ATTORNEY-GENERAL
THE HON PHILIP RUDDOCK MP

28 MAY 2007

07/2852
MC07/7558

Mr Mark Burgess
Chief Executive Officer
Police Federation of Australia
Level 1, 21 Murray Crescent
GRIFFITH ACT 2603

Dear Mr Burgess

I refer to your correspondence of 22 March 2007 regarding the *Telecommunications (Interception and Access) Bill 2007* (the Bill) and in particular, your concerns relating to the secondary disclosure of telecommunications data, and the use of this data for the purpose of police disciplinary proceedings.

While I appreciate this concern, in my view it is based on an incorrect interpretation of the operation of the law, if the Bill were passed.

As you may be aware, the relevant provisions of the Bill relate to the access, use and disclosure of telecommunications data, which is low-level data including call charge records and phone bills. This data does not include the actual content of telecommunications, which is regulated through existing provisions of the *Telecommunications (Interception and Access Act) 1979* (the TIA Act).

Primary and secondary disclosure of telecommunications information

The Bill will introduce a scheme for the secondary disclosure of telecommunications data. A primary disclosure of telecommunications data is one that is made by a telecommunications carrier or carriage service provider to a law enforcement or security body for the purposes of national security, a criminal investigation, the enforcement of a law that imposes a pecuniary penalty, or the protection of the public revenue.

A secondary disclosure of telecommunications occurs when the recipient of the primary disclosure passes that information on to another body.

Currently, the use and disclosure of lawfully accessed telecommunications data is regulated by the *Telecommunications Act 1997*. There are no provisions in this Act which permit an agency to disclose telecommunications data that it has lawfully received to another agency,

unless it is done in relation to the purpose of the primary disclosure. This prohibition extends to information which the second agency could have lawfully accessed from a carrier, if it was aware of the existence of the information.

The new legislation would not alter the threshold that must be met before an agency can lawfully access telecommunications data. However, the Bill proposes to create a new secondary disclosure provision that will allow enforcement agencies to disclose to another enforcement agency where it is reasonably necessary for the enforcement of the criminal law or law imposing a pecuniary penalty, or for the protection of the public revenue. In other words, this permits the secondary disclosure of information to an agency in circumstances where the receiving agency would itself have been able to access the information directly from the carrier.

You have indicated that the PFA is concerned that the new secondary disclosure provisions could lead to information being disclosed for the purposes of an investigation into alleged police misconduct, and that in your view this inappropriately applies a different standard to police officers than to the wider community.

This is only partially correct. It is possible that telecommunications data may be used in police disciplinary proceedings where, in a given jurisdiction, police disciplinary proceedings carry a 'pecuniary penalty'.

However, this is subject to three important caveats.

First, such secondary disclosure could only occur in circumstances in which the information could have been obtained under the primary disclosure rules.

Second, there is no specific provision enabling either the primary or secondary disclosure of telecommunications data relating to the investigation of police misconduct. As such, the Bill would not create any provisions that are not of general application to the wider community, including police officers.

Third, under the current legislation governing the employment of police in Australia, there is in fact little if any capacity to use this information in any police disciplinary investigations. This is by reason of the meaning of 'pecuniary penalty', which is limited to specific monetary penalties set out in relevant legislation and imposed by a court. The term does not include administrative sanctions that may have financial impact, such as for example, a demotion.

For these reasons, I am confident that the provisions proposed in the Bill do not contain any measures that single out police officers. Nor will they permit the general use of telecommunications data in police disciplinary proceedings, either on the basis of a primary or secondary disclosure.

Accordingly, I have decided to retain the provisions in the Bill in their current form.

Lawful disclosure of stored communications

In addition to the amendments which you have discussed, I note a proposed amendment to the stored communications regime of the TIA Act that also relates to police disciplinary proceedings.

The TIA Act provides that the chief officer of an agency may disclose lawfully intercepted information to another agency, where that information relates to a police disciplinary proceeding (section 68). However, it does not currently permit the similar disclosure of lawfully accessed stored communications to another agency. This change amounts to an alignment of the powers relating to the two categories of information.

It should be noted that within the TIA Act, 'police disciplinary proceeding' has a meaning limited by the definition in section 5 of the term 'proceeding', which requires a proceeding or proposed proceeding in the Federal Court, a state or territory court, or a tribunal, authority, body or person having the power to hear or examine evidence. This definition therefore excludes low-level purely internal administrative or managerial actions. While both disclosure provisions are specific to police officers, it should be emphasised that the information to be disclosed in relation to the police disciplinary proceeding must first have been obtained for the purposes of investigating a 'serious offence' sufficient to justify the issuance of a telecommunications interception warrant under sections 46 or 46A, or a 'serious contravention' sufficient to justify the issuance of a stored communications warrant under section 116.

Should you wish to discuss this issue further, the contact officer in this matter is Jonathan Curtis who can be contacted on (02) 6250 6359.

Yours sincerely

Philip Ruddock