INDEPENDENT COMMISSION AGAINST CORRUPTION
NEW SOUTH WALES

Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the mandatory data retention regime

Level 7, 255 Elizabeth Street, Sydney NSW 2000 | GPO Box 500 Sydney NSW 2001 | ABN 17 934 402 440
T 02 8281 5999 | F 02 9264 5364 | E icac@icac.nsw.gov.au | www.icac.nsw.gov.au

Executive summary

The Independent Commission Against Corruption of New South Wales ('**the Commission**') welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security ('**PJCIS**') regarding the review of the mandatory data retention regime.

The Commission has already contributed to the Home Affairs Portfolio submission. In addition, the Commission wishes to comment further on the following two areas:

- the continued effectiveness of the mandatory retention regime, in light of recent changes in the use of technology; and
- the appropriateness of the retention period.

The Commission considers that the mandatory retention regime remains effective. That is because even though recent technological changes have impacted the volume of data available, what is captured by the regime provides a forensically probative but relatively unintrusive avenue through which allegations of serious and systemic corruption can be investigated.

The Commission also considers that the current dataset retention period remains appropriate. That is because a significant proportion of the matters the Commission investigates comprise conduct spanning several years and includes allegations that may not be reported to the Commission until significant time has elapsed since the conduct first emerged. Shortening of the data retention period would adversely impact the Commission's ability to investigate the matters that come to its attention, especially those concerning long term, serious and systemic corrupt conduct.

Overview of the Commission

The Commission was established in 1988 in response to growing community concern about the integrity of public administration in NSW. The principal functions of the Commission are to investigate and expose corrupt conduct in the NSW public sector, to actively prevent corruption through advice and assistance, and to educate the NSW community and public sector about corruption and its effects. The *Independent Commission Against Corruption Act 1988* (NSW) gives the Commission broad jurisdiction to investigate any allegation or circumstance which, in its opinion, implies that corrupt conduct has occurred or is likely to occur. In deciding to investigate a matter, the Commission may use the powers it has under legislation to gather information. Investigations are diverse in character and can range from simple to complex and embrace past and current activities. They can require the use of various covert and overt methods of investigation.[1]

The Commission is an enforcement agency within the meaning of subsection 176A of the *Telecommunications Interception and Access Act 1979* ('**TIA Act**'). Commission Authorised Officers may authorise the disclosure of telecommunications data by a service provider if they are satisfied on reasonable grounds that any interference with the privacy of any person or person that may result from the disclosure or use is justifiable and proportionate, having regard to the following matters:

(a) the gravity of the conduct including the seriousness of any offence, pecuniary penalty and whether the authorisation is sought for the purpose of finding a missing person;

(b) the likely relevance and usefulness of the information or documents; and

[1] For more information see https://www.icac.nsw.gov.au/about-the-nsw-icac/overview/functions-of-the-icac.

(c) the reason why the disclosure or use concerned is proposed to be authorised.

Overview of the Mandatory Data Retention Regime

Four years ago, the Australian Government passed the *Telecommunications Interception and Access Amendment (Data Retention) Act* (2015). The amendments established Part 5-1A of the TIA Act, known as the 'mandatory data retention regime'.

The mandatory data retention regime requires carriers, carriage service providers and internet service providers to retain a defined set of telecommunications data for two years. The types of data to be retained include:

- the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service;
- the source of a communication;
- the destination of a communication;
- the date, time and duration of a communication, or of its connection to a relevant service;
- the type of a communication or type of relevant service used in connection with a communication, and;
- the location of equipment, or a line, used in connection with a communication.

Part 5-1A of the TIA Act prescribes that the data is available for law enforcement and national security purposes.[2]

Context to this submission

As noted above, the PJCIS has commenced a review of the mandatory data retention regime, and identified a number of areas of focus. The PJCIS has invited law enforcement agencies, including the Commission, to provide a submission addressing those topics.

As part of that process, the Commission has contributed to the Home Affairs Portfolio submission. In addition, the Commission wishes to comment further on the following areas:

- the continued effectiveness of the mandatory retention regime, in light of recent changes in the use of technology; and
- the appropriateness of the dataset retention period.

In short, the Commission's view is that the mandatory data retention regime continues to be effective for the reasons outlined below.

The Commission has used Telecommunications Data under the Mandatory Data Retention Regime

The TIA Act imposes duties on agencies to provide information to the Attorney-General for annual reporting. The number of authorised disclosures of historical and prospective telecommunications data made by the Commission is detailed in the table following.

[2] See https://www.legislation.gov.au/Details/C2019C00010

Type of Authorisation	2017-2018	2016-2017	2015-2016	2014-2015
Historical data – s178	291	207	262	532
Historical data – s178A	0	0	0	0
Historical data – s179	0	0	0	0
Prospective data – s180	25	7	2	18

Table 1. Authorisations made for access to existing or prospective telecommunications data.

The Mandatory Data Retention Regime remains effective

Since the mandatory data retention regime was introduced in 2015 the Commission has relied on telecommunications data to help investigate suspected corrupt conduct in a variety of matters. The Commission uses telecommunications data as a less intrusive – but forensically probative – line of inquiry to investigate allegations of serious and systemic corruption.

Recent changes in the use of technology, such as the increased use of encryption and 'over the top' ('**OTT**') applications (such as WhatsApp or WeChat) has lessened the amount of telecommunications data available to law enforcement and anti-corruption agencies. In the PJCIS review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018,* the Department of Home Affairs reported that over 90% of telecommunications content being lawfully intercepted by the Australian Federal Police is encrypted,[3] and inaccessible by third parties.

Importantly however, under interception warrants, the Commission can lawfully receive metadata associated with IP data sessions. Whilst the content of these sessions is encrypted, some metadata is not, and can be supplied to the intercepting agency. This is significant because even in the absence of the content of a call/session being available, the metadata itself can be a valuable investigative tool.

An example of such use is set out in the following case study.

Case Study – effectiveness of the regime

*In 2018, the Commission investigated allegations that a council employee had used credit awarded during a telecommunications service provider's promotion to purchase a large amount of Apple iPhones. The devices were not recorded on council asset registers, but were distributed to individuals including employees of the council and their associates. The council could not account for all of the devices. The Commission sought the disclosure of historical telecommunications data to confirm the International Mobile Station Equipment Identity number ('**IEMI**') of the devices. This data then led Commission investigators to seek service numbers and subscriber details for the service numbers. The investigation uncovered that a number of devices had been on–sold by council employees to third parties for financial benefit. The Commission referred information back to the council to consider disciplinary action under its Code of Conduct.*

Telecommunications data and the decreasing amount of unencrypted telecommunications content available to interception agencies is necessary for investigators to make informed decisions when investigating conduct.

[3] See the Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Submission 18 (https://www.aph.gov.au/DocumentStore.ashx?id=8704d357-2f09-4173-871a-f073166d4e10&subId=660956)

The Retention Period is appropriate and reducing it will adversely impact the Commission's work

Much of the telecommunications data to which the mandatory data retention regime is directed is already retained by carriers, carriage service providers and internet service providers as part of their ordinary business, for example for billing customers or other commercial reasons. Significantly, carriers, carriage service providers and internet service providers **must** retain some of the data within the defined set for billing purposes. The two-year period in the mandatory data retention regime is shorter than the requirements set out in section 286 of the *Corporations Act 2001*, which requires businesses to keep financial records for at least seven years after transactions are complete.[4] Shortening the period of time in which such material must be retained by those entities under the TIA Act will not have a substantial impact on how that data is handled by them.

A reduction to the mandatory retention period would seriously impede the ability of the Commission to investigate and expose serious and systemic corrupt conduct in the New South Wales public sector. That is because a significant proportion of the matters the Commission investigates comprise conduct spanning several years and includes allegations that may not be reported to the Commission until significant time has elapsed since the conduct first emerged.

The age of telecommunications data Commission Authorised Officers have sought since the introduction of the regime is set out in the table below.

	2017-2018	2016-2017	2015-2016	Total
Undated data*	32	51	52	135
0-3 month	34	16	35	85
3-6 month	8	20	32	60
6-9 month	3	12	44	59
9-12 month	14	8	25	47
12-15 month	9	6	8	23
15-18 month	11	39	8	57
18-21 month	10	8	15	33
21-24 month	11	0	0	11
24-36 month	96	16	15	127
36 months +	64	32	24	120
Total	**292**	**207**	**258**	**757**

*Undated data, such as IPND and 'point in time' authorisations, have been counted in this table.
NB Calculations differ in annual reporting for the Attorney-General.

Table 2. Age of data sought in authorisations made for access to existing or prospective telecommunications data.

The table shows that the Commission relies on telecommunications data within the mandatory two-year retention period and also that which exceeds the two year period.

Of the matters referred to investigations in that financial year, 61% involved conduct that took place more than 12 months prior to the Commission receiving an initial complaint or report (see Figure 1). Further, the majority of those matters involved conduct that occurred between 1 and 6 years prior to

[4] See https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/

the initial complaint or report. Of those matters, the average age of data relevant to the Commission was 2.9 years.[5]

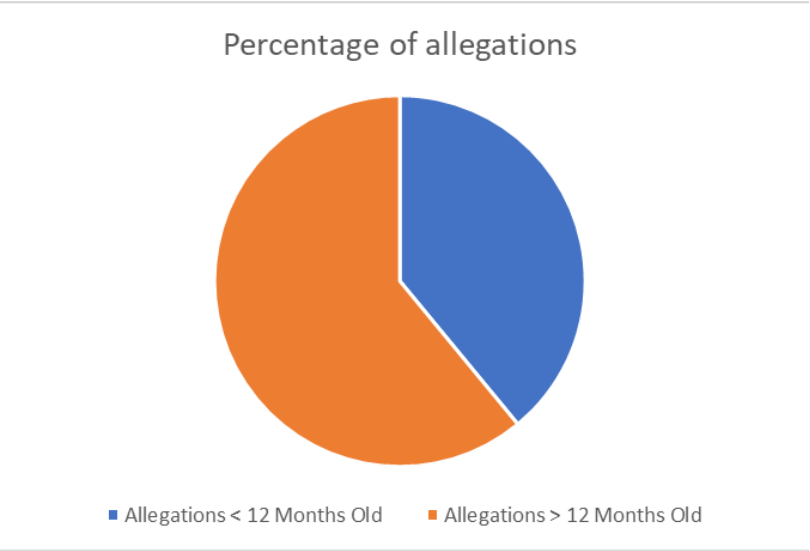

Figure 1. Age of allegations of corrupt conduct escalated to investigation in 2017-2018 financial year

The Commission's ability to investigate matters, especially those involving conduct that is serious and systemically corrupt over a long time, would be negatively impacted should the retention period be reduced.

Case Study – appropriateness of retention period

In 2018 the Commission held a public inquiry in relation to the conduct of two councillors and council staff, between 2013 and 2016.

The Commission began investigating the conduct of the individuals in March 2015. During the investigation Commission Authorised Officers made 135 authorisations for the disclosure of telecommunications data under sections 178 and S180 of the TIA Act. A significant number of the authorisations were for data dating back two years or more. On the value of this data, the Chief Investigator said "this data has been instrumental in enabling investigators understand the complex relationships between the relevant persons and underpinned successful applications for TIA and search warrants. Only having access to data retained for 6 months would have significantly prejudiced this investigation."

Conclusion

The Commission considers that the mandatory retention regime remains an important tool for law enforcement and national security. Whilst recent technological changes have impacted the data available, the Commission relies on telecommunications data as a forensically probative but unobtrusive avenue through which allegations of serious and systemic corruption can be investigated.

[5] The Commission's Assessments Section undertook a detailed analysis of matters referred for investigations between 1 July 2017 and 30 June 2018 and the associated age of those allegations.

The Commission considers the current data retention period is appropriate. A significant proportion of the matters the Commission investigates comprise conduct spanning several years and includes allegations that may not be reported to the Commission until significant time has elapsed since the conduct first emerged. Shortening of the data retention period would adversely impact the Commission's ability to investigate and expose corrupt conduct in the NSW public sector.