Office of the Victorian Privacy Commissioner

GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne

Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

Telephone 1300 666 444
Facsimile 1300 666 445

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au

28 June 2004

Our Ref: PL00157

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

By email: legcon.sen@aph.gov.au

Dear Senator Payne,

Inquiry into the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*

I refer to the letter dated 18 June 2004 from Mr Phillip Bailey, Acting Secretary for your Committee, and thank you for the invitation to make a submission on the above Bill.

As you know, I made a submission to your Committee in March 2004 on an earlier version of this Bill, the *Telecommunications (Interception) Amendment Bill 2004*. That Bill (and the one that preceded it, the *Telecommunications (Interception) Amendment Bill 2002*) attempted to clarify the operation of the *Telecommunications (Interception) Act 1979* ("the TI Act") to stored messages and ensure that law enforcement agencies could access these messages with a search warrant rather than the more stringent telecommunications interception warrant.

The Bill currently before the Parliament goes further than its predecessors in diluting privacy protection for emails and other stored messages. There is no attempt to clarify when protection is available under the TI Act for stored messages. On the contrary, the Bill proposes to amend the TI Act to simply remove the prohibition against interception of emails and other stored messages for a period of 12 months (during which time the Attorney-General's Department will review the TI regime in light of technologies that have emerged over the past 25 years).

According to the Explanatory Memorandum to the Bill, emails and other stored messages – including messages that have not yet been received or read by their intended recipients – will be able to be opened and read by any person who has lawful access to either the message or the equipment on which the message is stored. Messages, no matter when they were sent or read, will be able to be accessed for a 12 month period after the Bill commences. The limitations in Part 7 of the TI Act on how intercepted messages can be used and disclosed will no longer apply.

If passed, the Bill will remove the restrictions in the TI Act that limit the purposes for which Internet Service Providers ("ISPs") and other carriers and carriage service providers can intercept messages. To date, the TI Act has generally limited service providers to intercepting messages only to the extent necessary to operate and maintain the service or to trace and identify the sender of offensive or harassing communications.

Carriers and carriage service providers will continue to be bound by the *Telecommunications Act 1997*. However, while section 276 of that Act generally prohibits carriers and carriage service providers from disclosing the content of messages, a number of exemptions exist in the Act to permit use and disclosure

For instance, the *Telecommunications Act* does not restrict use or disclosure of the content of messages where it is done by a carrier or carriage service provider in the performance of their duties as an employee of the carrier or carriage service provider or as a telecommunications contractor: s. 279(1). This Act does not limit these duties to operating and maintaining the telecommunications system. This authority to use and disclose messages, combined with the proposed exclusion of stored messages from the TI regime, might have the effect of permitting ISPs to routinely scan the text of their customers' emails for purposes such as ad placement, a practice that is currently the subject of controversy in the United States in relation to Google's proposed Gmail service. (See the joint letter by the World Privacy Forum and 30 other privacy and civil liberties organizations calling upon Google to suspend their Gmail service: www.privacyrights.org/ar/gmailletter.htm).

The *Telecommunications Act* also permits carriers and carriage service providers to disclose the content of communications with (and without) a warrant. Ordinary search warrants, however, are not as protective of privacy as TI warrants. Unlike TI warrants, the search warrant power is not limited to the investigation of serious offences; there is no requirement to consider the use of less intrusive means of investigation; and there is an absence of reporting or other accountability requirements.

Where a search warrant is executed at a remote location (eg, at an ISP's premises), there is unlikely to be any opportunity for the sender or recipient to know of, much less question, the scope or execution of the search warrant. This may allow for overly broad and indiscriminate access to all of a person's communications, whether they are relevant to the investigation or not, and potentially encompassing communications that would otherwise be protected from disclosure (eg, those that are subject to legal professional privilege).

It may be appropriate for search warrants to be used to access emails already read by the recipient and stored on a home computer, in the same way that access can be sought to letters in a desk drawer. It is not appropriate, however, that emails and other stored messages be accessed prior to their receipt, without the recipient's knowledge, and in the absence of the important safeguards that already attach to TI warrants.

Emails are a unique form of communication and in need of a high level of protection. Communication by email is fast becoming the norm and, for good reason, is being encouraged to become the norm. It is a form of communication that is quick and efficient, effortless and relatively inexpensive. An essential requirement for the development of a trustworthy and effective communications network is an assurance of appropriate privacy protection.

I refer to the Introduction in my March 2004 submission and reiterate my views that:

1 Privacy in respect of one's communications has long been recognised as a fundamental human right. This is reflected in international instruments dating back to the 1948 Universal Declaration of Human

Rights and the 1966 International Covenant of Civil and Political Rights, as well as in domestic legislation protecting the integrity of postal and other communications.

2 Telecommunications is one of the common means by which many individuals discuss their most private and intimate thoughts, as well as the ordinary daily details of their lives. They may also engage in political discourse, discuss business ventures, seek legal and other professional advice. People have a legitimate and reasonable expectation that the State will not listen surreptitiously to these conversations. Accordingly, any such interception has been subject to strict regulation under law, with oversight.

3 The telephonic exchange of personal, intimate and confidential communications is rapidly being superseded by the use of electronic technologies that, by their nature, leave a digital trail behind capable of being stored and later accessed. Email and SMS communications can perhaps be the most common examples. New communications technologies are appearing on the market all the time, such as mobile phone cameras and "Palm pilots". It is important that the privacy protection for the users of such devices is clear so that these parts of the information and communications technology sector of the economy can flourish.

4 Access to one's communications through the interception of telephone and electronic communications is unlikely to be detected by either the sender or recipient. Unlike a broken seal on an envelope or a hovering eavesdropper, interception can take place invisibly, during the transit of the communication and prior to its receipt. Since there is no opportunity for the subject of the surveillance to tests its validity under law, the procedural safeguards and independent oversight are especially important.

Finally, I note that the Attorney-General, the Hon. Philip Ruddock, stated in his second reading speech that his department would review the TI Act during this 12-month period to ensure that the legislation keeps pace with the changes in technology that have occurred since that Act was first in 1979. There is no commitment in the legislation, however, to carry out this review, nor is there any indication of its terms of reference, no requirement for public consultation, and no commitment to make public the review's findings and recommendations.

A review of the TI Act is to be welcomed, particularly in light of emerging and converging technologies, regulation of which appear to cross legislative and jurisdictional boundaries. For example, the use of mobile phones would generally be regulated by Commonwealth TI legislation, but technological enhancements that allow phones to be used as optical surveillance devices, storage devices for text and images, and broadcasting equipment capable of transmitting data to the internet pose challenges to the current regulatory framework. Jurisdictional challenges may also arise with respect to email monitoring – see, eg, NSW's draft *Workplace Surveillance Bill*, released in June 2004, which seeks to regulate workplace emails and internet access. It would be desirable for the review to proceed irrespective of whether the Bill is passed. Any such review should be open for public comment. Appropriate technical expertise should be sought. And the review's findings and recommendations should be made public prior to any further legislative change.

If the Committee requires any further information, please do not hesitate to contact Ms Michelle Fisher of my office.

Yours sincerely,

PAUL CHADWICK
Victorian Privacy Commissioner