NSWCCL
New South Wales Council for Civil Liberties

New South Wales Council for Civil Liberties Inc
149 St Johns Road
Glebe NSW 2037
Australia
www.nswccl.org.au

Ph 61 2 9660 7582
Fax 61 2 9566 4162
Email office@nswccl.org.au
DX 1111 Sydney

Correspondence to:
PO Box 201
Glebe NSW 2037
Australia

Submission
to the Senate Standing Committee on Legal and Constitutional Affairs
concerning the Telecommunications (Interception and Access) Amendment Bill 2008

The New South Wales Council for Civil Liberties (CCL) is grateful for the opportunity to comment on this Bill.

Recommendation: That items 3-14, 20, 25, 31 and 35 of the Bill be rejected.

If passed, this Bill will substitute the phrase 'any telecommunications device' for 'a telecommunications device identified in the warrant' in paragraph 9A(1A)(b) of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act), with related changes elsewhere in section 9A and in sections 11B, 16, 42, 46A and 60.[1]

The effect is to allow a device-based named person warrant to be issued for interception of telecommunications, a warrant that is not specific as to the devices which may be tapped. That is, armed with such a warrant, an officer of a service may tap any or every device used by the person named in the warrant, or any device it is thought the person is likely to use. The Bill potentially authorises the interception of all telecommunications devices of persons associated with the person named in the warrant. This is because the named person might, conceivably, use a device in the possession of an associate or a family member.

This is no minor, technical change, despite what is said in the Explanatory Memorandum or the Minister's Second Reading Speech. It has important privacy implications, which are not addressed in the Minister's Second Reading Speech or in the Explanatory Memorandum.

CCL recommends that all the items in Schedule 1 which effect this change be rejected. Only identified devices should be intercepted.

Privacy is no trivial matter. Intrusion upon it lays the victim open to discrimination and victimisation. Covert intrusions leave the victim open to mistaken data matching. The knowledge that words and actions may be being monitored restricts autonomy and personal growth and the development and enjoyment of relationships. In the hands of the unscrupulous, covert surveillance leaves the victims open to blackmail.

Privacy is protected in the TIA Act in two ways. 1. Authorities that issue warrants are required to take privacy into account before they issue warrants, and warrants are not to

[1] The relevant items are numbers 3-14, 20, 25, part of 31, and 35

be issued if alternative means of investigation are possible. 2. There are several requirements on what may be done with the content of intercepted messages.

There is reason to be concerned that issuing authorities do not take the privacy requirement seriously before issuing warrants. Of 3,287 warrants sought in the year to June 2007, only 7 were rejected or withdrawn.[2] (In the previous two years, the figures are six out of 2,889 applications and 5 out of 2,934.) Of 71 applications for B-Party warrants (the most intrusive form of surveillance) none were rejected.[3] The total number of warrants issued in 2006-2007 is greater than that in the 2005-2006 year, when it exceeded the total number of equivalent warrants issued in the United States (2,929 in Australia as opposed to 1,839 in the United States).[4] An analysis of the figures shows that in 2005-2006, on a *per capita* basis, an Australian telephone was 23 times more likely to be bugged than an American telephone.

It is also worth noting that in the United States only judges may issue telecommunications warrants, while in Australia, almost all warrants (93%) are issued by non-judges. This is despite the fact that judges make up almost 60% of all the people authorised to issue warrants in Australia. The vast majority of warrants are being issued by lawyers who sit as members of the Administrative Appeals Tribunal (AAT). AAT members do not have tenure, are appointed by the government and work on contract. This means that AAT members are less likely to be as fearless as a judicial officer, which might explain why most warrants are issued by non-judges. Judges simply would not issue so many warrants: as is evidenced by the figures in the United States of America, where only judges may issue warrants and the *per capita* figures are vastly lower.

It is a reasonable conclusion that interceptions in Australia are being authorised and undertaken for inadequate reason, and without regard for the privacy of those affected. In the absence of an independent observer and participant in warrant hearings (such as the Queensland Public Service Monitor), it is not clear that warrants are only sought and issued when other means of obtaining information have been exhausted.

Even where the issuing authority is careful about the invasion of privacy involved in surveillance, it will be impossible for that authority to know the extent of the invasion. For if the Bill is passed, the officers executing a device-based named person warrant will be able to intercept devices which are not listed on the application.

A significant number of additional people will have their conversations and other messages listened to or read if this Bill is passed. These will include users of intercepted devices other than the targeted person, and those with whom they communicate. Until such time as devices are identifiable by unique identifiers and accidental interception of

---

[2] Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979: Annual Report for the year ending 30 June 2007*, Table 1.
[3] TIA Act Report (June 2007), n 2, Table 12.
[4] Administrative Office of the United States Courts, *2006 Wiretap Report* (April 2007), Table 2, <http://www.uscourts.gov/wiretap06/contents.html>.

the wrong devices is eliminated, they will also include persons not connected in any way with the targeted person. The broader the range of devices which are targeted, the greater the increase in invasion of privacy.

CCL accepts that telecommunications interception is a legitimate tool for the investigation of serious crime and the prevention of terrorism within a framework that provides adequate safeguards. It is worth noting, however, that the vast majority of interceptions are not concerned with the prevention of terrorism, or even of investigation of crimes involving terrorism. In the year to June 2007, of 3,280 warrants issued, only 33 were for terrorism prevention. For all the cases where life is in danger (terrorism, kidnap, murder and serious personal injury of loss of life), only 928 warrants were issued, or 28% of the whole. The remaining 2,349 were issued in connection with lesser (though mostly serious) offences (1,494 of them being drug offences). The telecommunications interception regime should be assessed and justified according to the general run of the mill type of situation in which is used - not the most serious possible cases. [5]

The TIA Act already intrudes excessively on privacy. No reason has been given for the changes proposed in this Bill. They should be rejected.

Martin Bibby
Convenor, Civil and Indigenous Rights Subcommittee,
9.iv.2008

[5] TIA Act Report (June 2007), n 2, Table 28.