Australian Government

Australian Commission for
Law Enforcement Integrity

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Submission by the Australian Commission for Law Enforcement Integrity

16 January 2015

1. Introduction

The Australian Commission for Law Enforcement Integrity (ACLEI) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security. This submission relates to the Committee's inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.

In summary, ACLEI supports the proposed amendments to the *Telecommunications (Interception and Access) Act 1979*:

- Schedule 2 – section 110A – anti-corruption agencies, including ACLEI, listed as *criminal law enforcement agencies*
- Schedule 1 – section 187C – period for keeping information and documents, and
- Schedule 3 – oversight by the Commonwealth Ombudsman.

To assist the Committee, Part 2 of this submission provides background about ACLEI's role and responsibilities. ACLEI's comments about section 187C of Schedule 1 and section 110A of Schedule 2 of the Data Retention Bill are in Part 3 of this submission. This submission focusses on the data retention aspects of the Bill.

2. Role and responsibilities of ACLEI

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

The objects of the LEIC Act (at section 3) are:

> *(a) to facilitate:*
> *(i) the detection of corrupt conduct in law enforcement agencies and*
> *(ii) the investigation of corruption issues that relate to law enforcement agencies and*
>
> *(b) to enable criminal offences to be prosecuted, and civil penalty proceedings to be brought, following those investigations and*
>
> *(c) to prevent corrupt conduct in law enforcement agencies, and*
>
> *(d) to maintain and improve the integrity of staff members of law enforcement agencies.*

The agencies subject to the Integrity Commissioner's jurisdiction under the LEIC Act are the Australian Crime Commission (ACC), the Australian Customs and Border Protection Service (ACBPS), the Australian Federal Police (AFP), the Australian Transaction Reports and Analysis Centre (AUSTRAC), the CrimTrac Agency, prescribed parts of the Department of Agriculture and the former National Crime Authority.

Role
ACLEI's primary role is to investigate law enforcement-related corruption issues, giving priority to systemic and serious corruption. ACLEI also collects intelligence about corruption in support of the Integrity Commissioner's functions.

The Integrity Commissioner must consider the nature and scope of corrupt conduct revealed by investigations, and report annually on any patterns and trends concerning corruption in law enforcement agencies.

ACLEI also aims to understand corruption and prevent it. When, as a consequence of performing his or her functions, the Integrity Commissioner identifies laws of the Commonwealth or the administrative practices of government agencies with law enforcement functions that might contribute to corrupt practices or prevent their early detection, he or she may make recommendations for these laws or practices to be changed.

Under section 71 of the LEIC Act, the Minister may also request the Integrity Commissioner to conduct a public inquiry into all or any of the following:

- a corruption issue
- an issue about corruption generally in law enforcement, or
- an issue or issues about the integrity of staff members of law enforcement agencies.

Independence

ACLEI is a statutory authority, and part of the Attorney-General's portfolio. The Minister for Justice is responsible for ACLEI.

Impartial and independent investigations are central to the Integrity Commissioner's role. Although the Minister may request the Integrity Commissioner to conduct public inquiries, the Minister cannot direct how inquiries or investigations will be conducted.

The LEIC Act contains measures to ensure that the Integrity Commissioner and ACLEI remain free from political interference and maintain an independent relationship with government agencies. Accordingly, the Integrity Commissioner:

- is appointed by the Governor-General and cannot be removed arbitrarily
- is appointed for up to five years, with a maximum sum of terms of seven years
- can commence investigations on his or her own initiative, and
- can make public statements, and can release reports publicly.

Receiving and disseminating information about corrupt conduct

The LEIC Act establishes a framework whereby the Integrity Commissioner and the relevant agency heads can prevent and deal with corrupt conduct jointly and cooperatively. The arrangement recognises both the considerable work of the agencies in the Integrity Commissioner's jurisdiction to introduce internal corruption controls (including detection and deterrence-focussed mechanisms) and the continuing responsibility that the law enforcement agency heads have for the integrity of their staff members.

An important feature of the LEIC Act is that it requires the head of an agency in ACLEI's jurisdiction to notify the Integrity Commissioner of any information or allegation that raises a corruption issue in his or her agency (section 19).

The LEIC Act also enables any other person, including members of the public or other government agencies or the Minister, to refer a corruption issue to the Integrity Commissioner.

Further, ACLEI is authorised under the *Telecommunications (Interception and Access) Act 1979* 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.

Special legislative arrangements make it lawful for 'whistle-blowers' to provide information about corruption direct to ACLEI. The LEIC Act provides for ACLEI to arrange protection for witnesses.

The Integrity Commissioner may disclose information to the head of a law enforcement agency, or other government agency, if satisfied that, having regard to the functions of the agency concerned, it is appropriate to do so.

The Integrity Commissioner is exempt from the operation of the *Privacy Act 1988*, reflecting the importance of ACLEI's collection and intelligence-sharing role.

Investigation options

The Integrity Commissioner decides independently how to deal with any allegations, information or intelligence about corrupt conduct concerning the agencies in ACLEI's jurisdiction.

The Integrity Commissioner is not expected to investigate every corruption issue that arises in Commonwealth law enforcement. Rather, the Integrity Commissioner's role is to ensure that indications and risks of corrupt conduct in law enforcement agencies are identified and addressed appropriately.

The Integrity Commissioner can choose from a range of options in dealing with a corruption issue. The options are to:

- investigate the corruption issue
- refer the corruption issue to the law enforcement agency for internal investigation (with or without management or oversight by ACLEI) and to report findings to the integrity Commissioner
- refer the corruption issue to the AFP (if the corruption issue does not relate to the AFP)
- investigate the corruption issue jointly with another government agency or an integrity agency for a State or Territory, or
- take no further action.

Section 27 of the LEIC Act sets out the matters to which the Integrity Commissioner must have regard in deciding how to deal with a corruption issue.

With these matters in mind, the Integrity Commissioner will investigate when there is advantage in ACLEI's direct involvement. Under the LEIC Act, the Integrity Commissioner must also give priority to serious or systemic corruption.

Accordingly, the Integrity Commissioner gives priority to corruption issues that may:

- may indicate a link between law enforcement and organised crime
- involve suspected conduct, such as the private use of illicit drugs, which would undermine an agency's law enforcement functions
- bring into doubt the integrity of senior law enforcement managers
- relate to law enforcement activities that have a higher inherent corruption risk
- warrant the use of the Integrity Commissioner's information-gathering powers, including hearings, or
- would otherwise benefit from independent investigation.

ACLEI prioritises corruption issues that have a nexus to the law enforcement character of the agencies in its jurisdiction, having regard to the objects of the LEIC Act.

In this way, ACLEI aims to pursue those investigations which are most likely to yield the highest strategic contribution to maintaining and improving integrity in law enforcement agencies.

Investigation powers

A challenge facing ACLEI is that law enforcement officers subject to investigation by the Integrity Commissioner are likely to be familiar with law enforcement methods, and may be skilled at countering them in order to avoid scrutiny. As a consequence, ACLEI has access to a range of special law enforcement powers.

The key investigative powers available to the Integrity Commissioner and ACLEI are:

- notices to produce information, documents or things
- summons to attend an information-gathering hearing, answer questions and give sworn evidence, and/or to produce documents or things
- intrusive information-gathering (covert)
    - telecommunications interception
    - electronic and physical surveillance
    - controlled operations
    - assumed identities
    - integrity testing (in relation to the ACBPS, ACC and AFP only)
    - scrutiny of financial transactions, and
    - access to specialised information databases for law enforcement purposes
- search warrants
- right of entry to law enforcement premises and associated search and seizure powers, and
- arrest (relating to the investigation of a corruption issue).

It is an offence not to comply with notices, not to answer truthfully in hearings, or otherwise to be in contempt of ACLEI.

3. Comments on the Data Retention Bill

In summary, ACLEI supports the data retention regime set out in the Data Retention Bill 2014.

- **Issue 1:** proposed section 110A lists *criminal law-enforcement agencies*, being those agencies that may (i) access telecommunications data and (ii) apply for a warrant to access stored communications. By including ACLEI as a criminal law-enforcement agency, the Bill recognises the central role ACLEI plays in detecting corruption in prescribed Commonwealth law enforcement agencies, and the importance of stored telecommunications and data to ACLEI investigations, given the covert nature of corruption. ACLEI also supports the Bill's listing of other anti-corruption agencies.
- **Issue 2:** proposed section 187C establishes a mandatory two-year retention period for telecommunications data. ACLEI supports the introduction of the proposed data retention framework. This measure is particularly important for corruption investigations, since corruption is by its nature secretive, uses insider knowledge to remain hidden and can take considerable time to come to light. Since law enforcement officers are more likely to have the skills required to conceal wrong-doing, it is important that ACLEI have access to retained records.
- **Issue 3:** Having regard to the privacy aspects of accessing retained data, ACLEI would welcome strengthened oversight measures to be exercised by the Commonwealth Ombudsman.

Issue 1: Listing of ACLEI as a 'criminal law-enforcement' agency

Schedule 2 of the Data Retention Bill (Section 110A) designates a number of Commonwealth and State agencies as *criminal law-enforcement agencies*, being those that would be able to continue to (i) access *stored communications* (under warrant) and (ii) obtain *telecommunications data*.

As with other criminal law enforcement agencies, analysis of this information for investigative purposes is a vital component of ACLEI's operations. Accordingly, ACLEI supports being listed as a criminal law-enforcement agency in the Data Retention Bill.

Data access essential

Access to telecommunications data and stored communications is an essential part of ACLEI's investigations, since these methods can help to uncover complex corruption and serious crime that would otherwise remain hidden.

Case study: Typical operations

Corruption investigations usually start with an incomplete intelligence picture – an allegation or other piece of information. Telecommunications data is the first building block of many ACLEI investigations.

Telecommunications data helps to build an intelligence picture by establishing the existence of links between individuals, and providing an indication of the possible strength of those relationships. It can also help to assess the credibility of other information – for instance, by establishing whether there are undeclared links between a law enforcement officer and a criminal, or to assist in establishing an alibi.

Historical data essential

Most serious crimes occur in secret, and the role of corruption is often to assist in keeping serious crimes hidden. Accordingly, it is frequently the case that ACLEI wishes to gather evidence about corruption that occurred in the past.

Access to retained historical telecommunications data is essential to fighting corruption, since it enables investigators to see how networks change over time.

Corrupt networks

The sophistication of corrupt networks (and organised criminals generally) develops over time. If left undisturbed, it is more likely that they will become competent at counter-surveillance and increase their ability to defeat law enforcement efforts.

One pattern seen in organised crime and corruption investigations is that central figures may give a number of people a small role in a larger plot – for instance to facilitate the importation or supply of illicit drugs. This method helps to conceal the corruption and protect the central figures from criminal prosecution.

The means and frequency of contact with each individual varies over time, making it difficult to know how wide a corrupt network is, or how deep the compromise may be. Older data can be more useful, since it increases the chances of hidden relationships being discovered.

Analysis of telecommunications data – particularly historical data – is an important tool to uncover this type of corruption.

Informing investigation strategy

Investigation – particularly covert investigation – is a relatively expensive undertaking. In the absence of other information, historical telecommunications data information can be crucial to informing operational decisions, such as:

- whether an investigation should receive priority or be set aside
- where resources (such as physical surveillance) should be targeted and for how long
- whether an integrity test or other strategy is warranted, and
- when, and in respect of whom, the Integrity Commissioner's coercive powers should be used to gather other information.

Often, the information collected through analysis of telecommunications data may be the only practical source of direct evidence of the commission of a serious offence.

This information can be an essential component of an application to use other statutory powers, such as to apply for a warrant to intercept telecommunications or to use a surveillance device.

Applying for a telephone interception warrant

Under the Telecommunications (Interception and Access) Act, ACLEI is eligible to apply for warrants to intercept telecommunications. An applicant must satisfy the nominated official (who is either a judicial officer or a member of the Administrative Appeals Tribunal) that information likely to be obtained by interceptions carried out under a warrant would be likely to assist in the investigation of a serious offence.

Noting the highly intrusive nature of telecommunications interception, the threshold for obtaining a warrant is set high. Due to the hidden nature of corruption, it can be difficult to obtain direct evidence of a high enough standard to obtain a warrant, especially in the early stages of an investigation.

Frequently, the analysis of historical telecommunications data supports the proposition that the interception of communications will afford further information likely to be of assistance in the investigation of a serious offence, or serious offences.

State anti-corruption agencies

State anti-corruption agencies use investigation methods very similar to ACLEI, and are subject to similar accountability regimes. Accordingly, ACLEI also supports the designation of other anti-corruption bodies as *criminal law enforcement agencies*, as named in the Bill.

Issue 2: Mandatory two year retention period

Based on its investigative experience, ACLEI supports a data retention scheme based on mandatory two-year retention, and notes that this practice would be in line with *European Union Directive 2006/24/EC*.

Although there is currently no legal obligation for telecommunication service providers to retain telecommunications data, most have until recently kept this information as part of their business model and billing practices. Some telecommunication service providers presently retain information for longer than two-years and this historical information has proven to be of assistance in investigations conducted by ACLEI.

However, due to vigorous competition and technological developments, many service providers are moving to flat-fee structures based on bulk usage. This telecommunications information, which historically has been available to law enforcement agencies, is becoming increasingly unavailable.

This situation, which is one component of what the Director of the US Federal Bureau of Investigations recently described[1] as *going dark*, presents a serious impediment to law enforcement agencies around the world.

Historical data is relevant at all stages

Throughout an investigation and prosecution, telecommunications data provides important information on individuals' networks and communication patterns, as the following example shows.

Case Study: Operation Heritage/Marca

Operation Heritage/Marca was a joint investigation between ACLEI and the AFP into the involvement of Commonwealth officials in a $45 million drug importation ring operating at Sydney International Airport. To date, 20 people have been convicted or found guilty of corruption-related offences, including five from the Australian Customs and Border Protection Service and one from the Department of Agriculture.

The investigation phase of Operation Heritage/Marca was conducted from 2011 to 2013, and evidence gathered during this period indicated that a drug importation ring had been operating since 2007. Starting from a small piece of information that strongly indicated (but did not prove) corruption, ACLEI analysts used telecommunications data to identify persons of interest and their associates.

The data immediately enriched the intelligence picture concerning the strength of the connection between corrupt officers and their associates, and illustrated how their relationships developed over time. The data informed the investigations strategy, which included:

- deployment of physical surveillance staff
- use of surveillance devices
- interception of telephones and other devices
- access to stored communications
- search warrants
- financial analysis, and
- coercive hearings conducted by the Integrity Commissioner.

Significantly, as the investigation progressed, investigators identified that an associate previously considered benign may have been involved in corrupt conduct at an earlier point. ACLEI was able to use telecommunications data it had collected 18 months earlier to demonstrate corrupt connections, and use other corroborative evidence to prove involvement in criminal offences some years earlier.

[1] *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* James B. Comey, Director, Federal Bureau of Investigation. Address to the Brookings Institution, Washington DC. October 16, 2014.

The person, who over time had become more cautious and evaded other forms of detection, turned out to be a central figure in the conspiracy. Had historical data not been available, the case against the person would not have been as strong and may not have proceeded to prosecution.

Coercive hearings also relied upon telecommunications data (collected early in the investigation) to prove contested facts. In one case, a person denied knowing or being in contact with a second person. When confronted with telephone records, which showed a long-standing historical connection between the two, the person capitulated and made various admissions.

Telecommunications data was critical throughout the whole investigation, and has since been relied on by the Director of Public Prosecutions in prosecuting these cases.

While telecommunications data was a crucial element in the success of Heritage/Marca, access to data was limited to the service providers' own time limits for retention.

Due to the length of the investigation, ACLEI is confident that the whole corrupt network had been identified. However, had a greater timespan of historical telecommunications data been retained by the carriers, the investigation could have been closed with even greater certainty.

Alternatives to retention

ACLEI notes that data retention alternatives, such as preservation notices, are currently available under the TIA Act. However, ACLEI's experience is that these alternatives are most relevant when it is desirable to ensure preservation of future information, such as when a person is under investigation and is likely to commit further crimes. Preservation of past data is limited entirely to the carrier's business practices.

The nature of corruption – particularly in a law enforcement context where officers are more aware of surveillance limitations and able to defeat them – means that relevant conduct is covert and may not come to light for some months or years after the event. It follows that preservation notices cannot assist an investigation if the data sought has already been deleted by the carrier.

Issue 3: Strengthened oversight

Having regard to concerns about privacy, ACLEI supports the strengthened oversight measures relating to access to telecommunications data, to be administered by the Commonwealth Ombudsman.