Australian Government

Australian Commission for
Law Enforcement Integrity

Senate Legal and Constitutional Affairs Committee

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

Submission by the Australian Commission for Law Enforcement Integrity

27 February 2014

1. Executive Summary

The use of communications-based investigation methods is a critical element of the Australian Commission for Law Enforcement Integrity (ACLEI) investigative capability, particularly given the knowledge and resilience of many of the subjects of ACLEI investigations. ACLEI's capability in this area is based, as in other areas of ACLEI's work, on partnership. By working with larger partner agencies, ACLEI is able to implement its own capability cost-effectively and efficiently.

Despite being a 'small-user', it is apparent from ACLEI's experience that the present legislation struggles to adapt to the methods that criminals and corrupt officials use technology, including how counter-measures are used to defeat the capture of evidentiary material.

As indicated in its submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into potential reforms of National Security Legislation, ACLEI considers that there would be merit in moving towards a multi-purpose, single warrant system that:

- retains independent authorisation at the commencement of an interception operation, with provision for independent authorisation of extensions;
- is target- or attribute-based, rather than technology-based;
- "matches measures to risks" and responds better to the organised crime "partition" model, for instance by adjusting the range of criminal penalty offences that establish the thresholds for warrant approval;
- is flexible, allowing investigators to respond to rapidly-changing operational circumstances, within set limits and in ways that provide for accountability after-the-fact (whether by post-inspection, or through the warrant extension process);
- simplifies procedures for sharing information, subject to appropriate safeguards, across multi-agency task-forces and other similar arrangement, as well as in emergency situations; and
- updates accountability mechanisms to be privacy-focussed, rather than process-focussed.

In addition, ACLEI considers that it would be appropriate that a revised TIA Act would:

- provide clear and consistent requirements for the retention of telecommunications data;
- subject to appropriate safeguards, permit the use of telecommunications data for disciplinary and misconduct proceedings;
- permit the sharing of source de-identified non-personal information derived from telecommunications content between law enforcement bodies;
- permit the use of telecommunications content to support unlawful disclosure prosecutions and in emergency situations; and
- where legislation provides for integrity and law enforcement agencies to undertake integrity testing operations, to permit the obtaining of an interception warrant for the purposes of such operations.

2. Introduction

ACLEI welcomes the opportunity to make a submission to the Senate Legal and Constitutional Affairs Committee (the Committee) concerning its *Inquiry into comprehensive revision of the Telecommunications (Interception and Access) Act 1979*.

To assist the Committee, Part 3 of this submission provides brief background about ACLEI and its role and responsibilities. Part 4 discusses ACLEI's experience as a user of telecommunications-based law enforcement powers and authorities in relation to:

- the importance of ACLEI (and anti-corruption agencies more generally) having access to telecommunications data and content as a critical tool to identify and investigate corruption issues;
- ACLEI's use of, and arrangements regarding, telecommunications data and content; and
- potential areas to strengthen the framework, to maintain and improve the effectiveness of these tools while ensuring appropriate safeguards to their use.

ACLEI, in 2012, made a submission to the Parliamentary Joint Committee on Intelligence and Security in relation to its inquiry into potential reforms of National Security Legislation. That submission, which comments on a number of issues relevant to this inquiry, is included for the Committee's information of at **Appendix 1**.

3. Role and responsibilities of ACLEI

The office of the Integrity Commissioner, and ACLEI, are established by the *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act).

ACLEI's primary role is to investigate law enforcement-related corruption issues, giving priority to serious and systemic corruption. Six agencies are presently subject to the Integrity Commissioner's jurisdiction under the LEIC Act, namely:

- the Australian Crime Commission (ACC), and the former National Crime Authority;
- the Australian Customs and Border Protection Service (ACBPS);
- the Australian Federal Police (AFP);
- the Australian Transaction Reports and Analysis Centre (AUSTRAC);
- the CrimTrac Agency, and
- prescribed aspects of the Department of Agriculture—presently the Secretary; staff members whose duties include undertaking assessment, clearance or control of vessels or cargo imported into Australia; who have access to the Integrated Cargo System; or who are holding or acting in the position of Regional Manager.

ACLEI is authorised under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to receive information about any corruption issue involving an agency within the LEIC Act jurisdiction that may be identified by other integrity agencies or law enforcement agencies as a result of their telecommunications interception activities. ACLEI's use of telecommunications data and content is discussed in more detail under Part 4.

ACLEI's role and responsibilities are described further at Part 2 to **Appendix 1**.

4. ACLEI's experience

4.1 The importance of telecommunications data and content to ACLEI

In ACLEI's experience, telecommunications interception and access to telecommunications data are invaluable tools for investigating corruption within Australian law enforcement agencies.

The information collected by these means may provide direct evidence—which would be impractical to obtain in any other way—of the commission of serious criminal offences. These methods—when combined with the Integrity Commissioner's coercive information-gathering powers (for instance, to hold a compulsory hearing)—can help to uncover complex corruption and serious crime that otherwise would remain hidden.

Case Study 1: Operation Heritage

ACLEI's recent Operation Heritage—in which five corrupt officers of the Australian Customs and Border Protection Service (ACBPS) and one from the Department of Agriculture were identified and prosecuted—demonstrates the utility and efficacy of telecommunication-based investigative tools for corruption investigations. A further 18 people, including some with connections to serious and organised crime groups, have also been prosecuted as a result of the investigation. A number of other ACBPS officers also resigned while subject to code of conduct proceedings.

During the course of this Operation—which was conducted jointly with the ACBPS and the AFP—ACLEI used access both to telecommunications data and to telecommunications interception to further the investigation. Telecommunications data, under a proper authorisation under the TIA Act, was used to trace and connect persons in the corrupt network, and to identify additional conspirators. Once persons of interest were identified, the content of telecommunications between the corrupt officers and their associates was intercepted, to inform the taking of investigative steps, to catch offenders 'in the act', and to provide evidence of the commission of offences. The Integrity Commissioner considers that telecommunications interception was critical to the successful outcomes of the investigation.

Operation Heritage illustrates how both data and content are used to support corruption investigations, and demonstrates the value of this tool for anti-corruption agencies.

4.2 ACLEI's current capability arrangements

4.2.1 Telecommunications interception

ACLEI is an intercepting agency for the purposes of the TIA Act, meaning certain designated staff members can apply to judicial officers, on ACLEI's behalf, for warrants to intercept communications and access stored communications.

ACLEI does not possess a dedicated technical telecommunications interception capability, and is unique among Commonwealth intercepting agencies in this regard. ACLEI has agreements with other Commonwealth law enforcement agencies to access capacity from time to time under their interception platforms to enable interception of ACLEI warrants. When ACLEI is granted a telecommunications interception warrant, access to content is facilitated through the intercepting agency, whose staff have been approved by ACLEI (under section 55 of the TIA Act) to exercise the authority conferred by warrants issued to ACLEI.

These arrangements enable ACLEI to access telecommunications content efficiently and cost-effectively. Without such arrangements, it would be unlikely that ACLEI could afford a similar dedicated capability.

ACLEI recognises that the use of such shared services may present some risks, and takes steps to ensure both that the integrity of investigations is not compromised and that telecommunications content remains appropriately protected. As an example of the ways in which ACLEI actively manages such risks, arrangements to access interception capabilities are in place with more than one agency—allowing ACLEI to respond appropriately to the disposition of individual investigations.

Telecommunications interception is a tool used, when appropriate, by ACLEI in its investigations into the most serious corruption issues. The predicate offence for the majority of warrants sought by ACLEI is the offence of *Abuse of Public Office* under section 142.2 of the *Criminal Code* (Cth), which is a serious offence for the purposes of section five of the TIA Act. This offence operates as a carve-out from the general rule for serious offences being offences of certain prescribed types and which carry a term of imprisonment of at least seven years. Content intercepted under warrant is used by ACLEI to advance its investigations into corrupt conduct, and ultimately to provide evidence for prosecution and certain disciplinary proceedings.

4.2.2 Use of Telecommunications Data

ACLEI is an enforcement agency for the purposes of the TIA Act. This arrangement means that designated ACLEI staff members can authorise the disclosure of specified historical information or documents when the ACLEI staff member is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

Since ACLEI is also a criminal law-enforcement agency under the TIA Act, designated ACLEI staff members can, in certain circumstances, authorise the prospective disclosure of specified information or documents that come into existence during the period for which the authorisation is in force. An officer can only make such an authorisation where he or she is satisfied that the disclosure is reasonably necessary for the investigation of a serious offence under the TIA Act or an offence punishable by imprisonment for at least three years.

ACLEI uses telecommunications data in corruption investigations in a variety of ways, often in combination with information collected by other means. For instance, telecommunications traffic data may be used to identify the extent of criminal and corrupt networks, and to identify the location of particular people at times when communications occur. Similarly, subscriber data may be used to verify the identity of particular persons of interest, such as the parties to particular conversations of interest or parties in regular contact, and to locate a residential or business address of a person of interest. Authorisations for the disclosure of telecommunications data are in practice operation- or investigation-specific, and are considered on a case-by-case basis to ensure the requirements of the TIA Act are met.

4.2.3 Accountability

ACLEI is subject to the reporting and accountability mechanisms of the TIA Act, in the ordinary way. In respect of warrants, this accountability regime includes regular inspections of ACLEI's interception practices by the Commonwealth Ombudsman.

4.3 Opportunities for strengthening arrangements

4.3.1 Telecommunications data

ACLEI considers that the current scheme for access to telecommunications data for law enforcement purposes is, with two exceptions, generally appropriate and fit for purpose.

Mandatory retention period

ACLEI sees merit in a legislated data retention requirement on telecommunications service providers, which would provide clarity as to how long a period of time service providers will retain telecommunications data, and ensure that such data can be properly accessed for law enforcement purposes. This data is already in the possession of service providers for their usual business practices, such as billing, which is generally destroyed after a short period of time.

It is important to note that the powers given to ACLEI (or indeed, any other criminal law-enforcement agency) under the TIA Act in respect of telecommunications data do not require service providers to take proactive steps to gather or retain information that the provider would not otherwise already hold. Additionally, the current regime for telecommunications data does not permit indiscriminate access by law enforcement agencies to bulk data. A mandatory retention period would require service providers to delay destruction of such data at least and until a specified period of time had elapsed, to enable recovery of relevant data for law enforcement purposes.

Case Study 2: Lack of data retention

In a recent ACLEI corruption investigation, it appeared that sensitive information about a law enforcement agency may have been unlawfully disclosed to a third party by use of an anonymous website contact form.

ACLEI was able to identify the IP address of the computer from which the alleged unlawful disclosure had been made, but when ACLEI sought to match the IP address to a particular internet user, the relevant internet service provider advised that—in accordance with usual business practices—the information had been destroyed when it was no longer necessary. There were no other means available to ACLEI to match the IP address to a person.

If the service provider had been under an obligation to keep its telecommunications data for more than a few months, the data might have been available to ACLEI for the purposes of the corruption investigation.

Permitted use—misconduct and disciplinary proceedings

ACLEI considers that telecommunications data, once properly and lawfully obtained for a criminal investigative purpose, should be able to be used for public sector misconduct and disciplinary proceedings.

ACLEI also considers that both telecommunications data and content should be permitted to be used for disciplinary purposes against persons in agencies overseen by designated integrity agencies.

ACLEI does not consider that telecommunications data should be able to be sought for a purely disciplinary purpose.

As an example, ACLEI can see a case for such material being relevant in disciplinary proceedings initiated against a law enforcement officer for failing to report contact with criminal identities, where the proof of contact may rely upon telecommunications data—obtained as part of an investigation into the criminal identity—showing the fact of contact. In such cases, ACLEI considers that the public interest in maintaining and upholding the integrity of law enforcement or the public sector would outweigh concerns about privacy.

4.3.2 Telecommunications content

Permitted use—de-identified information

The present telecommunications regime places strict limits on the use of intercepted content and warrant information and, in general, ACLEI considers those limits are reasonable. ACLEI raises a few issues for consideration in a revised interception regime, to improve appropriate information-sharing and use of intercepted content.

Presently, all intercepted content and warrant information is prohibited from onward disclosure, save for prescribed exceptions. This situation remains the case for all material obtained or related to an interception warrant, even if the material is de-identified as coming from a TIA Act warrant and/or contains no personal information about any identifiable person. The present restrictions in the TIA Act would, for example, prevent the Integrity Commissioner passing intelligence to other agencies about criminal and corruption methodologies employed by criminal entities, if they were observed in material obtained from TIA Act warrants properly granted for corruption investigations.

ACLEI suggests that the privacy considerations which properly limit the disclosure of personal information derived from or related to a TIA Act warrant shold not apply with the same force when material is non-personal in nature and the source is de-identified. Accordingly, ACLEI proposes that any new information-sharing regime should permit the sharing of source de-identified non-personal information between law enforcement bodies.

Permitted use—unlawful disclosure prosecutions

Once obtained, intercepted content and warrant information can be used by agencies for the investigation and prosecution of 'prescribed offences' within the meaning of the TIA Act, which at the low end, includes offences punishable by imprisonment for a period of at least three years.

The experience of integrity agencies has been that sensitive law enforcement information is a key commodity sought by criminal groups. However—at the Commonwealth level at least—offences criminalising the unlawful disclosure of information by officials tend only to carry a maximum term of imprisonment of two years, such as under section 70 of the *Crimes Act 1914*. Accordingly, intercepted content and warrant information cannot be used to prosecute these offences, or to seek a warrant relating to such criminal conduct.

Case Study 3: Inability to use evidence

In a recent corruption investigation conducted by ACLEI, evidence of an unlawful disclosure by a Commonwealth official was obtained by way of a properly granted TIA Act warrant. Since the alleged offence was below the statutory threshold, the material collected could not be used to found a prosecution for that offence.

There being no evidence, other than the intercepted content, ACLEI was inhibited as to the actions it could take in respect of the unlawful disclosure.

ACLEI considers that there is a demonstrated need for telecommunications interception in the investigation of information and data leaks—at least for the information to be able to be used for such purposes once obtained under another basis, if not also as the basis to found a warrant. Any future information-sharing regime should permit use of intercepted content and warrant information to be used for the investigation and prosecution of unlawful disclosure offences.

Permitted use—emergency situations

ACLEI also considers that a new information-sharing regime could usefully allow, clarify or put beyond doubt the ability of integrity agencies to use intercepted content and warrant information for purposes including the prevention of serious harm to any person in emergency situations.

Integrity testing

ACLEI considers that, where legislation[1] provides for integrity and law enforcement agencies to undertake integrity testing operations, it would be appropriate for the TIA Act regime to also permit the obtaining of an interception warrant for the purposes of the operation. This permission could be achieved in several ways, including by reducing the threshold for the grant of an interception warrant when an integrity test has been authorised, or legislating that the approval of an integrity test is a sufficient condition in and of itself for the grant of an interception warrant.

When an agency has determined that an integrity test is an appropriate investigative tool, there will also be circumstances when the integrity testing operation would be enhanced by additional recourse to telecommunications interception. ACLEI has been advised by the other Australian integrity agencies forming part of the Australian Anti-Corruption Commissions Forum that their integrity testing operations would—in many cases—be enhanced by telecommunications interception, should it be available.

[1] Crimes Act 1914, Part IABA