Our reference: 05-0124-01hc

Senator Marise Payne
Chair, Senate Legal and Constitutional Legislation Committee
Department of the Senate
Parliament House
Canberra ACT 2600

Dear Senator Payne

Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006

Thank you for the opportunity to make a submission to the Inquiry by the Senate Legal and Constitutional Legislation Committee (the Committee) into the provisions of the Telecommunications (Interception) Amendment Bill 2006 (the Bill).

My comments on the Bill are set out below.

Stored communications

Schedule 1 of the Bill clarifies protections for stored communications such as emails, SMS messages and voicemail messages, where these are held by a telecommunications carrier, and introduces a warrant regime to allow law enforcement and other agencies to access stored communications under certain circumstances. In doing this, Schedule 1 provides privacy protections for stored communications, and therefore clarifies public understanding of the level of privacy to be expected in using electronic communications such as emails and SMS messages.

The Office notes that the Bill provides for access, under a warrant, to stored communications by law enforcement agencies and other agencies such as those responsible for administering a law imposing a pecuniary penalty, or one which relates to the protection of the public revenue. This means that for the first time agencies such the Australian Customs Service, the Australian Tax Office, the Australian Securities and Investment Commission, and similar state and territory agencies, will be able to apply for warrants under the Interception Act.

The extension of the Interception Act to these agencies may prompt interest in the community about the degree to which private communications could be monitored by a broader range of government agencies for a wide variety of purposes. For these reasons, the reporting requirements in the Bill, including the Attorney-General's annual report to Parliament, are vital to ensure transparency and to allow for the ongoing monitoring of the operation of the new stored communications regime.

The nature of stored communications may also mean that a large number of communications are accessible via a stored communications warrant because, for example, an individual may store on a carrier's equipment communications to and from a wide variety of others, possibly going back years. In these circumstances, access to stored communications under a stored communications warrant may mean that many communications are made available to enforcement agencies that may not be relevant to the purpose for which the warrant was approved. In this context, it is important to meeting the privacy objects of the Interception Act (as articulated in the *Telecommunications (Interception) Act 1979* Annual Report to 30 June 2004 at 2.2) that communications that are not necessary for the particular investigation at hand be destroyed as soon as practicable.

To this end, the Office notes that the new s. 150(1) will require the destruction, "forthwith," of information or a record that was obtained by accessing a stored communications, where the chief officer of the relevant agency "is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2)". There may be a concern here that until such time as the chief officer of the agency has considered the question of whether the information or record is required, it will be lawful for the agency to keep the information or record. In some circumstances this may have the effect that it is lawful for an agency to keep irrelevant information indefinitely. The Office recommends that consideration be given to amending the Bill to ensure that agencies take regular steps to review whether information they have accessed via stored communications warrants is still required for a permitted purpose eg; by setting a maximum period for review. This would be consistent with good privacy practice.

B-party interception

The Office notes that B-party interception provisions in Schedule 2 of the Bill may significantly raise the likelihood that communications will be intercepted that are not relevant to the specific investigation that provided the basis for the interception warrant. The Office notes the special protections in the Bill that reflect this, including the requirement that B-Party interception be a "last resort" (s. 46(3)), and the shorter period for which warrants are valid (s. 49(3)).

The Office understands that the general prohibitions around the use and disclosure of intercepted information under Part VII of the Interception Act will apply to information collected via B-party interception warrants. However, given the significant potential for the collection of personal information not related to the particular investigation under B-Party warrants, the Office recommends that consideration be given to amending the Bill to contain stricter parameters around the use or disclosure of material collected via B-party interception warrants, as compared to traditional interception warrants. Such parameters may include enforceable prohibitions on the use or disclosure of intercepted material for any purpose other than the purpose stated in the warrant; and enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed.

Equipment-based interception
Schedule 3 of the Bill broadens the ways in which law enforcement agencies may seek to intercept communications under the Interception Act. The Office appreciates that intercepting a mobile phone handset on the basis of the handset itself, rather than on the basis of a SIM card, may provide a practical solution to the problem where individuals may use many SIM cards in the one handset. However, the provisions in Schedule 3 appear to move beyond just permitting interception of particular mobile phone handsets, for example in permitting telecommunications equipment to be identified on the basis of an email address or a "user account identifier".

The Office has not been able to fully determine the limits to the scope of the operation of Schedule 3, and so recommends that careful consideration be given to ensuring that the provisions of Schedule 3 do not give rise to an unintended reduction of the privacy protections in the Interception Act.

Repeal of s. 6(2)
The Office supports the repeal of s. 6(2) of the Interception Act. This section has given rise to confusion in the past about the circumstances under which phone calls may be covertly monitored. The repeal of s. 6(2) will assist in reinforcing the privacy objects of the Interception Act.

Yours sincerely

Karen Curtis
Privacy Commissioner

March 2006