



**Office of the Public Interest
Monitor**

PO Box 18198
Collins Street East, Victoria 8003
Telephone: (03) 9032 0666
Facsimile: (03) 9032 0699

**SUBMISSIONS OF THE PUBLIC INTEREST MONITOR (VICTORIA) IN
RELATION TO THE
‘REPORT OF THE INQUIRY INTO POTENTIAL REFORMS OF
AUSTRALIA’S NATIONAL SECURITY LEGISLATION’ BY THE
PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND
SECURITY**

The Public Interest Monitor (Victoria) seeks to make limited submissions in relation to aspects of:

- a. the recommendation of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly 71.2; and
 - b. recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia’s National Security Legislation* report, dated May 2013.
- a. **Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report**
- (i) The *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Telecommunications Act 1997* (Cth) continue to be effective, although the recommendations suggested in the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia’s National Security Legislation* report of May 2013 would strengthen the legislation and ensure it reflects changes in technological developments and also changing community perceptions and expectations in relation to law enforcement access to communications.
 - (ii) It is difficult to envisage general communications legislation subsuming the activities currently regulated under the TIA and TI Acts, as both of these Acts deal with matters particular to the telecommunications industry, including the issue of warrants and access to telecommunications data, which are specialised areas and need to be recognised as such.

(iii) The TIA Act should be amended to provide for the role of a Public Interest Monitor (hereinafter referred to as PIM) at the Commonwealth level. The Parliamentary Joint Committee on Intelligence and Security placed considerable emphasis on oversight, reporting and monitoring although did not address the issue of a PIM. The introduction of a PIM would provide an additional level of scrutiny prior to the issue of a warrant, strengthening the process of obtaining warrants particularly in relation to privacy issues and providing the community with a greater sense of security that a PIM is raising matters in the public interest and ensuring compliance with the legislative criteria by monitoring the activities of those to whom warrants are issued who are charged with investigating serious crime and national security matters. The role of a PIM is not to usurp that performed by the issuing officer, but rather to assist the issuing officer in determining the application, in the form of a contradictor.

b. Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013

(i) Recommendation 1

The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:

- **expresses the dual objectives of the legislation –**
 - ⇒ **to protect the privacy of communications;**
 - ⇒ **to enable interception and access to communications in order to investigate serious crime and threats to national security; and**
 - **accords with the privacy principles contained in the *Privacy Act 1988*.**
- a) The PIM supports the inclusion of the objectives clause into the TIA Act, specifying the dual objectives of the legislation and highlighting the importance of the protection of the privacy of communications, particularly in an era when telecommunications services are utilised widely for forms of communication not limited to verbal communication. The importance of the protection of the privacy of communications needs to be specifically considered in each application for a warrant under the TIA Act with reference to the particular facts of the investigation in relation to which the warrant is sought and balanced against the need to utilise the investigative tools available under the TIA Act to law enforcement agencies and those charged with investigating serious crime and threats to national security.

(ii) **Recommendation 2**

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the:

- **privacy impacts of proposed investigative activity;**
- **public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and**
- **availability and effectiveness of less privacy intrusive investigative techniques.**

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

- a) The factors to be considered in the proposed proportionality tests are extremely important factors, which need to be balanced with the need to utilise intrusive investigative tools available under the TIA Act to fight serious crime and threats to national security. Factors such as the privacy impacts of the proposed investigative activity and the availability and effectiveness of less privacy intrusive investigative techniques should be considered on a case by case basis and more particularly, with reference to the specific facts of the case before the issuing authority.
- b) Adopting a one size fits all approach when dealing with issues of privacy without actually turning ones mind to the precise impacts on privacy in the context of that particular investigation is not consistent with the requirement for an issuing authority to consider the impact on privacy of the proposed investigative activity in relation to the particular investigation in respect of which the warrant is sought.
- c) The availability and effectiveness of less privacy intrusive investigative techniques is important in assessing whether a warrant authorising the interception of communications should be issued, particularly when other less intrusive methods of investigation are available although have not yet been utilised. Telecommunications interception warrants should not be utilised by law enforcement agencies as the initial starting position for an investigation or the fall back position when other investigative methods may yield significant evidentiary material yet have not been undertaken, such as detailed financial analysis etc.

(iii) **Recommendation 3**

The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

- a) An evaluation of whether the privacy intrusion was proportionate to the public outcome sought may be beneficial, although the current reporting requirements do address this to some extent. Lawfully intercepted information may also be disseminated to another interception agency for the purpose of an investigation that other agency is undertaking. Although the lawfully intercepted information may not have assisted the original LEA to whom the warrant was issued, it may have significantly assisted another LEA in their investigation, which would not necessarily be reflected in such a reporting requirement. To obtain a more accurate reflection of the true value of this information, law enforcement agencies to whom lawfully intercepted information is disseminated would also need to report on this issue.

(iv) **Recommendation 4**

The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*.

- a) Effective accountability should encompass many factors in the process of seeking the issue of a warrant, including the application to an issuing authority and the storage and use of lawfully intercepted information, including information which is intercepted under a warrant but not utilised to further the investigation.
- b) Lawfully intercepted material is not limited to communications relating to the offences the subject of the investigation and often a considerable amount of material is harvested under a warrant which investigators/support persons must sift through to ascertain the relevance of the communications to the investigation. The other material, although intercepted under the warrant but deemed not relevant to the investigation may also be retained. Such information is usually stored on an agency's system and not destroyed until after the expiration of any appeal period if the matter reaches court. Whilst there are valid reasons for retaining this information, such as an assertion during a trial that a particular conversation relied upon by the prosecution as having a certain meaning does not have that meaning when viewed in the context of three or four surrounding conversations, the storage and management of this material should be the subject of specific legislative provisions.
- c) Further use of lawfully intercepted information which may not be readily identifiable as such needs to be addressed in any revised reporting

requirements. Such information can also be found in other documents such as information reports and case notes, whether in summary form or otherwise. The storage and reporting requirements of the legislation need to ensure this material is handled appropriately, destroyed at a particular time or if its retention is required, legislative mechanisms for its retention need to be particularised, to ensure the recognition of this information as lawfully intercepted information and to ensure it is dealt with as such.

Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.

- d) Oversight is currently performed by Commonwealth and State bodies, such as the Commonwealth Ombudsman and the Victorian Inspectorate. The records of Victorian law enforcement agencies such as Victoria Police and IBAC are inspected by the Commonwealth Ombudsman in relation to stored communications warrants. As such, oversight is fragmented and there is not a single oversight mechanism, which may result in insufficient oversight, issues not being detected and inconsistencies in the oversight due to differing processes or requirements by the oversight bodies.
- e) As stated in paragraph a(iii) above, a PIM at the Commonwealth level would provide an additional level of oversight or scrutiny prior to the issue of a warrant.

The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.

- f) Such consultation is supported as it is extremely important. At present, the State legislation does not refer to stored communications warrants, but only telecommunications interception warrants.
- g) Consideration and consultation should also be undertaken in relation to the extension of warrants obtained under the TIA Act to enhance operational efficiencies and simplify the application process for further TI warrants where a warrant is already in existence. When the TIA Act was first drafted, it may not have been envisaged that the duration and complexity of investigations undertaken by law enforcement agencies would be as intensive and time consuming as they are in the current environment. Providing law enforcement agencies with a mechanism through which to have a warrant extended may be beneficial.

(v) **Recommendation 5**

The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

- a) There has been recent media attention and significant criticism of the ability of agencies to obtain telecommunications data and the consequential implications on the privacy of those who utilise telecommunications services. Local councils can access telecommunications data under the TIA Act on the basis that disclosure of the said data is reasonably necessary for the enforcement of a law imposing a pecuniary penalty. The matters in respect of which telecommunications data is obtained by some agencies does not appear commensurate with the invasion of privacy occasioned by the disclosure of such data. A reduction in the number of agencies able to access telecommunications data by using the gravity of the conduct which may be investigated utilising telecommunications data as a threshold on which access is allowed is supported.

(vi) **Recommendation 6**

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- **privacy impact of the threshold;**
- **proportionality of the investigative need and the privacy intrusion;**
- **gravity of the conduct to be investigated by these investigative means;**
- **scope of the offences included and excluded by a particular threshold; and**
- **impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.**

- a) The PIM supports this recommendation as the threshold for accessing the content of communications under the authority of a stored communications warrant is low and enables agencies who are not 'interception agencies' as defined in the TIA Act to access communications that have "passed over" the telecommunications system. Such data includes emails and SMS messages, thus remains a considerable intrusion on privacy, which may not be proportionate to the gravity of the offence being investigated.
- b) An enforcement agency can seek access under warrant to stored communications. An enforcement agency includes any body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. The distinction between communications that are "passing over" and those that have "passed over" should no longer be retained as discussed further at paragraph b(ix).

(vii) **Recommendation 7**

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model ‘attribute based interception’ on the existing named person interception warrants, which includes:

- **the ability for the issuing authority to set parameters around the variation of attributes for interception;**
- **the ability for interception agencies to vary the attributes for interception; and**
- **reporting on the attributes added for interception by an authorised officer within an interception agency.**

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

- **attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;**
- **oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and**
- **reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.**

- a) The concept of attribute based interception is attractive and would appear to provide law enforcement agencies with a more reliable and efficient method by which to obtain information relevant to the investigation of serious crime and national security matters. Enabling an issuing authority to issue a warrant permitting the interception of any communications made by a particular person would assist law enforcement agencies in accessing information which may be relevant to the investigation in respect of which the warrant is sought.
- b) Although the concept is attractive, as a matter of practicality, it is unclear exactly how such a warrant would operate. The issue of an attribute based interception warrant potentially widens the net of available information, which also increases the impact on the privacy of those the subject of the warrant and other individuals who may contact/be contacted by that person. All of the information intercepted under the warrant would need to be provided to the applicant agency, to determine relevance, potentially increasing the amount of

irrelevant material that is also provided to the applicant agency. Rigorous use, storage, retention and dissemination provisions would be required to govern appropriate dealings with this information, particularly information that is not deemed relevant to the investigation but nevertheless stored on an applicant agencies data storage systems.

- c) Enabling interception agencies to add specific attributes to the warrant post the issue of the warrant on the authority of an authorised officer of the interception agency would also need to be subject to specific and rigorous legislative requirements similar to those an issuing authority must have regard to when issuing the warrant. The legislation would need to ensure that a lesser threshold with respects to checks and balances to verify the information seeking the addition of another attribution through internal agency authorisation was not permitted and did not occur, due to the significant invasion of privacy and the extension of the breadth of information available to an agency under the one attributed based warrant, which would not require the presentation to an issuing authority of further information in relation to the additional attribute. The same level of scrutiny issuing authorities are required to bring to bear on applications for the issue of warrants should be imposed on internal authorised officers, requiring the applicant to meet certain specified legislative criteria in a written application before the authorised officer can authorise the addition of another attribute. Requiring a written application would also ensure that those charged with the oversight of attribute based interception can make an informed and accurate assessment as to the appropriateness of the enabling of any additional attribute post the issue of the warrant and provide accurate reports, in the absence of involvement by an issuing authority after the warrant has been issued.

(viii) **Recommendation 8**

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure:

- **protection of the security and privacy of intercepted information; and**
 - **sharing of information where necessary to facilitate investigation of serious crime or threats to national security.**
- a) Review of the information sharing provisions is important to ensure that material obtained under the TIA Act is properly used, stored and disseminated. The information sharing provisions should also permit sharing of information to agencies which are not themselves interception agencies in certain circumstances, where the gravity of the alleged offence/conduct is significant, such as to Corrections Victoria in relation to an allegation of corruption by a staff member. The legislative provisions would also need to address how a recipient agency who is not an interception agency uses and stores this information and also whether (and in what circumstances) the recipient agency may disclose and/or disseminate that information.

- b) The legislative provisions in relation to information sharing need to be particularised to ensure there is no ambiguity and information sharing provisions should also specify what responsibilities agencies with whom the information is shared have in relation to reporting, use, storage, retention and destruction of the information, including any derivative information such as a summary, an information report or a case note.

(ix) **Recommendation 10**

The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunication (Interception and Access) Act 1979* be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features:

- **a single threshold for law enforcement agencies to access communications based on serious criminal offences;**
- **removal of the concept of stored communications to provide uniform protection to the content of communications; and**
- **maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.**

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- **interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;**
 - **rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;**
 - **reporting by law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and**
 - **Parliamentary oversight of the use of interception.**
- a) A single warrant regime incorporating the current stored communications warrants would be beneficial. With societal change in the preferred methods of communication and a greater emphasis on the use of SMS' and emails and the advancements in technological developments relating to telecommunications services, there is no reason that the distinction between lawfully intercepted information and stored communications information should be retained. The impact on privacy is significant regardless of whether a communication is "passing over" or has "passed over" a telecommunications service.

- b) The threshold for access to such information should be increased and law enforcement agencies investigating offences in relation to which the penalty is the imposition of a pecuniary penalty should not necessarily be entitled to access stored communications information. Although such agencies should retain the ability to access telecommunications data, they should not be permitted to obtain stored communications information due to the impact on privacy where the subject matter of the inquiry does not relate to serious criminal offences or national security matters.
- c) Rigorous oversight is also important, although oversight post the issue of a telecommunications interception warrant may be viewed as less effective than scrutiny prior to the issue of such a warrant. The introduction of a Public Interest Monitor at a Commonwealth level would provide additional oversight prior to the issue of any warrant, which would only enhance any rigorous oversight procedures adopted post the issue of a warrant. The current oversight mechanisms do not address the issue of deficiencies or concerns in an application, impacting on the issue of whether a warrant should be issued, as the focus is on inspection post the issue of the warrant for limited purposes, namely to ensure the agency is dealing with material obtained under the warrant in accordance with the legislation. A system whereby scrutiny occurred during the application process before the warrant was issued coupled with robust oversight post the issue of the warrant is preferable to that current in place.

(x) **Recommendation 18**

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:

- **clear protection for the privacy of communications;**
- **provisions which are technology neutral;**
- **maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;**
- **clearly articulated and enforceable industry obligations; and**
- **robust oversight and accountability which supports administrative efficiency.**

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:

- **Independent National Security Legislation Monitor;**
- **Australian Information Commissioner;**
- **Ombudsmen and the Inspector-General of Intelligence and Security.**

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

- a) The PIM supports such a review, to bring the legislative provisions of the TIA Act into line with technological advancements and also with changing community expectations in relation to the protection of the privacy of individuals, upon which the powers available under the TIA Act can be a significant intrusion. Such a review should ensure that agencies who do not need access to telecommunications information such as that obtained under a stored communications warrant can not access that information and that limited access is provided to telecommunications data, commensurate or proportionate to the gravity of the alleged offence being investigated.
- b) Oversight is important prior to the issue of a warrant under the TIA Act and also post the issue of the warrant, in relation to interception agencies adequately fulfilling reporting requirements and obligations in relation to the use, dissemination, storage and destruction of product obtained under a warrant. Any reduction in the reporting requirements due to what law enforcement agencies perceive as being administrative burdensome needs to be borne in mind against the significantly intrusive investigative tools provided by the TIA Act. A reduction in reporting requirements is not necessarily supported, particularly if a move towards an attribute based warrant is envisioned, which provides a law enforcement agency with increased interception powers controlled internally post the issue of a warrant and should be the subject of greater accountability and oversight.

Brendan A Murphy QC
Principal Public Interest Monitor

28 February 2014