ibac independent broad-based anti-corruption commission

From the Office of the Commissioner

Our ref: CD/19/33448

20 June 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Via email: pjcis@aph.gov.au

Dear Committee Secretary

Review of the mandatory data retention regime

I refer to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) review of the mandatory data retention regime proscribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

The Independent Broad-based Anti-corruption Commission (IBAC) makes the following submission in relation to the relevant focus areas of the Committee.

Effectiveness of the scheme

IBAC considers that the data retention scheme remains an essential law enforcement tool, and the current thresholds to obtain telecommunications data are appropriate.

While the use of applications that encrypt data is increasing, the importance of telecommunications data in IBAC investigations has not waned, as it often complements other investigative techniques. The majority of IBAC investigations use telecommunications data as a source of evidence in the investigation of police misconduct and corrupt conduct. It is used to identify persons of interest, establish connections and relationships between them, establish patterns of offending, timelines and it can also be used to rule out offending.

Telecommunications data is also often relied upon in prosecutions. In some cases, the use of telecommunications data can render the use of more invasive investigative techniques, such as surveillance or telecommunications interception, unnecessary.

Examples of the general usefulness of telecommunications data is included at Annexure 1.

Level 1, North Tower, 459 Collins Street, Melbourne Victoria 3000 | GPO Box 24234, Melbourne Victoria 3001
Telephone: 1300 735 135 | Facsimile: (03) 8635 6444 | DX 210187 | info@ibac.vic.gov.au | www.ibac.vic.gov.au

Use and Disclosure

While not listed as a specific focus area of the Committee, IBAC supports amendments to the use and disclosure provision at s 182(2) of the TIA Act to broaden its scope.

IBAC works to prevent and expose public sector corruption and police misconduct in Victoria. While some of IBAC's investigations result in criminal charges, it may be that there is ultimately insufficient evidence or it is not in the public interest to prosecute, but sufficient evidence has been obtained to warrant disciplinary action.

Under the current provisions the only relevant permitted purpose open to IBAC to use and/ or communicate telecommunications data, is for the enforcement of the criminal law.

IBAC may refer matters to another entity, including the public body the subject of the investigation, for consideration of disciplinary or other action. Where the supporting evidence for the disciplinary action has been derived from telecommunications data, IBAC cannot presently communicate the information to the agency. This hampers appropriate follow-up action where misconduct that meets the disciplinary threshold has been identified and substantiated.

For example, in an operation where IBAC was investigating allegations of prison officers introducing contraband into a maximum security prison, including illicit drugs; it was found that a prison officer was maintaining contact with former prisoners and making requests on their behalf within the prison system. This evidence was obtained from telecommunications data but the TIA Act did not permit the disclosure of the data to prison management.

By contrast, despite the more intrusive nature of the information, IBAC was able to communicate 'lawfully intercepted information' (derived from telecommunications interception under warrant) to the agency for the purpose of providing recommendations following the investigation as a permitted purpose under section 5(f)(iii) of the TIA Act.

Appropriateness of the dataset and retention period

IBAC submits that a data retention period of two years strikes the appropriate balance between the needs of law enforcement agencies and corruption and integrity agencies to protect the community, while minimising privacy intrusions for individuals.

Many historical investigations rely on the ability to demonstrate connections and communications between persons from the time offending is alleged to have commenced. Once criminal conduct is suspected or a crime committed, historical data is valuable in corroborating other evidence and supporting prosecutions.

IBAC has commenced investigations into corrupt conduct or police misconduct a year or more after the relevant conduct has commenced. This may require access to retained data covering longer periods which facilitates identification of collusion or patterns of behaviour to shape investigative techniques.

For example, IBAC investigated a number of allegations of serious corruption by former senior officers of the Department of Education in two operations where the allegations of offending dated back to 2007. While the investigations took place early in the data retention scheme, call charge record (CCR) data was requested and obtained for data that had been held since 2011, which demonstrated connections between persons of interest. IBAC subsequently laid charges laid in both investigations against a number of persons.

Costs

Although data retained for longer periods (12 months+) can be requested by agencies, the charge by service providers for this data can be prohibitive. These costs have not decreased despite the Data Retention Industry Grants Programme to service providers commenced, which was designed to assist in offsetting service provider costs of data retention.

One IBAC investigation involving a large number of potential persons of interest had 26 requests for CCR and reverse call charge records data held for periods of 24 months+ that totalled $20,900. Requests for this operation were reduced, and certain elements of the offending may not have been subject to comprehensive investigative analysis.

Higher costs are also charged for data spanning significant periods of time, such as six to twelve months. In a similar manner to IBAC's consideration of older data, requests have been curtailed due to costs even though there had been an investigative need to establish connections over longer periods of time.

IBAC has observed that costs vary between service providers and fees are applied inconsistently. IBAC made the same CCR request to two different service providers where the costs were $462 and $1250 respectively. In another example, IBAC made two requests to the same service provider for the same span of time for different service numbers. The fees charged were $396 and $462.

In addition, service providers frequently provide data outside of the parameters of IBAC's requests. During inspections of telecommunications data, the Commonwealth Ombudsman placed the onus on IBAC to ensure that additional data is quarantined and not available for the investigation. Service providers continue to charge for data provided outside of the request parameters and there are significant resourcing implications in processing the additional data.

IBAC considers there is a need for consistency between service providers and would welcome standardised processes and costs between service providers, as well as greater oversight and regulation of this aspect of the data retention regime.

Regulations and determinations made under the regime

Requirement to include name of person from whom a disclosure is sought

During inspections at IBAC, Commonwealth Ombudsman officers have noted that the authorisation for telecommunications data (both existing and prospective) must include, amongst other things, 'the name of the person from whom disclosure is sought'. This means

in effect that the name of a staff member of the telecommunications carrier who will be disclosing the data is included in the authorisation template. It is impractical to require the name of a person merely facilitating the disclosure to be included on an authorisation seeking telecommunications data. The instrument could be amended to require the authorisation to include 'the company and/or person from whom disclosure is sought' rather than 'the name of the person'.

Records required to be kept pursuant to section 187(3)

As requested by the Committee via email on 9 April 2019, please see attached at Annexure 2 a summary of the information required to be kept under section 187N(3).

[redacted]

Yours sincerely

[redacted]

The Honourable Robert Redlich QC
Commissioner

Annexure 1 – Operational examples of general usefulness of telecommunications data

Operation	Details
OP1	IBAC conducted an investigation in 2017 into corrupt activity by a drug rehabilitation officer which led to the identification of an extensive network of individuals involved in drug trafficking and perverting the effective performance of the court system through misrepresentation in bail and community correction orders proceedings. Over 20 individuals were subsequently charged with offences including trafficking a drug of dependence, perjury, pervert (and attempt to pervert) the course of justice. A range of prospective and retained TD records (including CCRs for 0-3 months, 3-6 months and 6-9 months) were used to identify communications in key periods to substantiate interactions between persons of interest.
OP2	IBAC conducted an investigation into fraudulent procurement processes, where it was identified that an individual had provided work to companies controlled by family members to the value of $1.56 million. Retained data was used to identify connections and duration of the offending behaviour, and this investigation was subsequently the subject of a special report to State Parliament in April 2017. Of note in this investigation, retained call charge records were requested form both Telstra and Optus almost three years after the data period (data requested for period of Dec 2012 in November 2015). While this period predated the data retention regime, IBAC obtained results from Telstra; Optus advised that they only held data for 6-8 weeks.
OP3	In December 2015, IBAC commenced an investigation into the leaking of information concerning allegations of drug trafficking within multiple Victorian public service organisations. During the investigation, a person of interest subverted the execution of a lawful search by IBAC by concealing the location of a mobile device. Call charge records (0-3 months) obtained following the search were instrumental in disproving the alibi provided by the person of interest.
OP4	An IBAC investigation identified an individual who was unlawfully accessing, altering and disclosing official records to known members of an Outlaw Motorcycle Gang (OMCG). Call charge records (0-3 months and > 12 months) were correlated with IT system logs to demonstrate collusion and connection between the individuals during periods of unlawful access and alteration. The main person of interest subsequently entered a plea of guilty to a number of charges of misconduct in public office.
OP5	IBAC undertook a preliminary inquiry into suspected links between a serving police member and a known member of an OMCG. IBAC obtained telecommunications data for the previous few months from the telecommunications providers for mobile phones of both individuals. While this data demonstrated that the two devices had made repeated contact over the period, location data included from the telecommunications data was paired with other information reports to identify the users of the devices as the children of the two individuals, who attended the same school. As a result, IBAC determined the link was unsubstantiated and closed the inquiry. The use of retained telecommunications data in this instance negated the need for more intrusive forms of intelligence collection, such as surveillance and telecommunications interception, and completed the inquiry in a timely manner, minimising the unnecessary use of finite investigative resources.

OP6	During the execution of a search warrant, a person of interest informed IBAC investigators that they had discarded a 'faulty' mobile phone a few days before the search. Investigators were sceptical about the coincidental timing of this action, and requests were made for IMEI / IMSI correlations from the telecommunications provider from 2016 onwards. This data confirmed movements of SIM cards over multiple devices over a long period of time. This information enabled IBAC to form a comprehensive picture of phone ownership and use over the relevant period. Without this data, there would have been no evidence of particular behaviours, connections and a nexus proving a theft.
OP7	During an investigation suspected fraudulent procurement, call charge records for a 21 month period were obtained for several services for the purpose of identifying commencement of relationships and specific communications. The provision of this historic data enabled investigators to establish likely timelines and locations of parties in order to exclude particular individuals and focus the inquiry for more efficient application of resources.

UNCLASSIFIED

Annexure 2: PJCIS request for information requested pursuant to section 187N(3)

Total number of authorisations

2015/2016			2016/2017*		2017/2018*	
178	179	180	178	180	178	180
151	1	134	277	139	701	287

*IBAC did not have any section 179 requests in 2016/17 and 2017/18

Section 186(1)(e) – offences for which authorised officers made authorisations

	2015/2016			2016/2017		2017/2018	
Offences	178	179	180	178	180	178	180
Abduction, harassment and other offences against the person				15	1	19	
ACC investigation							
Acts intended to cause injury						20	2
Bribery or corruption	22		6	143	84	344	169
Cartel offences							
Conspire/aid/abet serious offence							
Cybercrime and telecommunications offences							
Dangerous or negligent acts and endangering a person							
Fraud, deception and related offences	87	1	28	80	39	93	23
Homicide and related offences							
Illicit drug offences	17		10	12	10	39	
Loss of life							
Miscellaneous offences				6		12	
Offences against justice procedures, government security and government operations	25		26	13		151	93
Organised offences and/or criminal organisations							
Other offences relating to the enforcement of a law imposing a pecuniary penalty							
Other offences relating to the enforcement of a law protecting the public revenue							
People smuggling and related							
Prohibited and regulated weapons and explosive offences							
Property damage and environment pollution							
Public order offences							
Robbery, extortion and related offences						23	
Serious damage to property							
Sexual Assault and related offences							
Terrorism offences							
Theft and related offences				8	5		
Traffic and vehicle regulatory offences							
Unlawful entry with intent/burglary, break and enter							

UNCLASSIFIED

Section 186(1)(f) – lengths of time for which the information had been held when the authorisations were made

2015/2016

0-3 mth	3-6 mth	6-9 mth	9-12 mth	12-15 mth	15-18 mth	18-21 mth	21-24 mth	24+ mth
112	22	5	3	2	0	1	0	7

2016/2017

0-3 mth	3-6 mth	6-9 mth	9-12 mth	12-15 mth	15-18 mth	18-21 mth	21-24 mth	24+ mth
221	17	7	0	6	7	2	5	12

2017/2018

0-3 mth	3-6 mth	6-9 mth	9-12 mth	12-15 mth	15-18 mth	18-21 mth	21-24 mth	24+ mth
607	32	10	8	5	8	8	2	21

Section 186(1)(g) and (h) – type of retained data

	2015/2016	2016/2017	2017/2018
Total number of authorisations relating to retained data which includes information in item 1 ss187AA(1)	96	203	555
Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)	71	76	146

Section 186(1)(i) and (j) – number of authorisation made under JIWs and JIWs issued

	2015/2016			2016/2017		2017/2018	
	178	179	180	178	180	178	180
Total number of authorisations made under journalist information warrants	0	0	0	0	0	0	0
Total number of journalist information warrants issued to the agency during that year	0	0	0	0	0	0	0

Section 186(1)(k) – information of a kind declared under subsection (1E) of this section

As far as IBAC is aware, there is no information that has been declared under this section.