal of the requirement to identify the device from which communications are to be intercepted, and the substitution of a requirement to specify only the details of devices that the named person is using, or is likely to use, to the extent that they are known at the time of applying for the warrant, weakens the connection between the grounds which must be made out in order for a warrant to be issued, and the actual interception that may end up being carried out under the authority of the warrant.

One potential consequence of such a dilution of accountability would be to encourage the undertaking of 'fishing expeditions', as agencies become freer to form their own, untested, views as to which devices a person is likely to use. This also further exposes the communications of third parties, not named in the warrant, to the possibility of interception, which is objectionable for the reasons given earlier in this submission.

[17] *Telecommunications (Interception and Access) Act 1979* (Cth) s 7.

The dilution of accountability also has more general implications for the conduct of investigating and intelligence-gathering agencies. Recent events pertaining to security policing and intelligence-gathering – in particular, the well-known arrest and subsequent release of Dr Mohammed Haneef, and also the recent finding by Justice Adams of the New South Wales Supreme Court that ASIO officers, in the course of investigating Izhar Ul-Haque, had 'committed the criminal offences of false imprisonment and kidnapping at common law and also an offence under s86 of the *Crimes Act* 1900'[18] – strongly suggest that investigatory agencies need to be held more accountable in the exercise of their statutory powers, not less so. The effect of the Bill would be precisely the opposite of this, however: it would broaden the scope of interception powers while reducing the onus on an officer seeking a warrant to explain and justify to the issuing authority the details of what will be done under the warrant.

This is not simply a matter of protecting the human rights of those whose communications might be intercepted. It is also about ensuring and strengthening the integrity and lawfulness of agencies themselves. History – including the recent Australian history mentioned above – shows that one important way to ensure that agencies act efficiently, effectively and lawfully is to require them to account for the exercise of their powers. This can be achieved, in part, by insisting upon a stricter rather than a looser connection between the grounds on which a warrant is issued, and the activity undertaken pursuant to that warrant.

In his judgement referred to above, Justice Adams also found that

> The evidence of the ASIO conduct, considered alone, would be sufficient to establish oppressive conduct within the [*Evidence Act 1995* (Cth)]. But the oppression was continued, in my view, by the conduct of the AFP…
>
> The impropriety of [the ASIO officers] was intentional and calculated to produce the very admissions that were made. It was grave. There is no

[18] *R v Ul-Haque* [2007] NSWSC 1251 [62].

> suggestion that the officers acted contrary to ASIO protocols and good reason for thinking that they did not.[19]

These findings strongly support the suggestion that, in order to protect their own interests as well as the interests of those whom they investigate, the accountability of these agencies needs to be strengthened and not weakened as it would be by the Bill.

4. Absence of reporting requirements

The Act currently establishes a variety of annual reporting requirements pertaining to the application and issue of named person warrants.[20] These include a requirement to report, in relation to service-based named person warrants, how many of those in a given year involved the interception of a single, of two to five, of six to ten and of more than ten telecommunications services, and also to report how many telecommunications services in total were intercepted, in a given year, pursuant to such warrants.[21]

If the proposed amendments pertaining to the issuing of device-based named person warrants were to be enacted, than similar reporting requirements in respect of such warrants ought also to be enacted. This would permit a degree of public scrutiny of the use to which the new power was being put, were it to be enacted.

[19] Ibid [98], [105].
[20] *Telecommunications (Interception and Access) Act 1979* (Cth) s 100. Items 43 and 46 of the Bill would make certain amendments in relation to these, namely, the removal of the requirement, in relation to named person warrants, to report on warrant applications that included requests that the warrants authorise entry on premises (the requirement arises under section 100 of the Act). The Explanatory Memorandum states that the existing requirement 'is redundant because a Part 2-5 warrant does not authorise entry on to premises.' This is in fact not strictly true, because warrants apt to be issued under section 46 may also authorise entry on to premises, but it is the case that Part 2-5 *named person warrants* (issued under section 46A) may not authorise entry on to premises: *Telecommunications (Interception and Access) Act 1979* (Cth) s 48.
[21] *Telecommunications (Interception and Access) Act 1979* (Cth) s 100(1)(eb)(ec),(2)(eb)(ec).