Australian Government

Australian Commission for Law Enforcement Integrity

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

REVIEW OF THE MANDATORY DATA RETENTION REGIME

Submission by the
Australian Commission for
Law Enforcement Integrity

28 June 2019

INTRODUCTION

1. The Australian Commission for Law Enforcement Integrity (ACLEI) welcomes the opportunity to make a submission to the Review of the Mandatory Data Retention Regime by the Parliamentary Joint Committee on Intelligence and Security.

2. The office of the Integrity Commissioner and ACLEI, are established by the *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act). ACLEI supports the Integrity Commissioner in the vital work of preventing, detecting, investigating and prosecuting corrupt conduct by staff members of various Commonwealth law enforcement agencies, and assisting to maintain and improve the integrity of staff members of those agencies. As the only Australian Government agency dedicated solely to these tasks, ACLEI has a special role in the Australian Government's anti-corruption framework.

3. ACLEI holds a unique position among the enforcement agencies able to access telecommunications data under the provisions of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). Not only because a number of the Commonwealth law enforcement agencies with the power to access telecommunications data under the TIA Act come within the Integrity Commissioner's jurisdiction, but also because of the challenges which are peculiar to many of the investigations which ACLEI conducts.

4. It is largely for this reason that, while ACLEI has contributed data to the Home Affairs Portfolio submission to the review, ACLEI has chosen also to provide a separate submission to the Committee.

INDEPENDENCE

5. ACLEI is an Australian Public Service Statutory Agency, and part of the Attorney-General's portfolio. The Attorney-General is the Minister responsible for ACLEI.

6. Impartial and independent investigations are central to the Integrity Commissioner's role. 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.

7. Heads of Commonwealth law enforcement agencies under the Integrity Commissioner's jurisdiction are required under the LEIC Act to notify the Integrity Commissioner of any information or allegation that raises a corruption issue in his or her agency.

8. 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.

INVESTIGATIVE POWERS

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

10. The key investigative powers available to the Integrity Commissioner and ACLEI are:
    - notices to produce information, documents or things
    - summons to attend a coercive hearing, answer questions and give sworn evidence, and/or to produce documents or things
    - intrusive information-gathering (covert), including but not limited to:
        - telecommunications interception
        - physical and technical surveillance
        - controlled operations
        - assumed identities
        - integrity testing
        - scrutiny of financial transactions
    - 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).

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

ACLEI'S STRATEGIC APPROACH TO CORRUPTION

12. Australia—unenviably—is one of the world's most profitable markets for illicit drug importations. This situation places those agencies with law enforcement, border regulation, and anti-money laundering functions at increased risk of criminal infiltration and corrupt compromise by organised crime groups. These corruption risks have high potential impacts on individuals, Australian society and the economy. ACLEI's jurisdiction has been extended on three occasions to take account of changes in risk.

13. ACLEI's strategy is to prioritise its detection, disruption and deterrence efforts against high-impact risk themes—those areas of administration, regulatory or law enforcement activity that would be undermined significantly if corruption were to become established. This approach aligns with the LEIC Act which directs that the Integrity Commissioner must give priority to serious corruption and systemic corruption.

14. Accordingly, one of the most frequent targets of ACLEI's investigations is the threat of corruption-enabled border crime—including instances involving facilitation of the importation of illicit drugs or other contraband. A growing aspect of ACLEI's work is in other areas of border regulation, such as biosecurity and visa operations, where corruption can be used as a method to circumvent controls. The potential impacts of this form of corruption may vary—such as advancing the interests of one business entity over another for economic advantage (resulting from a bribe), or enabling money laundering to occur (as part of organised criminal activity).

THE NEED FOR DATA RETENTION

15. Information lies at the heart of every investigation. Access to the correct information is critical to the success of every investigation.

16. Telephony has grown exponentially in recent decades, with communication via voice calls, text messaging, email, social media, and video calls now readily available wherever a mobile network exists.

17. Australia is recognised internationally for its take up of technology. According to one source, Australia is known for adopting new technologies at a faster rate than most other countries. It entered the new millennium with one of the highest rates of internet access in the world.[1] The Australian Institute of Family Studies, quoting from an Australian Bureau of Statistics report published in 2013, reported that as of December 2012, there were 17.4 million mobile telephone subscribers with access to the Internet in Australia.[2] According to *Deloitte*, its 2018 'Mobile Consumer Survey' showed that Australia remains one of the leading global adopters of the smartphone, with 89% of Australians owning one.[3] *Statista* reports that the total number of mobile telephone users in Australia, is predicted to have risen to twenty million by 2019.[4]

18. Data released by the Australian Bureau of Statistics showed that the proportion of Australian households with access to the internet at home grew from 56% in 2004-05 to 86% in 2014-15, remaining relatively constant until 2016-17 when the most recent survey was undertaken.[5] Of those Australian households with access to the internet at home in 2016-17, 91% used mobile or smart telephones to access the internet.[6]

19. Serious and organised crime actors are among those Australians who have harnessed the power of technology to improve their ability to communicate.

20. The amount of telecommunications data in the form of records, created principally by telecommunication providers for billing purposes, has increased, particularly alongside the growth in mobile telephony. While not their intention, criminal actors have left a digital trail of information behind them—including in the form of telecommunications data—with a significant proportion of that information providing indicators of their criminal activities.

21. Law enforcement quickly learnt the value in exploiting this same information for intelligence and evidentiary purposes. Likewise, integrity agencies find the information to be of significant value in many of their investigations, particularly where it enables links between corrupt officials and criminal actors to be identified or confirmed.

22. Access to telecommunications data covered by the mandatory data retention regime forms an essential component in ACLEI's investigations, primarily because of the advantage provided by this information, in uncovering complex corruption and serious crime that would otherwise remain hidden.

23. Typically, corruption investigations commence with an incomplete intelligence picture. Telecommunications data is one of the primary building blocks for many of ACLEI's investigations.

[1] https://www.internationalstudent.com/study_australia/why_study_australia/technology/ (accessed 5 June 2019)
[2] https://aifs.gov.au/cfca/publications/using-technology-service-delivery-families-children/technology-use-australia (accessed 5 June 2019)
[3] https://www2.deloitte.com/au/mobile-consumer-survey (accessed 5 June 2019)
[4] https://www.statista.com/statistics/274677/forecast-of-mobile-phone-users-inaustralia/ (accessed 5 June 2019)
[5] https://www.abs.gov.au/ausstats/abs@.nsf/0/ACC2D18CC958BC7BCA2568A9001393AE?Opendocument (accessed 5 June 2019)
[6] Ibid

24. Telecommunications data assists in developing intelligence pictures, 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.

CHALLENGES POSED BY TECHNOLOGICAL ADVANCES

25. As technology has continued to develop, the ability for criminal actors to encrypt their communications has become routine, putting much of the record of their communication beyond the reach of conventional law enforcement methodologies.

26. As technological advances have changed the way in which people communicate, the way in which telecommunication providers charge customers has changed, as has the form of data (including transactional information, or metadata, the type of information that has proven to be of such value to law enforcement) which the providers need to collect. The datasets which are required to be kept under data retention legislation are, by and large, no longer required by telecommunications providers.

27. Should the requirement for telecommunication providers to retain transactional information be removed or reduced, there is little doubt that such information, which is so vital to many of the investigations conducted by law enforcement generally, and integrity agencies in particular, would quickly become unavailable, thwarting many hitherto successful investigations.

THE REVIEW

28. ACLEI takes very seriously the privacy concerns which were highlighted in the debate around the data retention regime amendments to the TIA Act and again in the lead up to the commencement of the regime, and which stem from the retention of telecommunications data by telecommunications providers for extended periods of time.

29. It is important to note that it is not the content of communications which is retained, but only the information around the delivery of the communication. While of little value to individuals, this information has proven to be of great value to integrity agencies and law enforcement more generally.

CONTINUED EFFECTIVENESS OF THE SCHEME

30. The nature of ACLEI's work in investigating corruption sees ACLEI using telecommunications data in the majority of its investigations, particularly as the LEIC Act requires the Integrity Commissioner to give priority to serious corruption or systemic corruption.

31. For instance, ACLEI sought telecommunications data in 75% of the investigations it conducted, for which at least part of the investigations' information collection phases occurred during either the 2017-18 or 2018-19 Financial Years.

32. ACLEI uses telecommunications data for a number of purposes, including:
    - identifying the existence, extent and strength of relationships between law enforcement officials and criminal entities
    - demonstrating the historicity of alleged corrupt relationships

- identifying patterns of behaviour, which in some instances can indicate the commission of offences; and
- disproving allegations of corruption, thus clearing law enforcement officers of suspicion, without the need for more intrusive, and potentially personally damaging, investigations.

Access to historical data is essential

33. Most serious criminal activity is carried out in secret. The role of corruption is often to assist in maintaining secrecy around criminal activity. Accordingly, it is frequently essential for ACLEI to be able to gather evidence about corruption which has occurred in the past.

34. Access to historical telecommunications data is indispensable in the fight against corruption, particularly as it enables investigations to understand who comprised criminal networks at various points in history, when those networks were engaged in preparing for or committing crimes, and how the networks and their modus operandi change over time.

35. The nature of corruption—particularly in a law enforcement context where officials are more aware of surveillance limitations and consequently are able to defeat them—means that relevant conduct is covert and may not come to light for months or even years after the event.

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

37. One pattern seen in 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.

38. The means and frequency of contact with each individual varies over time, making it difficult to gain an appreciation of the size and reach of a corrupt network, or how deep the compromise may be. Access to historical data is essential, since it increases the prospect of hidden relationships being revealed.

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

40. Investigations—particularly covert investigations—are a relatively expensive undertaking. In the absence of other information, historical telecommunications data can be crucial to informing operational decisions, such as:
    - whether an investigation should receive priority or be set aside
    - where resources (such as surveillance) should be targeted and for how long
    - whether an integrity test or other investigative strategy is warranted, and
    - when, and in respect of whom, the Integrity Commissioner's coercive powers should be used to gather other information.

41. 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.

42. 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.

APPROPRIATENESS OF DATASET AND RETENTION PERIOD

43. Section 187AA of the TIA Act details the telecommunications data which is required to be retained under the data retention regime.

The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (i) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device.
The source of a communication	Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.
The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
The type of a communication or of a relevant service used in connection with a communication	The following: (a) the type of communication; *Examples: Voice, SMS, email, chat, forum, social media.* (b) the type of the relevant service; *Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE.* (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. *Examples: Call waiting, call forwarding, data volume usage.* *Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).*

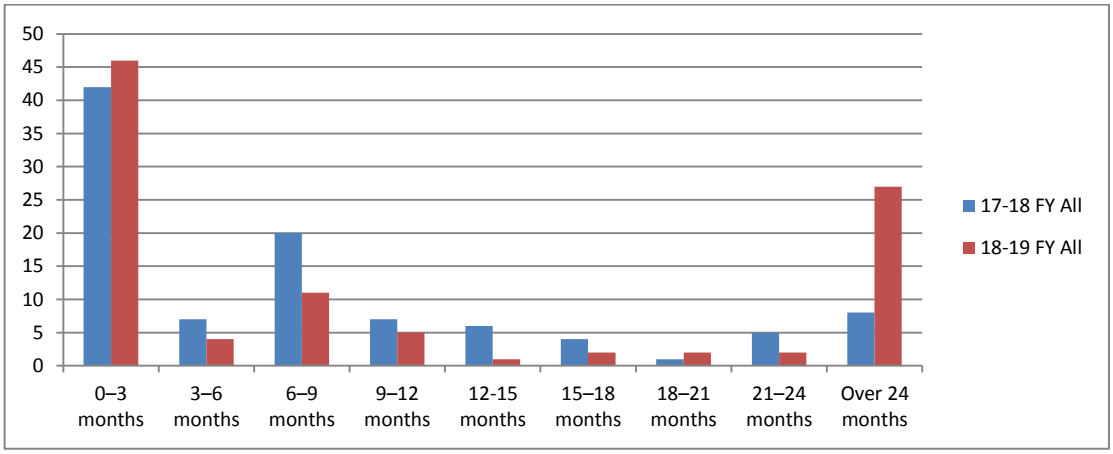
The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. *Examples: Cell towers, Wi-Fi hotspots.*

44. The *Telecommunications Act 1997* restricts the disclosure of telecommunications data. Executive Directors (Senior Executive Service Band 1) and operational Directors (Executive Level 2) at ACLEI, as Authorised Officers for the purposes of the TIA Act, can authorise the disclosure of telecommunications data.

45. Authorised Officers can authorise such disclosures, if they are satisfied that each disclosure is reasonably necessary for the enforcement of the criminal law, and then only if they are satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from each disclosure or use is justifiable and proportionate, having regard to the following matters:

- the gravity of any conduct in relation to which the authorisation is sought, including:
  - the seriousness of any offence in relation to which the authorisation is sought
- the likely relevance and usefulness of the information or documents, and
- the reason why the disclosure or use concerned is proposed to be authorised.[7]

46. The following graph depicts the analysis of the number of authorisations for disclosure of telecommunications data, made by ACLEI Authorised Officers during the 2017-18 and 2018-19 financial years. The numbers are expressed as percentages of the total number of authorisations made by ACLEI in those years, divided across the age of the data being sought.



Percentage of requests for telecommunications data, by age of information, across 2017-18 and 2018-19 Financial Years – including Integrated Public Number Database searches

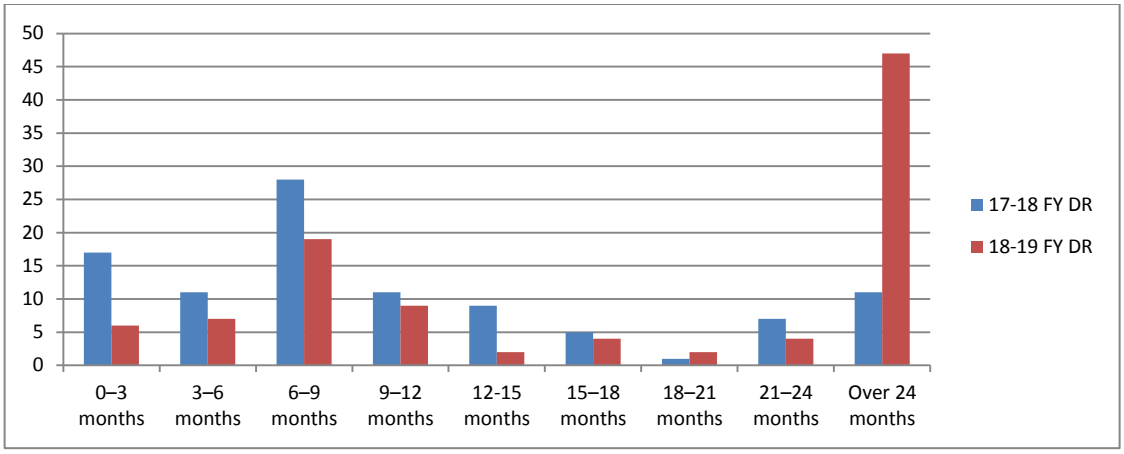
47. The graph shows that the largest number of authorisations in both years was for data up to three months old. This reflects the high number of authorisations granted to access current subscriber information for telecommunications services that was held in the Integrated Public Number Database.

[7] Refer to TIA Act, s 180F

48. Searches of the Integrated Public Number Database are frequently made to identify the subscribers of telephone numbers appearing in the call charge records of persons of interest. While there is no way to know before the Integrated Public Number Database is searched, whether it will hold subscriber information covering the same period covered by the call charge records being analysed, it is significantly more cost-effective than seeking detailed subscriber checks from providers in the first instance, and avoids the delays associated with subscriber checks.

49. The Integrated Public Number Database is also usually the primary resource consulted in order to identify the numbers for telecommunication services used by persons of interest.

50. The following graph depicts the analysis of the number of authorisations for disclosure of telecommunications data, made by ACLEI Authorised Officers during the 2017-18 and 2018-19 financial years, excluding authorisations for searches of the Integrated Public Number Database. Again, the numbers are expressed as percentages of the total number of authorisations made by ACLEI in those years, divided across the age of the data being sought.



Percentage of requests for telecommunications data, by age of information, across 2017-18 and 2018-19 Financial Years – excluding Integrated Public Number Database searches

51. It is worth noting that the percentage of authorisations made for disclosure of telecommunications data which is more than two years old, that is, outside the time period for which it is presently mandatory for providers to retain telecommunications data, more than quadrupled in the 2018-19 financial year when compared to the previous year.

CASE STUDIES

52. ACLEI knows from experience, that if all the telecommunications providers reduced their holdings to the minimum period required under the data retention regime, it would not be able to access critical evidence that may either incriminate or clear people of interest. Without the required telecommunications data, many investigations would almost certainly be unable to be resolved successfully.

53. ACLEI has a number of examples which provide strong evidence of the need for a minimum two year mandatory retention period. Some of these examples demonstrate that ideally, telecommunications data should be mandatorily retained for longer periods. Unfortunately, given the nature of the work which ACLEI conducts

and the strict confidentiality requirements of the LEIC Act, it is not possible to provide detailed information in every instance.

Case Study Number 1

54. Operation Heritage was an investigation into the involvement of Commonwealth officials in a $45 million drug importation ring operating at Sydney International Airport. Twenty-six people were convicted or found guilty of corruption-related offences, including eight from the then Australian Customs and Border Protection Service and one from the then Department of Agriculture.

55. The investigation phase of Operation Heritage 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.

56. 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.

57. 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.

58. 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 telecommunications data not been available, the case against the person would not have been as strong and may not have proceeded to prosecution.

59. 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 telecommunications data, which showed a long-standing historical connection between the two, the person capitulated and made various admissions.

60. Telecommunications data was critical throughout the whole investigation, and was later relied on by the Commonwealth Director of Public Prosecutions in prosecuting these cases.

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

62. Due to the length and thoroughness 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 providers, the investigation could have been closed at an earlier point in time (thus saving Commonwealth funds on the investigation) and with even greater certainty.

Case Study Number 2

63. In late-2012, ACLEI commenced an investigation which had been sparked by information provided by a member of the public in mid-2012. The information suggested that a number of people, who were allegedly involved in the large-scale importation and distribution of illicit drugs, were able to source information from law enforcement officials. As ACLEI considered the information, it identified other reports of a similar nature, which appeared to be related.

64. In 2013, through the analysis of telecommunications data dating back to early 2010, ACLEI was able to identify apparently long-standing links between at least two people who had long been suspected of involvement in the importation and distribution of illicit drugs, but against whom sufficient evidence to charge them had not been obtained previously; a former member of a law enforcement agency; and a serving member of the same law enforcement agency. ACLEI was also able to use recent telecommunications data to demonstrate that the links between the parties continued to the (then) present day.

65. ACLEI's investigation resulted in a number of people being successfully prosecuted for corruption-related offences. It is very difficult to envisage how a successful result could have been achieved in the investigation without access to historic telecommunications data.

66. During the investigation, ACLEI became aware of the possibility that people suspected of involvement in the importation and distribution of illicit drugs had been able to evade detection for many years, dating back to at least 2005, due to their ability to obtain confidential law enforcement information. At least two of the law enforcement officials allegedly involved, were still employed in the law enforcement agency in 2013. Had telecommunications data dating back to 2005 been available in 2013, ACLEI would likely have been able to uncover historic corruption and take appropriate action.

Case Study Number 3

67. ACLEI received information in early 2015, which alleged that an organised crime entity had the ability to access confidential and sensitive law enforcement information.

68. ACLEI's investigation included the extensive analysis of a large volume of telecommunications data dating from 2011 to 2018, for a number of telecommunications services. The analysis identified the existence of relationships and a significant level of contact between law enforcement officials and organised crime entities.

69. Access to the telecommunications data covering a period of years, was critical to the success of the investigation.

Case Study Number 4

70. In the first quarter of 2018, the Integrity Commissioner was notified of information which had come to light in late 2017, which concerned possible corrupt conduct in a law enforcement agency in 2015 and 2016.

71. In order to properly and effectively investigate this corruption issue, telecommunications data dating back to early 2015 needed to be collected and analysed. Fortunately some of the telecommunications providers involved happen to presently retain data for longer than the mandatory period. However, ACLEI has not been able to access all the data required, as other providers involved have not retained the data required by ACLEI.

Case Study Number 5

72. In March 2018, ACLEI received information alleging that some of the illegal activities of a named criminal entity were being enabled by an unknown law enforcement officer. The Integrity Commissioner decided to investigate the allegations. In order to discover if the criminal entity was in contact with any law enforcement officers, telecommunications data in the form of call charge records covering a seven month period, dating back to January 2018, for a service believed to be used by the criminal entity, was obtained.

73. Analysis of the call charge records and subscriber information subsequently obtained in relation to the numbers called, found no information to indicate the criminal entity was in contact with any law enforcement officials. The outcome of the analysis aligned with the results of other inquiries conducted as part of the investigation. The Integrity Commissioner decided to terminate the investigation due to there being no information capable of substantiating the allegation.

74. ACLEI's analysis of the call charge records and subscriber information showed contact between the criminal entity and other known criminal entities in New South Wales. ACLEI shared this intelligence with the New South Wales Police Force. ACLEI's ability to share intelligence in this manner is evidence of how ACLEI's corruption investigations can also benefit other law enforcement activities.

Costs

75. In the 2017-18 and 2018-19 Financial Years, ACLEI paid approximately $84,000 to telecommunications providers to obtain telecommunications data in support of its investigations. Of this amount, approximately $64,000, or 76% of ACLEI's total expenditure on telecommunications data for the period, was spent on information other than that available in the Integrated Public Number Database.

76. The LEIC Act empowers the Integrity Commissioner to require people to give information and produce documents and other things for the purpose of an investigation. While telecommunications providers could be required to produce telecommunications data without ACLEI needing to pay for it, ACLEI exercises the powers available to it judiciously, and instead chooses to access telecommunications data through normal commercial channels open to law enforcement agencies.

CONCLUSION

77. It will be many years before the telecommunications data which is presently still retained by telecommunications providers, outlives its usefulness to law enforcement.

78. ACLEI wholeheartedly supports the accomplishments of the data retention regime in requiring providers that previously did not retain data for any significant length of time, and not beyond that which was absolutely required by those providers for their business purposes, to retain telecommunications data for a minimum period.

79. However, the dangers of mandating a minimum retention period include the possibility that telecommunications providers, which presently retain more data than is required under the regime, will eventually, and perhaps sooner rather than later, reduce their holdings, and that all providers will treat the minimum as a maximum.

80. This would mean that in years to come, historical telecommunications data which has proven, and still proves, to be of significant value to corruption investigations (as well as criminal investigations more broadly), will no longer exist. Thus, corrupt activity which has not yet come to light, but which is presently evidenced in records being created even now, will stand much less chance of being exposed, and may in fact never come to light.

81. Accordingly, in the absence of an increase in the minimum period for which telecommunications data must be retained by telecommunications providers, ACLEI strongly encourages maintaining the status quo in regard to retention periods and types of data which must be retained.

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire

Australian Government
Attorney-General's Department

Under section 186 of the *Telecommunications (Interception and Access) Act 1979,* the head of an enforcement agency must provide the Attorney-General after each 30 June a report that outlines the use of accessed telecommunications data.
Note: Grey field ▭ *sum is an automatically generated figure.*

Agency Name: Australian Commission for Law Enforcement Integrity 2015 - 2016 FY

1 Access to Historical Telecommunications Data - s186(1)(a), s186(1)(b)

1.1 Authorisations for historical data - s178

1.1.1	Total number of authorisations made for access to existing information or documents in enforcement of the criminal law	2123

1.2 Authorisations to locate missing persons - s178A

1.2.1	The number of authorisations made for access to existing information or documents for the location of missing persons	0

1.3 Authorisations for historical data - s179

1.3.1	Total number of authorisations made for access to existing information or documents in enforcement of a law imposing a pecuniary penalty or protection of the public revenue	0

2 Access to Prospective Telecommunications Data - s186(1)(c)

2.1 Specified duration of prospective authorisations - s180

2.1.1	Total number of authorisations made	87
2.1.2	Total number of days authorisations specified in force	3315
2.1.3	Average specified duration	38.10345

2.2 Actual duration of prospective authorisations - s180

2.2.1	Total number of days original authorisations actually in force	3270
2.2.2	Original authorisations discounted	1
2.2.3	Average period in force	38.02326

3 Foreign law enforcement - s 186(ca), 186(cb) - AFP only

3.1 Foreign law enforcement - ss180A, 180B, 180C, 180D

3.1.1	Number of authorisations made under ss180A, 180B, 180C and 180D	0
3.1.2	Number of disclosures made pursuant to ss180A, 180B, 180C and 180D	0
3.1.3	Names of foreign countries pursuant to s186(1)(cb)(i) TIA Act	Not applicable

4 Offences where authorisations were made for historical data and prospective data - s186(1)(e)

4.1	Offences	s178	s179	s180
4.1	Abduction, harassment and other offences against the person	0	0	0
4.2	ACC investigation	0	0	0
4.3	Acts intended to cause injury	0	0	0
4.4	Bribery or corruption	1808	0	67
4.5	Cartel offences	0	0	0
4.6	Conspire/aid/abet serious offence	0	0	0
4.7	Cybercrime and telecommunications offences	0	0	0
4.8	Dangerous or negligent acts and endangering a person	0	0	0
4.9	Fraud, deception and related offences	0	0	0
4.10	Homicide and related offences	0	0	0
4.11	Illicit drug offences	0	0	0
4.12	Loss of life	0	0	0
4.13	Miscellaneous offences	0	0	0
4.14	Offences against justice procedures, government security and government operations	0	0	0
4.15	Organised offences and/or criminal organisations	0	0	0
4.16	Other offences relating to the enforcement of a law imposing a pecuniary penalty	0	0	0
4.17	Other offences relating to the enforcement of a law protecting the public revenue	0	0	0
4.18	People smuggling and related	0	0	0
4.19	Prohibited and regulated weapons and explosive offences	0	0	0
4.20	Property damage and environment pollution	0	0	0
4.21	Public order offences	0	0	0
4.22	Robbery, extortion and related offences	0	0	0
4.23	Serious damage to property	0	0	0
4.24	Sexual Assault and related offences	0	0	0
4.25	Terrorism offences	0	0	0
4.26	Theft and related offences	0	0	0
4.27	Traffic and vehicle regulatory offences	0	0	0
4.28	Unlawful entry with intent/burglary, break and enter	0	0	0

5 Duration of the retention of data covered by s178, 178A, 179 and 180 authorisations- s186(1)(f)

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire

5.1

		0-3mth	3-6mth	6-9mth	9-12mth
5.1.1	Of the authorisations made, how many were for data which had been retained for periods of:*	20	3	2	2
		12-15mth	**15-18mth**	**18-21mth**	**21-24mth**
		3	0	0	5

5.1.2	Total number of the authorisations made for information or documents held for lengths of time exceeding 24 months	0

***** disregard authorisations made for prospective data under 180(2), except to the extent they include authorisations under subsection 180(3)

6 Type of retained data covered by s 178, 178A, 179 and 180 authorisations - s186(1)(g) and (h)

6.1

6.1.1	Total number of authorisations relating to retained data which includes information in item 1 ss187AA(1)	1773
6.1.2	Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)	35
6.1.3	Total number of authorisations relating to retained data which includes information from all items (1-6) in ss187AA(	1808

7 Journalist Information Warrants - s186(1)(i) and (j)

7.1

		s178	s178A	s179	s180
7.1.1	Total number of authorisations made under journalist information warrants	0	0	0	0

7.1.2	Total number of journalist information warrants issued to the agency during that year	0

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire

Australian Government
Attorney-General's Department

Under section 186 of the *Telecommunications (Interception and Access) Act 1979,* the head of an enforcement agency must provide the Attorney-General after each 30 June a report that outlines the use of accessed telecommunications data.
Note: Grey field [ ] *sum is an automatically generated figure.*

Agency Name: Australian Commission for Law Enforcement Integrity 2016 - 2017FY

1 Access to Historical Telecommunications Data - s186(1)(a), s186(1)(b)

1.1 Authorisations for historical data - s178

1.1.1	Total number of authorisations made for access to existing information or documents in enforcement of the criminal law	629

1.2 Authorisations to locate missing persons - s178A

1.2.1	The number of authorisations made for access to existing information or documents for the location of missing persons	0

1.3 Authorisations for historical data - s179

1.3.1	Total number of authorisations made for access to existing information or documents in enforcement of a law imposing a pecuniary penalty or protection of the public revenue	0

2 Access to Prospective Telecommunications Data - s186(1)(c)

2.1 Specified duration of prospective authorisations - s180

2.1.1	Total number of authorisations made	91
2.1.2	Total number of days authorisations specified in force	3920
2.1.3	Average specified duration	43.07692

2.2 Actual duration of prospective authorisations - s180

2.2.1	Total number of days original authorisations actually in force	2712
2.2.2	Original authorisations discounted	20
2.2.3	Average period in force	38.19718

3 Foreign law enforcement - s 186(ca), 186(cb) - AFP only

3.1 Foreign law enforcement - ss180A, 180B, 180C, 180D

3.1.1	Number of authorisations made under ss180A, 180B, 180C and 180D	0
3.1.2	Number of disclosures made pursuant to ss180A, 180B, 180C and 180D	0
3.1.3	Names of foreign countries pursuant to s186(1)(cb)(i) TIA Act	

N/A

4 Offences where authorisations were made for historical data and prospective data - s186(1)(e)

4.1	Offences	s178	s179	s180
4.1	Abduction, harassment and other offences against the person	0	0	0
4.2	ACC investigation	0	0	0
4.3	Acts intended to cause injury	0	0	0
4.4	Bribery or corruption	629	0	91
4.5	Cartel offences	0	0	0
4.6	Conspire/aid/abet serious offence	0	0	0
4.7	Cybercrime and telecommunications offences	0	0	0
4.8	Dangerous or negligent acts and endangering a person	0	0	0
4.9	Fraud, deception and related offences	0	0	0
4.10	Homicide and related offences	0	0	0
4.11	Illicit drug offences	0	0	0
4.12	Loss of life	0	0	0
4.13	Miscellaneous offences	0	0	0
4.14	Offences against justice procedures, government security and government operations	0	0	0
4.15	Organised offences and/or criminal organisations	0	0	0
4.16	Other offences relating to the enforcement of a law imposing a pecuniary penalty	0	0	0
4.17	Other offences relating to the enforcement of a law protecting the public revenue	0	0	0
4.18	People smuggling and related	0	0	0
4.19	Prohibited and regulated weapons and explosive offences	0	0	0
4.20	Property damage and environment pollution	0	0	0
4.21	Public order offences	0	0	0
4.22	Robbery, extortion and related offences	0	0	0
4.23	Serious damage to property	0	0	0
4.24	Sexual Assault and related offences	0	0	0
4.25	Terrorism offences	0	0	0
4.26	Theft and related offences	0	0	0
4.27	Traffic and vehicle regulatory offences	0	0	0
4.28	Unlawful entry with intent/burglary, break and enter	0	0	0

5 Duration of the retention of data covered by s178, 178A, 179 and 180 authorisations- s186(1)(f)

5.1

		0-3mth	3-6mth	6-9mth	9-12mth
5.1.1	Of the authorisations made, how many were for data which had been retained for periods of:*	33	25	29	14
		12-15mth	**15-18mth**	**18-21mth**	**21-24mth**

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire

		14	8	5	2

5.1.2 Total number of the authorisations made for information or documents held for lengths of time exceeding 24 months — 120
***** disregard authorisations made for prospective data under 180(2), except to the extent they include authorisations under subsection 180(3)

6 Type of retained data covered by s 178, 178A, 179 and 180 authorisations - s186(1)(g) and (h)

6.1

6.1.1	Total number of authorisations relating to retained data which includes information in item 1 ss187AA(1)	464
6.1.2	Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)	165
6.1.3	Total number of authorisations relating to retained data which includes information from all items (1-6) in ss187AA(1	0

7 Journalist Information Warrants - s186(1)(i) and (j)

7.1

		s178	**s178A**	**s179**	**s180**
7.1.1	Total number of authorisations made under journalist information warrants	0	0	0	0

7.1.2 Total number of journalist information warrants issued to the agency during that year — 0

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire

Australian Government
Attorney-General's Department

Under section 186 of the *Telecommunications (Interception and Access) Act 1979,* the head of an enforcement agency must provide the Attorney-General after each 30 June a report that outlines the use of accessed telecommunications data.
Note: Grey field ▭ *sum is an automatically generated figure.*

Agency Name: Australian Commission for Law Enforcement Integrity 2017-2018

1 Access to Historical Telecommunications Data - s186(1)(a), s186(1)(b)

1.1 Authorisations for historical data - s178

1.1.1	Total number of authorisations made for access to existing information or documents in enforcement of the criminal law	413

1.2 Authorisations to locate missing persons - s178A

1.2.1	The number of authorisations made for access to existing information or documents for the location of missing persons	0

1.3 Authorisations for historical data - s179

1.3.1	Total number of authorisations made for access to existing information or documents in enforcement of a law imposing a pecuniary penalty or protection of the public revenue	0

2 Access to Prospective Telecommunications Data - s186(1)(c)

2.1 Specified duration of prospective authorisations - s180

2.1.1	Total number of authorisations made	182
2.1.2	Total number of days authorisations specified in force	8056
2.1.3	Average specified duration	44.26374

2.2 Actual duration of prospective authorisations - s180

2.2.1	Total number of days original authorisations actually in force	7068
2.2.2	Original authorisations discounted	24
2.2.3	Average period in force	44.73418

3 Foreign law enforcement - s 186(ca), 186(cb) - AFP only

3.1 Foreign law enforcement - ss180A, 180B, 180C, 180D

3.1.1	Number of authorisations made under ss180A, 180B, 180C and 180D	0
3.1.2	Number of disclosures made pursuant to ss180A, 180B, 180C and 180D	0
3.1.3	Names of foreign countries pursuant to s186(1)(cb)(i) TIA Act	

Not applicable

4 Offences where authorisations were made for historical data and prospective data - s186(1)(e)

4.1	Offences	s178	s179	s180
4.1	Abduction, harassment and other offences against the person	0	0	0
4.2	ACC investigation	0	0	0
4.3	Acts intended to cause injury	0	0	0
4.4	Bribery or corruption	413	0	182
4.5	Cartel offences	0	0	0
4.6	Conspire/aid/abet serious offence	0	0	0
4.7	Cybercrime and telecommunications offences	0	0	0
4.8	Dangerous or negligent acts and endangering a person	0	0	0
4.9	Fraud, deception and related offences	0	0	0
4.10	Homicide and related offences	0	0	0
4.11	Illicit drug offences	0	0	0
4.12	Loss of life	0	0	0
4.13	Miscellaneous offences	0	0	0
4.14	Offences against justice procedures, government security and government operations	0	0	0
4.15	Organised offences and/or criminal organisations	0	0	0
4.16	Other offences relating to the enforcement of a law imposing a pecuniary penalty	0	0	0
4.17	Other offences relating to the enforcement of a law protecting the public revenue	0	0	0
4.18	People smuggling and related	0	0	0
4.19	Prohibited and regulated weapons and explosive offences	0	0	0
4.20	Property damage and environment pollution	0	0	0
4.21	Public order offences	0	0	0
4.22	Robbery, extortion and related offences	0	0	0
4.23	Serious damage to property	0	0	0
4.24	Sexual Assault and related offences	0	0	0
4.25	Terrorism offences	0	0	0
4.26	Theft and related offences	0	0	0
4.27	Traffic and vehicle regulatory offences	0	0	0
4.28	Unlawful entry with intent/burglary, break and enter	0	0	0

5 Duration of the retention of data covered by s178, 178A, 179 and 180 authorisations- s186(1)(f)

TIA Act 1979 Annual Report
Telecommunications Data Questionnaire

5.1

		0-3mth	3-6mth	6-9mth	9-12mth
5.1.1	Of the authorisations made, how many were for data which had been retained for periods of:*	172	30	80	30
		12-15mth	**15-18mth**	**18-21mth**	**21-24mth**
		26	15	3	18

5.1.2	Total number of the authorisations made for information or documents held for lengths of time exceeding 24 months	39

***** disregard authorisations made for prospective data under 180(2), except to the extent they include authorisations under subsection 180(3)

6 Type of retained data covered by s 178, 178A, 179 and 180 authorisations - s186(1)(g) and (h)

6.1

6.1.1	Total number of authorisations relating to retained data which includes information in item 1 ss187AA(1)	188
6.1.2	Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)	225
6.1.3	Total number of authorisations relating to retained data which includes information from all items (1-6) in ss187AA(	0

7 Journalist Information Warrants - s186(1)(i) and (j)

7.1

		s178	s178A	s179	s180
7.1.1	Total number of authorisations made under journalist information warrants	0	0	0	0

7.1.2	Total number of journalist information warrants issued to the agency during that year	0