Our reference: 04-0076-01hc

Senator Marise Payne
Chair
Senate Legal and Constitutional Legislation Committee
Room S1.61, Parliament House
Canberra ACT 2600
AUSTRALIA

Dear Senator Payne

Inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 – Question on Notice and Supplementary Submission

Thank you for the opportunity to appear before the Committee last week.

At the hearing you invited me to provide observations on the potential impact of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (the Bill), if enacted, on uninvolved third parties.

In the case of a law enforcement or other agency collecting stored communications in the course of investigating unlawful activity, an uninvolved third party (third party) is an individual who is not subject to the investigation.

As we noted in our submission, the provisions of the Bill appear to mark a reduction in personal privacy in the context of communications. This is because, if enacted, the Bill would allow easier access to stored communications by law enforcement agencies, other Commonwealth agencies, internet service providers and other telecommunications service providers, and possibly others. Such access could occur with less consideration of privacy issues than is required in the issuing of an interception warrant.

As we noted in our submission, it is not clear what level of privacy protection would remain for stored communications and therefore, it is not clear what level of protection would apply in particular to information about third parties. However, on our preliminary analysis, the protections would appear to be markedly reduced in both cases.

Protections in the Information Privacy Principles
The Information Privacy Principles (IPPs) in the *Privacy Act 1988* (the Privacy Act) apply to information about individuals handled by most Commonwealth agencies, including the Australian Federal Police (AFP).

It is important to note in the context of the current Bill that the IPPs do not include a requirement to destroy data that is not relevant to an agency's functions or activities. This is in contrast, for example, to the National Privacy Principles (NPPs) that apply to the private sector (see NPP 4.2). Therefore, information about third parties may be able to be retained indefinitely by an agency.

In light of this, the Committee may wish to consider whether there are adequate existing legislative obligations, in relation to the destruction of unnecessary or irrelevant personal information (for example, that not needed in an investigation), on agencies and others that might be permitted to collect

information about third parties from stored communications, if the Bill is enacted. While we are aware of comments made by the AFP suggesting that such provisions may exist, in the time available we have not been able to consider their effectiveness.

Oversight and Accountability
The *Telecommunications (Interception) Act 1979* (the Interception Act) includes an oversight and accountability scheme. By removing stored communications from the protections of the Interception Act, important privacy protections relevant to the privacy of third parties will no longer apply.

For example, under the Interception Act, before issuing an interception warrant for a Class 2 offence, the Judge or AAT member must consider, amongst other things, the degree of interference with the privacy of any person.

In relation to all interception warrants, oversight and accountability mechanisms include the following.

- Only suitably independent authorities may issue interception warrants (e.g. Judges or certain AAT members).
- The Australian Federal Police and the Australian Crime Commission are required to maintain records relating to interceptions and the use of intercepted information. Also, the Interception Act requires the Ombudsman to conduct regular inspections of those records.
- Information collected from an interception may only be used for specified purposes, and may only be passed on to specified agencies.
- Reports must be made to the Attorney-General.
- The Attorney-General is required to table an annual report setting out the number of warrants issued for various purposes.

In the absence of these protections, the oversight and accountability of the handling of the personal information of third parties by law enforcement and other investigative agencies will be limited to a lesser accountability framework under the Telecommunications Act.

For instance, under the Telecommunications Act, telecommunications service providers are required to report information about certain disclosures to the Australian Communications Authority (ACA), which includes this data in an Annual Report. This public reporting is less detailed than that required under the Interception Act.

Also, the Privacy Commissioner has limited powers under s. 309 of the Telecommunications Act to monitor the compliance of telecommunications service providers with their record keeping obligations under the Telecommunications Act. With the work of the Office of the Federal Privacy Commissioner's compliance section currently focussed on complaint-handling, it is not carrying out audits in a range of areas, including under this provision.

I hope this information is of assistance to the Committee in its deliberations.

Yours sincerely

Timothy Pilgrim

Timothy Pilgrim
Acting Privacy Commissioner

9 July 2004