



Inquiry into comprehensive revision of *Telecommunications (Interception and Access) Act 1979*

Submission to the Senate Legal and Constitutional Affairs References Committee

February 2014

The Independent Commissioner Against Corruption (“ICAC”) makes this submission to the Senate Legal and Constitutional Affairs Committee in response to the call for submissions concerning the inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

As ICAC is a relatively new interception agency with limited operational experience with the TIA Act this submission makes brief observations and comment on the TIA Act in response to the recommendations of the *Australian Law Reform Commissioner (“ALRC”) For Your Information: Australian Privacy Law and Practice report*, dated May 2008, namely recommendation 71.2, (“the ALRC report”) and the recommendations from the Parliamentary Joint Committee on Intelligence and Security into the potential reforms of Australia’s National Security Legislation report (“the PJCIS report”).

Introduction

The Independent Commissioner Against Corruption was established on 1 September 2013 by the *Independent Commissioner Against Corruption Act 2013* (the ICAC Act).

The functions of the ICAC include;

- to identify and investigate corruption in public administration
- to assist in identifying and dealing with misconduct and maladministration in public administration
- to prevent or minimise corruption, misconduct and maladministration in public administration through education and evaluation of practices, policies and procedures.

The primary object of the Commissioner is to investigate serious or systemic corruption in public administration and to refer serious or systemic misconduct or maladministration in public administration to the relevant body. The ICAC has powers to assume powers of inquiry agencies and conduct investigations into misconduct or maladministration in public administration.

The ICAC is a declared agency for the purposes of the TIA Act. ICAC does not have its own technical telecommunications interception capability, but relies upon an agreement with another agency to access capacity. Other agencies can provide lawfully intercepted information and interception warrant information to the ICAC where that information relates or appears to relate to a matter that may give rise to an investigation by the ICAC.

The ICAC has a suite of investigative powers in recognition of the particular challenges involved in investigating corruption in public administration. Those challenges include the familiarity that some subjects of investigations may have with investigative techniques which enables them to hide their activities or frustrate investigations.

Amongst other investigative powers, the ICAC has power to obtain information coercively, through search warrants, notices to produce documents, production of written statements of information about a specified matter and to summons a person to appear before an examination to give evidence and to produce documents. Not all evidence obtained at an examination will necessarily be admissible in subsequent criminal proceedings. The ICAC Act provides that evidence obtained at an examination will not be admissible against a person in a criminal proceeding where a person has claimed that the answer to a question that they are required to answer might tend to incriminate the person or make them liable to a penalty.

Access to telecommunications data and lawfully intercepted communications is considered a vital tool in investigations into serious corruption offences, which is capable of enhancing the effectiveness of other investigative techniques and in the case of intercepted communications, is likely to obtain direct admissible evidence that cannot otherwise be obtained through other methods of investigations.

Recommendation 71-2 (e) from the ALRC report: Whether the Telecommunications (Interception and Access) Act should be amended to provide for the role of a public interest monitor.

The ICAC supports a review of the TIA Act to ensure it provides appropriate accountability, but the case for a public interest monitor is not convincing. The TIA Act presently strikes a balance between the two competing public interests being the public interest in advancing investigations of serious offences and the public interest in protecting a person's privacy. The TIA Act does this by *only* permitting such privacy incursions for investigations of serious offences, where other investigative techniques are unlikely to provide the information sought.

Recommendations in the PJCIS report

Recommendation 5: That the AGD review the threshold for access to telecommunications data, reduce 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.

Telecommunications data is a very useful investigative tool particularly for covert investigations as it can be used to establish connections and relationships. The data can assist in determining the identity of persons and their whereabouts. The access and use of telecommunications data does not involve the same degree of privacy incursion compared to interception of telecommunications. The data can only be accessed in restricted circumstances and is subject to similar restrictions on use and further communication. The ICAC does not support warrant based access to telecommunications data.

Recommendation 8: Review of the information sharing provisions of the TIA Act 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.**

Other interception agencies can provide lawfully intercepted information and interception warrant information to the Commissioner where that information relates or appears to relate to a matter that may give rise to an investigation by the ICAC. The present scheme that facilitates the sharing of information tends to be inefficient and could be detrimental in time critical situations.

The TIA Act permits the Commissioner to provide intercepted information and interception warrant information to other officers in ICAC in the circumstances prescribed in the TIA Act. In this way lawfully intercepted information provided to the Commissioner by another agency can then be provided to ICAC investigators as appropriate.

In practice it means that SA Police cannot provide a full briefing of a matter involving a potential issue of serious corruption in public administration to the ICAC investigators where that briefing contains intercepted information. Either the briefing must omit the lawfully intercepted information, or the briefing must be given only to the Commissioner who may then provide the intercepted information to the ICAC investigators in accordance with s67 of the TIA Act.

The current prescriptive approach is inefficient from an operational perspective. The ICAC considers that there is a clear need for a scheme that allows for the efficient sharing of information between agencies whilst retaining existing protections relating to the secondary use of such material.

A scheme that facilitates the sharing of information should also ensure that information can then be used for the purpose for which it was disclosed in a consistent manner. The following demonstrates the need for review of the provisions that deal with both the sharing of information and the permitted uses of that information once it is received.

A permitted purpose, for a Police Force of a State, includes "an investigation of, or an inquiry into, alleged misbehavior, or alleged improper conduct, of an officer of that State, being an investigation or inquiry under a law of that State or by a person in the person's capacity as an officer of that State" and a report into such an investigation or inquiry. The permitted purpose is couched in terms sufficiently wide to encompass misconduct of an officer of the State. The definition of officer of the State is not exhaustive, but is sufficiently wide to capture a number of public officers, including police officers.

A Police Force of a State which has intercepted information relevant to an investigation of misconduct by a Police officer is permitted to use that information for that purpose, pursuant to s67 of the TIA Act.

Section 68 of the TIA Act permits an agency to communicate intercepted information and telecommunications data to the ICAC, where the information relates, or appears to relate "to a matter that may give rise to an investigation by the Independent Commissioner Against Corruption". It is important to note that the words do not limit investigations to investigations relating to corruption in public administration. As the ICAC can investigate alleged misconduct by an officer of the state where the ICAC exercises the powers of an inquiry agency, it appears that an interception agency, such as SA Police, may be permitted to provide intercepted information that relates to alleged misconduct of an officer of the state to the ICAC.

However, even if the intercepted information is communicated to the ICAC and done so lawfully, the ICAC cannot use the information obtained for the purposes of a misconduct investigation as the definition of permitted purpose in relation to ICAC is limited to an investigation into corruption in public administration or a report on such an investigation.

This limitation creates the odd result that SA Police is permitted to provide to the ICAC information that the ICAC cannot use, and that SA Police is permitted to use intercepted information in connection with a misconduct investigation of a police officer, whereas it cannot be used for such an investigation where that investigation is carried out by the ICAC.

The ICAC supports a review of the manner in which information sharing between agencies can be facilitated and how that information can then be used.

Recommendation 18: Revision of the interception regime.

There is a clear need for the TIA Act to be comprehensively revised. The ICAC supports recommendation 18 and in particular the release of a draft TIA Act for public consultation.

Recommendation 42: Mandatory data retention.

As carriers determine the duration that data is retained, the time that elapses before the data is destroyed varies between carriers. The ICAC supports a legislated data retention requirement to ensure there is a consistent minimum practice across carriers or carriage services which will preserve the ability to access and analyse telecommunications data.