PARLIAMENT of AUSTRALIA

Submission No. 11 - Australian Privacy Charter Council

Parliamentary Joint Committee on the Australian Security Intelligence Organisation

Review of the Australian Security Intelligence Organization Legislation Amendment Bill 1999
Submissions

Submission No. 11 - Australian Privacy Charter Council

THE AUSTRALIAN PRIVACY CHARTER COUNCIL

Hosted by the School of Law, University of New South Wales

Convenor : Nigel Waters

Secretary : Tim Dixon

School of Law, University of NSW

Sydney NSW 2052

Phone 02 9810 8013

E-Mail: watersn@zip.com.au

Cheryl Scarlett, Secretary

Parliamentary Joint Committee on ASIO

Parliament House

CANBERRA ACT 2600

25 April 1999

Dear Ms Scarlett

Review of the Australian Security Intelligence Organization Legislation Amendment Bill 1999

Thank you for sending the papers relating to this review.

I attach a submission on behalf of The Australian Privacy Charter Council, but repeat again our concern about the inadequate period of consultation on this important Bill. In our view, there needs to be not only a longer period, but also an opportunity to make follow up submissions after we have seen the transcripts of the Committee's hearing.

This two stage process is necessary in this instance because of the secrecy surrounding ASIO's operations - public interest groups such as ours do not have the level of information that would normally be available with most legislation about what currently happens and why the amendments are considered necessary. The explanatory memorandum only provides some of the background, and it would help us give informed comments if we could read what the Committee finds out at its hearing on Tuesday 27 April.

Please let me know if we can be of further assistance to the Committee.

Yours sincerely

Nigel Waters

Convenor

Review of the Australian Security Intelligence Organization Legislation Amendment Bill 1999

Submission by the Australian Privacy Charter Council

April 1999

Introduction

The Australian Privacy Charter Council exists to promote the Charter Principles, which are a statement of best practice for the protection of privacy, including the fair handling of personal information, and minimisation of the level of surveillance of Australians in their day to day activities. I attach a copy of the Charter.

While we appreciate the sensitivity of any inquiry or review involving national security and intelligence matters, this sensitivity makes it all the more important that there is a careful consideration of any changes in the parameters of ASIO's activities.

The Charter Council is particularly concerned about any extension of ASIO's ability to intrude into the personal affairs of Australians, especially if they have given no 'cause' for investigation. We are also concerned that there should be no diminution, and if possible an increase, in the level of accountability, scrutiny and safeguards applying to ASIO.

We note that although ASIO is exempt from the Privacy Act 1988, it is subject to guidelines for the conduct of its activities which are based on the Information Privacy Principles of that Act, compliance with which is monitored by the Inspector General of Intelligence and Security.

We submit that the period of consultation on this important Bill is wholly inadequate. We have difficulty in understanding how these changes can be required so urgently as to necessitate such an abbreviated period of consultation and consideration. In our view, there needs to be not only a longer period for informed debate, but also an opportunity to make follow up submissions after we have seen the transcripts of the Committee's hearing.

This two stage process is necessary in this instance because of the secrecy surrounding ASIO's operations - public interest groups such as ours do not have the level of information that would normally be available with most legislation about what currently happens and why the amendments are considered necessary.

Overall context

We note from the Second Reading Speech that the government does not intend to extend ASIO's functions, and that the amendments are not occasioned specifically by any one event or threat, including the next year's Sydney Olympics. The amendments are claimed to be only ensuring ASIO's ability to meet a changing operational and technological environment. While this is superficially re-assuring, the public needs to be assured that there is no 'creeping' extension of functions, and that any changes that intrude on civil liberties and privacy are the minimum necessary to maintain the existing level of capability. The declaration in the speech that the changes "simply will enable the Organisation to meet its statutory responsibilities in more efficient and effective ways" hints at more than just a maintenance of the status quo. ASIO is one organisation whose performance must not be measured solely in terms of results or ends - the *means* by which those results are achieved are critically important as well.

Some of the comments in this submission may go to ASIO's existing powers and functions, rather than just to the effect of the proposed amendments. We submit that the Committee should be prepared to consider such comments in view of the fact that this is a rare opportunity to publicly debate ASIO's role. The government argues that the operational environment has changed, and it is surely therefore legitimate to discuss not only whether the proposed changes are necessary, but also whether there are other changes, not on the government's agenda, which may also be desirable.

Changes in the environment not mentioned by the government include the end of the "Cold War". While there are clearly still both old and new threats to national security which justify a continued role for intelligence services, one would have expected the removal of a major threat to yield a significant dividend in terms of resources. It is difficult to judge the extent of any such dividend from the limited information available. From the most recent annual report (1997-98), ASIO's staffing appears to have been reduced by about 20% since 1993/94, but this might have been expected anyway given the growth of technological means of intelligence gathering. While the foreword mentions a budget of some $53 million, no time series is given to indicate the overall growth trend.

The Committee will be fully aware of the tendency of bureaucratic organisations to resist shrinkage. It is obviously particularly important that an organisation such as ASIO should not be allowed to 'invent' reasons for survival and growth which are not founded squarely on the statutory reasons for their existence. We do not suggest that this motive necessarily underlies the proposed amendments - merely that vigilance against any such tendency is essential.

Warrants

Test for the issue of warrants

The proposed change to the test for the issue of warrants in s.25 (new s.25(2)) is much more significant than the Explanatory Memorandum suggests. Changing the test from 'serious impairment' (current s.25(1)) to 'substantially assist' represents a major reduction in the threshold. To say, as the Explanatory Memorandum does, that this is merely 'simplifying the description of the matters about which the Minister must be satisfied' is positively misleading. This proposed change is fundamental and deserves a serious justification and much wider debate.

Controls over warrants - Time periods

We have no objection in principle to the proposed extension of the warrant provisions to ensure technological neutrality. However, we do not believe the case has been made for the proposed substantial weakening of the controls over warrants. In particular, the extension from 7 to 28 days for the maximum duration of warrants (ss 25(10) and 27(a)(3)(a)), and the provision of a period of up to 28 days before a warrant commences (s.25(8)) mark a major increase in ASIO's discretion and loss of detailed control by the Minister. Any such change which makes it easier for ASIO to obtain a warrant, or to use one warrant instead of making separate applications, runs the risk of encouraging a less disciplined use of ASIO's powers.

Access to computer data

The Council is concerned that the implications of the proposed new s.25 in relation to access to computer data have not been fully thought through. As the government is well aware, the importance of trust in electronic transactions cannot be overestimated. Confidence in the integrity of electronic transactions is essential for the take up of new forms of commerce and service delivery and for Australia's future in the global information economy. However well intentioned, empowering ASIO to add, delete or alter data, and to modify access control and encryption systems (even if technically feasible) fatally undermines this trust and confidence. It is

difficult to see how the supposed limitations on this power - not obstructing lawful use or causing loss or damage - would work in practice, and in any case they would not restore the confidence which, once lost, is gone forever. The Council does not claim detailed expertise in the area of electronic commerce or cryptography applications, but understands enough to know that this proposal is fraught with dangers and needs much more discussion in the relevant technical communities as well as in the general public arena.

Recovery of tracking devices

The proposed provision for tracking devices to be recovered 'as soon as practicable' after expiry of the relevant warrant (ss 26B(7) and 26C(7)) appears to create a risk of abuse which is not discussed. Unlike the similar provisions proposed for recovery of listening devices (s26(6A), it will not in practice be possible for ASIO to comply with the assurance given in the Explanatory Memorandum (for listening devices) that "this item does not authorise ASIO to use [a device] after the warrant has lapsed or is revoked" By definition, it will be necessary to *use* a tracking device to locate it so that it may be recovered. If ASIO is allowed to delay recovery indefinitely, as is proposed, then this amounts to an indefinite extension of the warrant.

Warrants for inspection of delivery service articles

If this new section (s.27AA) does no more than replicate the provisions relating to articles in the course of delivery by Australia Post, the Council would have no difficulty (other than the general concern about authority for warrants explained below). However, there appear to be some important safeguards and limitations applying under s.27A which are missing from s.27AA. In particular, the restriction on the exercise of this power to information about people other than citizens and permanent residents (s.27A(9) is not included. If this is a deliberate difference it is clearly very significant, and yet no explanation or justification appears to be offered. In the time available, the Council has not been able to conduct an exhaustive comparison of ss 27A and proposed 27AA. We submit that the Committee should insist on such a comparison, and explore the reasons for any differences.

Authority to issue warrants

We also take the opportunity of the proposed extension of warrant issuing powers to object in principle to the absence of any independent scrutiny of warrant applications. The Attorney-General, who issues warrants, is also the Minister responsible for ASIO and neither that office-holder, or any other member or servant of the Executive can be seen as genuinely independent. We are aware of the difficulties that have arisen recently over the issuing of law enforcement warrants by the judiciary (see the Council's submission to the review of Telecommunications Interception attached). In our view, the significance of ASIO's powers justify the removal of warrant issuing function to some independent officer - perhaps one or more retired senior judges nominated by the judiciary.

Proposed amendments to the Financial Transaction Reports Act 1988, and the Taxation Administration Act 1953

These amendments would provide ASIO with direct access to FTR and Tax information which at present they would presumably only be able to access indirectly via joint investigations with authorised recipients, or under a warrant. The Council notes the argument in the Explanatory Memorandum that activities prejudicial to national security are likely to be connected with concealed movements of money. But no explanation is given as to why the existing means of access to such information are not adequate. Given the importance of warrant processes in the statutory scheme for ASIO, the proposed provision of an alternative, and much easier route to the same information needs much greater justification. The Council notes in particular the very specific focus of the original FTR legislation on organised and major crime, and the assurances that were given to the public at the time that this focus would be maintained. We have already seen over the last decade a gradual extension of the range of public interests being served by FTR information, subverting these assurances.

In relation to FTR information, the proposed safeguards of a memorandum of understanding with the Director of AUSTRAC, and a review of ASIO's personal information guidelines involving the Privacy Commissioner, would be welcome, but are no substitute for a much better justification for direct access. We submit that the Committee should insist on this justification and on an opportunity for further public discussion.

Reporting requirements

The Charter Council welcomes the increasing amount of information about ASIO's activities contained in the unclassified version of its Annual Report. Unfortunately, the most significant information most relevant to ASIO's intrusions into individuals' personal affairs remains secret. We fail to see how the publication of some general details of intelligence collection (edited out of the unclassified Report - see page 53) and of statistics on the number and types of warrants approved by the Attorney General (see page 22) could prejudice ASIO's operations. Regrettably, the community is still asked to rely on assurances that the accountability of ASIO to the Minister, monitored by the Inspector-General of Intelligence and Security is sufficient. It is not. We submit that the introduction of new forms of warrant, covering new intelligence gathering and surveillance techniques, provides an opportunity to improve the accountability mechanisms. Specifically, ASIO should be required to report annually on the number and type of warrants applied for, and the number of approvals or refusals, to give some idea of the scale of intrusion involved, and of the trends over time.

If the amendments to the FTRA and TAA were to go ahead, both ASIO and the Inspector-General, as well as AUSTRAC and the Tax Commissioner, should be required to report *publicly* on the volume of requests for information from those two sources.

Related matter - Disclosures to ASIO under the Telecommunications Act 1997

The Council takes this opportunity to draw to the Committee's attention a related matter.

Part 13 of the Telecommunications Act 1997 provides for carriers and carriage service providers to disclose personal information to an officer of ASIO where that officer is authorised as needing it for the ASIO's purposes. Unlike the equivalent provisions for disclosure to law enforcement agencies, there is no requirement on the carriers and carriage service providers to keep a record of the disclosures to ASIO. The Council is concerned that there is no effective safeguard against abuse of this power by ASIO, or against impersonation of an ASIO officer by third parties. When Telecommunications was a state monopoly, specialised Telstra staff could be relied on to know ASIO contacts personally, providing some, albeit informal, safeguard. Now that there are many hundreds of

organisations covered by the Telecommunications Act, it is unrealistic to expect them to do anything but take the ASIO officer's word for the 'need', and take the bona fides of the officer at face value. At least a record keeping requirement, subject to inspection by a statutory officer, would provide some small check on potential abuse.

Council representatives have raised this issue in the Australian Communication Industry Forum working parties which are developing codes of practice on privacy and assistance to law enforcement, but it is seen as being too difficult and/or bound up with statutory requirements to be within their terms of reference to address. We submit that the Committee should inquire into the issue and insist on better safeguards.

End of submission

Attachment A - Australian Privacy Charter

Attachment B - Australian Privacy Charter Council submission to the Attorney-General's Department's review of Telecommunications Interception Policy, April 1999

A copy of this submission is also available from the Committee Secretariat.