



VICTORIA POLICE

Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013

Victoria Police is pleased to provide this submission to the Senate Committee on Legal and Constitutional Affairs Committee Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013 (the **Bill**). This submission is limited to commenting on the proposed amendments contained in the Bill which would directly impact upon Victoria Police.

Accordingly, this submission comments on the proposed amendments to the *Telecommunications (Interception and Access) Act 1979* (the **TIA Act**) which would introduce standard warrant authorisation procedures for requests for access to information or documents (non-content) (**telecommunications data**) for law enforcement purposes.

Victoria Police's existing access to telecommunications data

As an enforcement agency under the TIA Act, Victoria Police is able to access historical telecommunications data pursuant to section 178 of the TIA Act. Victoria Police has previously indicated the utility of this access in its submission to the Commonwealth Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) Inquiry into Potential Reforms of National Security Legislation:

The lawful use of non-content data such as subscriber information and call records accessed pursuant to section 178 of the TIA Act is crucial in terms of the intelligence and evidence gathering required before access to prospective information and/or a telecommunications interception warrant is applied for. It is a legislative requirement to demonstrate to an issuing authority that the suspect is utilising the particular telecommunications serve and the likelihood of evidence being obtained in relation to the targeted serious offence. Subscriber information and call records data is invaluable in this regard. All requests for access to such data are first approved by an officer authorised pursuant to section 5AB(1) of the TIA Act who is responsible for satisfying themselves the request meets the necessary thresholds. Victoria Police has stringent standards in terms of dealing with such information.

(See page 5 of the submission. A copy of the submission is publicly available on the Inquiry's website)

Further to the above comment, access to historical telecommunications data often provides exculpatory evidence, which then precludes the need to access prospective telecommunications data or apply for telecommunications interception warrants.

As a criminal law-enforcement agency under the TIA Act, Victoria Police is able to access prospective telecommunications data pursuant to section 180 of the TIA Act. The value of this access is synonymous with access to information or documents pursuant to section 178. Access to prospective information or documents may provide the further intelligence or evidence necessary to make an interception warrant application, or provide exculpatory evidence which then renders an interception warrant application unnecessary.

The current regime specifies that requests pursuant to sections 178 and 180 must be made by an agency head, deputy head or authorised officer, who must be satisfied that the access is reasonably necessary for the intended purpose. At Victoria Police, an authorised officer is a senior member who is at the rank of Inspector or higher.

Anticipated impacts of the proposed amendments

Victoria Police recognises and supports the importance of privacy principles and the need to ensure the privacy of communications. Victoria Police also recognises and supports the community expectation that alleged criminal offences are properly investigated and prosecuted.

However, as a result of the continually changing nature of crime and the increasing use of technology by the community, access to telecommunications data is increasingly invaluable in criminal investigations. Victoria Police recognises and supports the need for law enforcement agencies to have appropriate access to telecommunications data. Accordingly, Victoria Police does not support the Bill in its current form.

Victoria Police strongly submits that the requirements of the current regime are proportionate to the privacy impacts that follow from an agency receiving confirmation that a communication has or has not occurred, with no details of content.

Victoria Police has significant concerns about the negative consequences for the resourcing of and the effectiveness of investigations if the current 'authorisation' regime was replaced with a warrant regime as suggested by the Bill. The Annual Report compiled under the TIA Act for the year commencing 1 July 2011 and ending 30 June 2012 states that Victoria Police made 67,173 requests for access to existing information or documents pursuant to section 178 of the TIA Act and 787 requests for access to prospective information or documents pursuant to section 180 of the TIA Act. These figures may be compared with the 293 interception warrants obtained and the nine stored communications warrants obtained by Victoria Police during the same reporting period.

A warrant regime would be unduly onerous on investigators and hinder criminal investigations due to the considerable resources that are allocated to prepare a warrant application and to subsequently provide the application to the Victorian Public Interest Monitor and to an issuing authority. There would also be considerable resourcing implications for the Victorian Public Interest Monitor and issuing authorities including the Commonwealth Administrative Appeals Tribunal.

The level of resourcing that would be required to progress a warrant for access to telecommunications data is likely to not be proportionate to the intelligence or evidentiary value of the information that would be obtained. Further, the practical time delay that would result in progressing investigations would consequently reduce the number of investigations able to be pursued due to resources being less available.

The telecommunications content and data access regime has been subject to ongoing legislative reform due to the changing nature of technology. Victoria Police is aware that on 24 June 2013, that the PJCIS tabled its report entitled 'Report of the Inquiry into Potential Reforms of Australia's National Security Legislation'. The Report made recommendations in relation to a holistic review of the regime. This included a recommendation that the Commonwealth Attorney-General's Department review the threshold for access to telecommunications data (see recommendation 5).