LECC
Law Enforcement
Conduct Commission

Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the mandatory data retention regime

The Law Enforcement Conduct Commission

The Law Enforcement Conduct Commission (LECC) is a statutory agency established under section 17 of the *Law Enforcement Conduct Commission Act 2016* (NSW) for the oversight of law enforcement in New South Wales (NSW). The LECC commenced operations on 1 July 2017 and replaced the Police Integrity Commission (PIC), the Police Compliance Branch of the NSW Ombudsman's office and the Inspector of the Crime Commission.

The LECC is an independent body exercising the royal commission powers to detect, investigate and expose misconduct and maladministration within the NSW Police Force (NSWPF) and the NSW Crime Commission (NSWCC). The LECC also has the power to independently oversight and monitor the investigation of critical incidents by the NSWPF, if it decides that it is in the public interest to do so. Furthermore, the LECC oversees NSWPF and NSWCC investigations of alleged misconduct by officers of those agencies

The LECC is declared as an "Agency" for the purposes of the *Telecommunications (Interception and Access) Act 1979 (Cth)* (TIA Act) allowing it to apply for, and be issued, telecommunications interception warrants. The LECC is also a criminal law enforcement agency for the purpose of the TIA Act allowing it to access telecommunications data in support of criminal investigations.

We would like to thank the Parliamentary Joint Committee on Intelligence and Security for the opportunity to present the following submission in relation to the review of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

Review of the Current Data Retention Regime

The current data retention regime continues to effectively provide the LECC with access to invaluable data used as evidence and information within criminal investigations. The LECC continues to rely on data beyond the two year retention period and notes there has been some degradation the schemes effectiveness due to the uptake of over-the-top messaging services, which are not captured by the regime.

The LECC puts forward the following as key considerations towards the review of the regime:

- The LECC relies heavily on the access to telecommunications data as it is used 90% of its criminal investigations.
- The LECC supports the continuation of a two year threshold, but notes that in 25% of its criminal investigations data two years or older was requested.
- The LECC requests the committee to consider amendments to the regime to allow the communication of telecommunications data to NSWPF for the purpose of disciplinary proceedings or consideration by the police Commissioner to terminate an officer.

In this submission we refer to and make comment on the committee's terms of reference.

The continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill

Effectiveness of Data Retention Scheme

Telecommunications data is primarily used as a source of information and evidence for investigations of serious misconduct and other criminal offences. In more complex and prolonged investigations, telecommunications data is used to build a picture of suspected offences by identifying persons of interest, establishing relationship networks and levels of contact. By the same token, this data has also been used to eliminate suspicion without having to resort to more intrusive investigative measures.

Operational Example A

In one instance the LECC investigated an Officer of the NSWPF for allegations of money laundering, serious fraud and improper relationship occurring many years. Call charge records (CCRs) were requested for historical data from four years ago to establish contact between parties at the time the alleged fraud commenced. Telstra was able to provide this data and it was invaluable in proving a long term relationship between the Subject Officer and another person of interest complicit in the activity. In addition, the data corroborated allegations of specific fraudulent activity through financial institutions.

This data, when combined with other intelligence, also showed a pattern of behaviour around other corrupt conduct. The CCRs significantly contributed to a body of evidence indicating serious fraud, which enabled the LECC to apply for and be issued with telecommunications interception warrants.

Again at the prosecution phase of the operation, multiple requests for telecommunication data that occurred in excess of four years ago were submitted and successfully retrieved by the carrier. Ten further requests for data created in excess of four years ago were successfully obtained from the carrier. This CCR data was vital to prove contacts between the Officer, key people and financial institutions at the time the fraud was allegedly committed.

Use of Telecommunications Data in Investigations

Telecommunications data is critical to the LECC and is used in approximately 90% of criminal investigations. The LECC's analysis of telecommunications data can reduce the reliance on more intrusive evidence gathering techniques. The LECC has an operational system allowing it to request, store and analyse telecommunications data and have it accessible to our investigators. As indicated in the figure below, the main offences that telecommunications data is used to assist the LECC in investigating are bribery and/or corruption, illicit drug offences and fraud.

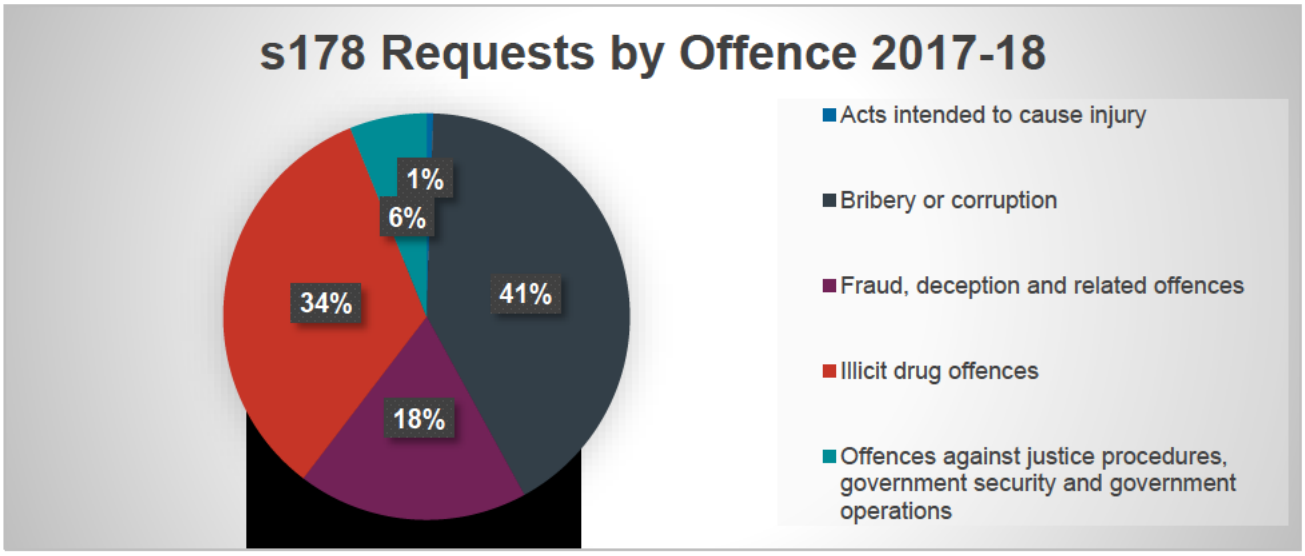

Figure 1. Source: LECC's Case Management System, 2017-2018

Operational Example B

The LECC investigated an Officer of the NSWPF for his involvement in the sale and supply of prohibited drugs. During the investigation, the LECC requested call charge records (CCRs) to allow intelligence analysts and investigators to examine communications around the alleged incident.

In addition, an analysis of communications over a longer period and access to subscriber information under the data retention laws allowed investigators to identify people the Officer was communicating with and assess their criminal history. Through this analysis and other investigative enquiries, enough evidence was obtained to apply for a telecommunication interception warrant for trafficking controlled drugs, an offence under section 302.4(1) of the *Criminal Code 1995* (Cth).

Once in place, the LECC could establish the Officer was using illicit drugs (MDMA and cocaine). Evidence was also established that the Officer had committed perjury in the course of his duty.

As well as establishing connections through CCRs, the LECC also utilised telecommunications data to analyse the relationship between location data and other metadata between targets.

The Use of Telecommunication Data in Surveillance

Surveillance is a highly sought after resource in investigations. The use of telecommunications data, particularly location based data, has increased the effectiveness of deployments of physical surveillance. It has also allowed location based data to inform operations where physical surveillance is unable to be deployed. This allows target location data to be provided in a cost effective way by supporting a larger number of investigations.

Historically it can be said that around 30% of all surveillance deployments were inefficient due to the absence of the target or the inability to locate the target. With access to phone mapping, this situation is nullified in that deployments are able to be more targeted with this knowledge of the target's current location.

Operational Example C

During a surveillance deployment, the target was observed attending a particular address. Further enquiries established a suspicion that the address was being used for the sale of illicit drugs. The LECC was able to use a prospective telecommunications data authorisation to monitor further attendance by the target at this address. The LECC system utilised geo-fencing technology configured to alert when prospective location data was received from the targets phone in the vicinity of the address.

Operational Example D

Prior to deploying the surveillance team for a remote tasking, the target's phone location was monitored for several weeks. This information provided useful patterns of movement indicating the target's routines on particular days of the week. As such, better operational planning was conducted enabling more effective deployment of surveillance.

The Impact of Changing Technology

As technology has developed, there has been a shift towards over-the-top (OTT) communication services provided by social media and messaging platforms. This has impacted the LECC as data from these platforms cannot be captured in the same way as carrier metadata. The shift for some consumers to these new platforms has had a deleterious impact on the effectiveness of access and use of telecommunications data.

For example, telecommunications data created by voice calls or SMS on mobile phones is retained under the current data retention regime for a minimum two years. This data contained within CCRs, where appropriate, can be authorised and accessed by agencies. However, where persons of interest choose to make the equivalent voice or text communications via Whatsapp, Facebook messenger or Facetime etcetera, the associated telecommunications data is not retained under this regime. As a result of the societal uptake of these OTT services, agencies have lost the ability to analyse some of the telecommunications data traditionally obtained within CCRs.

Deficiencies in Mandatory Data Retention Regime

It is appropriate in many circumstances that the results of LECC investigations be provided to the NSWPF for consideration of internal disciplinary proceedings or for consideration of termination of appointment of an officer.

It is critical that police, who hold statutory powers including arrest and the application of force, exercise their duties in an appropriate way. In order to maintain this, LECC relies heavily on telecommunications data to investigation police misconduct including criminal conduct. The communication of misconduct information to the NSWPF, which may allow police to take disciplinary action, is an important function of the LECC and allows both agencies to ensure the integrity of policing within NSW.

Under section 182 of the TIA Act, the current regime allows the LECC to communicate telecommunications data information for the enforcement of the criminal law. Notably, section 68 of the TIA Act allows the LECC to communicate lawfully intercepted information for the purposes of a police disciplinary hearing, for a decision by the police Commissioner to terminate the appointment of an officer and/or for the misbehaviour or improper conduct of an officer. The LECC notes that the lawfully intercepted information that can be communicated under s68 includes not only the metadata, but also the content, meaning it is significantly more intrusive than telecommunications data alone.

The LECC requests that telecommunications data disclosures also be made lawful for this purpose. The LECC would propose that the committee consider provisions of s182(2) be amended in line with s68(d) for the consideration of the communication of telecommunications data for disciplinary action and termination of employment.

The appropriateness of the dataset and retention period

The LECC investigations rely principally on integrated public number database enquiries (IPNDe), CCRs and subscriber checks. For LECC investigations, the current datasets are appropriate.

Importantly for the LECC, access to telecommunication data allows the investigation of corruption offences that result from a pattern of behaviour detected over a period of time. It is common for the LECC to request data spanning a period of years to establish connections at the time the corruption began and as it evolved. As can be seen in Figure 2, for the 2017-18 period, 29% of LECC requests were for telecommunications data created over two years ago. The majority of those requests, the datasets provided important evidence to substantiate the alleged misconduct.

The LECC supports the current retention period of two years, but also suggests that a higher retention threshold would be useful for its investigations.

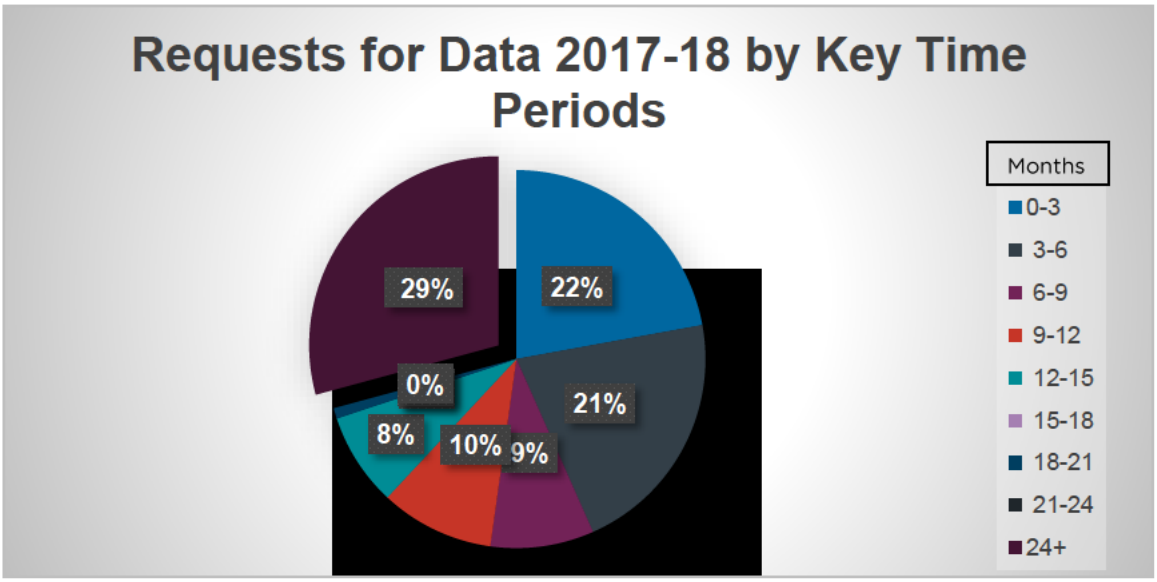

Figure 2. Source: LECC's Case Management System, 2017-2018

Costs, including ongoing costs borne by service providers for compliance with the regime

The LECC is charged appropriately by the carriers for the data and supports a no profit no cost sharing arrangement.

Any potential improvements to oversight, including in relation to journalist information warrants

The LECC is inspected by the Commonwealth Ombudsman for its use of the regime. Inspections are rigorous and thorough typically with four inspectors auditing the LECC records over a week. We believe this is a rigorous and appropriate oversight.

The LECC has not required any data from journalists to date and has implemented a robust system, so that any access to data requiring a journalist information warrants is detected.

Any regulations and determinations made under the regime

NIL comment.

The number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security

NIL complaints received.

Security requirements in relation to data stored under the regime, including in relation to data stores offshore

The LECC maintains highly secure systems with strong electronic and physical and security supplemented by strong information handling procedures to protect its stored data.

Any access by agencies to retained telecommunications outside the TIA Act framework, such as under the Telecommunications Act 1997

Since the introduction of the regime, the LECC has relied solely on access under s178 and s180 of the TIA Act for access to telecommunications data.

Developments in International jurisdictions since the passage of the Bill

NIL comment.

Conclusion

Under the current retention regime the LECC is able to effectively and efficiently access telecommunications data that is critical to the majority of its criminal investigations.

The LECC supports the continuation of the current data retention period of minimum two years for telecommunications providers. However, we note that as the majority of LECC authorisations for access to telecommunications data support investigations into bribery and corruption offences, the LECC often relies on carriers to provider data beyond this two year retention period. For this reason, we support the minimum two year retention period and acknowledge the usefulness of a higher retention period.

Finally, the LECC requests that the committee to consider an amendment to s182(2) to allow the lawful communication of telecommunications data for the purposes of a police disciplinary hearing, for a decision by the police Commissioner to terminate the appointment of an officer and/or for the misbehaviour or improper conduct of an officer. More sensitive lawfully intercepted information, is able to be communicated for this purpose under the same Act and the LECC requests the Committee consider the appropriateness of a similar provision be made for telecommunications data.