Australian Government

Office of the Privacy Commissioner

Telecommunications (Interception and Access) Amendment Bill 2007

Submission to the Senate Legal and Constitutional Affairs Committee

July 2007

1. Office of the Privacy Commissioner

The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

2. Background

The Office welcomes the opportunity to comment on the *Telecommunications (Interception and Access) Amendment Bill 2007* (Cth) (the Bill).

In 2005 Mr Anthony Blunn AO conducted a review (the Blunn Review)[1] of the *Telecommunications (Interception and Access) Act 1979 (*the Interception Act*)*[2]. Among other matters, the Blunn Review recommended that interception powers and functions should be consolidated into the Interception Act rather than being spread between the Interception Act and the *Telecommunications Act 1977* (the Telecommunications Act). The Bill relates to the second stage of the Australian Government's legislative program towards implementing the recommendations from the Blunn Review.[3]

In February 2007 the Office made a submission to the Attorney General's Department regarding the contents of the Exposure Draft of the Bill.[4] While the Office in general welcomed the intent of the Bill it considered that stronger consolidated powers for law enforcement agencies should be balanced by a requirement for agencies to consider privacy concerns when exercising their powers.

The Office is pleased that a number of the issues raised in our previous submission have been addressed in the Bill and Explanatory Memorandum. Specifically, the Explanatory Memorandum and Second Reading Speech now define the distinction between call data and the content of a communication. This means that under the provisions of the Bill only call data is able to be lawfully disclosed and not the content of the communication, including

[1] *Report of the Review of the Regulation of Access to Communications*, A S Blunn AO, August 2005 located at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~xBlunn+Report+13+Sept.pdf/$file/xBlunn+Report+13+Sept.pdf

[2] The Telecommunications (Interception) Act 1979 was renamed to the Telecommunications (Interception and Access) Act 1979 in 2006 [40/2006].

[3] News Release dated 8 February 2007 from the Attorney-General The Hon Philip Ruddock MP located at http://www.ag.gov.au/agd/WWW/ministerruddockhome.nsf/Page/Media_Releases_2007_First_Quarter_0252007_-_8_February_2007_-_Telecommunications_Amendment_Bill_out_for_comment.

[4] Located at http://www.privacy.gov.au/publications/subtel0207.html.

voluntary disclosures that may be made by carriers to ASIO and law enforcement agencies. In the opinion of the Office, the information provided mitigates the risk that content will be inadvertently disclosed.

The Office now submits the following issues for consideration by the Committee.

3. The proposed Amendment Bill

3.1 Voluntary disclosures to ASIO and law enforcement agencies

At present under subsections 282(1) and 282(2) of the Telecommunications Act an employee of a carrier is allowed to make voluntary disclosures relating to call data. This applies where, in the course of their employment, the employee comes across information which is relevant to the performance of ASIO's functions or the activities of law enforcement agencies.

The Bill proposes to consolidate these provisions within the Interception Act by repealing subsections 282(1) and (2) and creating similar provisions in the Interception Act. The provisions proposed by the Bill will not prohibit the voluntary disclosure of call data[5] to ASIO and law enforcement agencies if the disclosure is in connection with the performance of ASIO's functions and, in the case of enforcement agencies, that the disclosure is reasonably necessary for the enforcement of the relevant law.

In our submission to the Attorney-General's Department, the Office suggested that this provision include positive obligations on law enforcement agencies to destroy irrelevant material containing personal information collected under these provisions together with information which is no longer needed by such law enforcement agencies and to do so in a timely manner. The Office notes that a similar requirement exists in section 79 of the Interception Act relating to restricted records.

The Office considers there is merit in such a requirement.

3.2 Authorisations for access to prospective information

The protection of privacy often requires balancing competing interests and assessing the proportionality of the privacy impacts of a proposal in relation to the issue that is being tackled. The Explanatory Memorandum to the Bill notes that there is a greater privacy impact for individuals through the disclosure of personal information on a prospective basis, that is information collected in near real time. Commensurate with this risk, the Bill provides that access to this type of information requires a higher level of authorisation than for access to existing information.

Under clause 180(5) of the Bill, certifying officers of criminal law-enforcement bodies are required to have regard to the extent to which the privacy of any person or persons would be likely to be interfered with by the disclosure of

[5] As defined by Blunn as *information or a document relating to a telephone call but which excludes the content or substance of call*, see n1 p34

prospective information. The Explanatory Memorandum states that this would include, for example, an assessment of the value of the information sought compared to the privacy of the user or users of the telecommunications service in question.

The Office submits that there is merit in providing practical guidance to certifying officers to enable them to discharge the obligation stated in clause 180(5) satisfactorily. Such guidance could take the form of a note to the Bill or detail in the Explanatory Memorandum. For example it could be suggested that certifying officers should consider the proportion of 'innocent' third parties whose personal information is to be collected incidentally when only information of a particular person or a much smaller number of persons is required. Additionally, a check list could be prepared which requires the certifying officer to be satisfied that the enforcement agency or body has appropriate procedures or protocols in place to deal with issues such as: the handling of irrelevant information; preventing secondary uses and disclosures; data security; and the timely destruction of records.

The Office made similar comment in our submission to the Attorney-General's Department on the Exposure Draft.

3.3 Interception capability[6] (Clause 189)

Clause 189(4) Schedule 1 of the Bill provides that the Minister, inter alia, must take into account the privacy of the users of telecommunications systems in the making of a determination on the interception capability or special assistance capability in respect of specified carriage services. As a consequence of the capability assessment, the Office understands that the personal information of telecommunications users will be collected.

The Office's submission to the Attorney-General's Department suggested the inclusion of a note to the clause, or in the explanatory memorandum, which provides guidance about how the privacy of telecommunications users will be taken into account in the making of the determination. The Office reiterates this view and suggests that such a note would assist by making it apparent where privacy issues may arise. By way of example, the prohibition on secondary uses and disclosures in clause 182 Schedule 1 does not apply here and suggests that this is one matter that could be included in such guidance material.

The earlier version of the Bill provided that the Minister must consult certain bodies prior to making a determination in relation to interception capabilities and including consulting such other persons as the Minister thinks appropriate. However, the current version of the Bill omits reference to consultation mechanisms but retains the requirement for the Minister to take into account the 'privacy of the users of telecommunications services' in clause 189(4)(c).

[6] As defined in Section 320 of the Telecommunications Act 1977 as [in relation to a carriage service*] "…the capacity of the network or facility to enable a communication passing over it to be intercepted".*

The Office is willing to assist with providing advice on the privacy impacts of a determination made under clause 189(4)(c). The Office supports the inclusion of appropriate consultation mechanisms in this process including consultation with the Privacy Commissioner.

3.5 Privacy Commissioner's monitoring role

The Office notes that the Commissioner has the function under section 309 of the Telecommunications Act to monitor:

- Whether a record made under section 306 sets out a statement of the grounds for disclosure
- Whether that statement is covered by Division 3 (which deals with exceptions).

The Bill amends section 309(2)(a) and (b) to provide that the Commissioner has the added function of monitoring compliance with the record keeping requirements under section 306A. The new provision relates to prospective disclosures made by carriers, carriage service providers and number database operators to law enforcement agencies as defined in the Bill. However we would expect that the Inspector General of Intelligence and Security (IGIS) would have a monitoring role in relation to other intelligence agencies such as ASIO.

The Office supports the new monitoring powers it will have under section 306A.

3.6 Other Matters

The Office suggests that IGIS could play a role in overseeing the development and implementation of privacy guidelines for intelligence agencies such as ASIO who will have responsibilities under this Bill. These guidelines could address matters such as:

- relevant purposes of collection
- accuracy
- secure storage
- secure destruction
- use and disclosure

The IGIS already plays a role of this kind having assisted the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO) and the Office of National Assessments (ONA) to develop privacy rules or guidelines.[7]

[7] For the privacy rules / guidelines of the DIGO, DIO and ONA, see IGIS, Annex 5, 6 and 7, 2005-06 available at http://www.igis.gov.au/annual.cfm.

3.7 Review of Interception Act

The Office's submission to the Attorney-General's Department and to the Blunn Review in 2005 both referred to previous recommendations it had made in relation to legislative review and recommended that the operation of the Interception Act should be subject to overall independent review including key stakeholder and public consultation at least every five years. The Office reiterates this view.

Key Recommendations

The Office submits that privacy protections should be balanced against law enforcement activities. Further, we suggest that encouraging exempt agencies to implement standards for the handling of personal information will support better decision-making through improved data quality.

With these issues in mind, the Office makes the following recommendations:

1. there may be a role for IGIS in assisting exempt agencies to develop and implement standards for handling personal information;
2. that the Bill include provisions to place positive obligations on law enforcement agencies to destroy irrelevant material containing personal information collected through voluntary disclosure;
3. that certifying officers authorised to approve access to prospective information should be provided with practical guidance to enable them to discern when the privacy of any person or persons is likely to be interfered with (clause 180(5));
4. In relation to interception capability activities (clause 189),:
    - a note be appended to clause 189(4), or comment made in the explanatory memorandum, which provides guidance about how the privacy of telecommunications users will be taken into account when making a Determination; and / or
    - the inclusion of appropriate consultation mechanisms in this process including consultation with the Privacy Commissioner.
5. the operation of the Interception Act should be subject to an independent review at least every five years.