PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY REVIEW OF THE MANDATORY DATA RETENTION REGIME

VICTORIA POLICE

VICTORIA POLICE SUBMISSION

Introduction

Section 187N of the *Telecommunication (Interception and Access) Act 1979* (the TIA Act) requires the Parliamentary Joint Committee on Intelligence and Security (the Committee) to review the operation of Part 5-1A of the TIA Act and the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. The Committee is required to report on the review by 13 April 2020.

On 5 April 2019, Victoria Police received an invitation to make a submission on any or all of the areas of focus for the Committee's inquiry. These focus areas are noted at Appendix A.

Victoria Police is pleased to provide a submission to the Committee. In this submission, Victoria Police addresses the following focus areas of the Committee's Inquiry:

- the continued effectiveness of the scheme;
- the appropriateness of the dataset and retention period;
- costs;
- oversight; and
- security requirements in relation to data stored under the regime.

Victoria Police welcomed and supported the introduction in 2015 of the legislative framework mandating telecommunications suppliers in Australia to retain a defined set of telecommunications data for two years, ensuring that such data remained available for law enforcement and national security investigations. We note the mandatory data retention regime was originally introduced as part of a suite of legislative reforms to respond to the national security threat in Australia at that time and in recognition that security and law enforcement agencies should have the resources and powers necessary to keep the community safe[1]. In our opinion, the need for and importance of legislatively mandated data provision to assist police investigations has only increased since the introduction of the regime.

Victoria Police strongly submits that the mandatory data retention regime remains of critical importance. In particular, Victoria Police recommends that the two year timeframe for data retention as prescribed in section 187C of the TIA Act should be maintained. We are of the view that this timeframe provides an appropriate balance between the protection of privacy and the ability of Victoria Police to conduct its investigations effectively.

We also consider that the Review presents an opportune time to revisit some aspects of the regime in order to ensure its continued effectiveness. Specifically, Victoria Police requests the Review consider:

- prescribing a standard format and secure process for the datasets to be provided to law enforcement agencies; and
- introducing oversight of the costs levied for the provision of telecommunications data.

These issues are outlined further in the following submission.

[1] Parliamentary Joint Committee on Intelligence and Security *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, page vii

Continued effectiveness of the mandatory data retention regime

Telecommunications data is a vital investigative tool used by Victoria Police to support its capability to detect and investigate serious and organised crime. It is widely used by Victoria Police, as evidenced by the volume of requests carried out each year and reflected in annual reporting (see Appendix B). This data can provide key evidence and/or intelligence and is frequently used to refine an investigation. Access to this data is also used in lieu of more intrusive investigation methods, such as telecommunications interception.

As technology continues to evolve and is increasingly used in the commission of crime, Victoria Police stresses the importance of access to telecommunications data to effectively investigate crime and keep the community safe. Some case studies follow which demonstrate the critical importance of the mandatory data retention regime to Victoria Police investigations.

Case study 1

Victoria Police investigated a series of blackmails, extortions and assaults committed from July to October 2013 by a syndicate of members of an outlaw motorcycle gang (OMCG). Eight persons were charged with a number of offences including threats to kill, extortion, blackmail, aggravated burglary and intentionally causing injury.

This was a circumstantial case and a large amount of telecommunication data was required to prove the movements of suspects, the connection of events before and after each offence and to link the suspects.

Telecommunication data utilised included Integrated Public Network Database Enquiry (IPNDE), call charge records, reverse call charge records and cell tower location and mapping. This data was instrumental in achieving a successful prosecution.

.

Case study 2

In 2016, Victoria Police investigated a series of related offences comprising trafficking drugs of dependence, firearms offences and conspiracies to engage in conduct endangering life. The majority of the syndicate were identified and charged with this offending however those individuals believed to be responsible for ordering and directing the offences to occur were not charged.

In 2018, a suspect believed to be one of those responsible for ordering and directing some of the offending was identified. As a result, telecommunications data requests were made to obtain IPNDE data, incoming and outgoing call records and cell tower information. The data showed communication between the new suspect and co-accused at specific times of offending and allowed the three suspects' movements to be mapped to and from offence locations before, during and after the offences. The availability of this data led to fresh prosecutions.

Case study 3

Victoria Police investigated a serious assault committed by OMCG members in 2014. The offenders were subsequently charged and the matters were to proceed to trial in 2016. Prior to the first of separated trials, the first accused offered to plead guilty to significantly lesser charges. Prosecutors had concerns about the evidence in existence not conclusively confirming OMCG affiliation and the identity of both parties.

Investigators re-analysed the accused's mobile phone and obtained telecommunications data including IPNDE, incoming and outgoing call records and cell tower information. The requests for data were submitted two years after the offence.

This analysis and the records obtained comprehensively proved the issues beyond doubt. The first accused pleaded guilty to the more serious charges and received a high-range sentence, upheld on appeal and establishing significant case law in relation to offending on behalf of or in connection to an OMCG. The co-accused also elected to plead guilty rather than go to trial based on the new phone evidence.

Case study 4

Victoria Police conducted an investigation into firearms trafficking by an associate of an OMCG. Investigators obtained telecommunications data including incoming and outgoing call records to assist investigators to identify the suspect's associates and discover a rural property. From this intelligence, investigators executed a search warrant at this property and the suspect's home address, seizing numerous illegal firearms.

Further analysis of historical data (aged approximately 12 months) identified the accused to have been in contact with a prominent OMCG figure confirming the association. The data also assisted investigators with identifying an excavation business, chemical companies and another rural property owned by the suspect where numerous tunnels had been dug for the illegal storing of chemicals.

Case study 5

Victoria Police, in conjunction with Queensland Police, conducted an investigation into the stalking and harassment of a number of people using multiple methods such as email, Facebook, Instagram, Viber, WhatsApp and Skype. The suspect also obtained numerous SIM cards in false names that were used to call and send messages to the victims.

The offending occurred over a number of years during which the suspect set up fake profiles including impersonating a well-known television identity to stalk strangers and even a close friend. One of the profiles was used to befriend the victims (known as catfishing) and others were used to harass, intimidate and threaten them. One of the victims ultimately took their own life.

The initial investigation was commenced by Queensland Police who applied for telecommunications data at the time the matter was reported. Victoria Police took over the investigation in 2017 and identified more victims dating back to 2011.

Victoria Police investigators were unable to obtain relevant historic telecommunications data such as incoming call records from telecommunications providers over numerous periods dating back to 2011. Similarly, SMS records were unavailable. Historic IPNDE checks only provide detail on the previous four subscribers which also created issues in trying to identify who the number was registered to at the time of offending. The inability to obtain the historical information from these social media service providers hindered the investigation. Timely access to information from social media providers would have significantly reduced the impact the offending had on the victims in this matter.

Investigators conducted numerous telecommunications and data checks such as IPNDE, subscriber, International Mobile Equipment Identity (IMEI), incoming and outgoing call records and account payment details. Available telecommunications data played an important role in securing findings of guilt for the stalking of six people. The unavailability of data contributed to one charge not able to be proven beyond reasonable doubt.

The appropriateness of the dataset and retention period

Retention period

As outlined in the Introduction, Victoria Police is strongly of the view that the current mandatory data retention period of two years should be maintained. The ability to access older data is particularly important for serious and complex cases where investigations may continue for a significant period of time. We consider the two year mandatory timeframe provides an appropriate balance between the protection of privacy and the ability of Victoria Police to conduct its investigations effectively.

Further, we note that section 187C(3) of the TIA Act does not preclude the retention of data beyond the mandatory retention period. As an example, call records by the three main carriers are kept for periods of between three and seven years. Victoria Police considers that any change to limit the ability to retain data for more than two years would be a significant impediment in the investigation of serious and organised crime in Victoria.

Data types retained

Victoria Police considers the legislation should continue to require the current datasets to be retained: that is, subscriber or account holder of the telecommunications service, the source, destination, type, time and duration of a communication and the location of equipment used in the communication (section 187AA of the TIA Act).

Prospective information

A prospective information (PI) authorisation under s180 gives Victoria Police data such as time, date, location, etc. Currently, content and limited metadata are only available to Victoria Police under a telephone intercept warrant (ie s46 and 46A of the TIA).

Metadata such as date/time, media access control (mac), source and destination internet protocol (IP) addresses, user agents, domain information, and ports and protocols used in IP sessions would provide value in knowing what IP-based communication is occurring on a targeted subscriber's internet session.

Accessing the information under s180 would be a less intrusive means of obtaining the metadata than the interception of calls and therefore have less impact on an individual's privacy.

Victoria Police requests the Review explore whether carriers have the capacity to filter the metadata from the content with a view to providing this metadata to law enforcement agencies under section 180 of the TIA Act.

Standardised format for datasets

It is reassuring to Victoria Police that specified information is available to law enforcement agencies under the mandatory data retention regime. However, disparate datasets are received from providers including different format and content. This creates an administrative burden for Victoria Police members who spend large amounts of time re-formatting data in order to firstly make sense of the data and then utilise it to develop an accurate depiction of the links between parties involved in the offending.

Victoria Police requests the Review consider creating regulations which would enable the government to stipulate the minimum standards and fields for compliance by telecommunications carriers. We recommend that an agreed format be outlined and prescribed in the *Telecommunications Act 1997*; for example, in Division 2—Obligations of ACMA and carriers and carriage service provider Section 314 – "Terms and conditions on which help is to be given".

The secure transmission/exchange of information electronically is also extremely important as it protects the privacy of those whose data is being sought. Victoria Police currently utilises methods such as email and fax to send and receive information from carriers and carriage service providers which is outdated and not secure.

Victoria Police would welcome changes to require the data to be provided in a standardised format and exchanged in a consistent and appropriately secure manner.

Costs

Access to telecommunications data by law enforcement agencies comes at a financial impost. Section 314(2) of the *Telecommunications Act 1997* stipulates that carriers should not profit from assisting law enforcement agencies: "*The person must comply with the requirement on the basis that the person neither profits from, nor bears the costs of, giving that help*". Despite this, there is no oversight of what carriers charge law enforcement agencies for access to data and the cost of data varies depending on the data set requested and can vary widely amongst providers.

It is not sufficiently transparent if carriers are meeting these obligations. Consideration should be given to incorporating regulations in the legislation to ensure that carriers charge agencies on a cost recovery basis only. Cost considerations are taken into account by authorised officers before approving requests for data and this can occur to the detriment of the investigation.

An example of price disparity can be shown as follows.

<u>OPTUS</u>

CCR, SMS and data records are provided separately

	1 day	1 week	1 month*	2 months*
CCR	$100	$100	$200	$256
SMS	$100	$100	$100	$100
Data	$100	$100	$200	$400
Total	$300	$300	$500	$756

*1 month = 28 days, 2 months = 56 days

TELSTRA

CCR, SMS and data records are provided in the same request

	1 day	1 week	1 month*	2 months*
CCR				
SMS				
Data				
Total	$30	$210	$900	$930

*1 month = 30 days, 2 months = 60 days

VODAFONE

CCR, SMS and data records are provided in the same request

	1 day	1 week	1 month*	2 months*
CCR				
SMS				
Data				
Total	$28	$28	$112	$224

*1 month = 28 days, 2 months = 56 days

While Victoria Police accepts that costs are levied for the provision of telecommunications data, we request the Review consider options for management of this process by a Commonwealth regulatory body which could act as an interface in future dealings between agencies and providers. This body could influence the provision of data in a standardised format, ensure it is delivered in a clear, consistent and secure manner and at an equitable cost.

Oversight

Victoria Police believes there are sufficient safeguards and accountability mechanisms in place to obtain, protect and lawfully disclose information under the TIA Act. Existing authorisation arrangements under the TIA Act provide the appropriate balance between protection of privacy and the ability of Victoria Police to conduct its investigations effectively and in turn increase community safety by ensuring the data is necessary and proportionate. Decisions to approve data requests are not made arbitrarily but rather by authorised officers at the rank of Inspector after careful deliberation as required pursuant to section 180F of the TIA Act.

Oversight of law enforcement agencies' application processes and subsequent use of data is carried out by the Office of the Commonwealth Ombudsman. An inspection takes place on a yearly basis where Ombudsman staff spend a number of days at Victoria Police checking data and processes. Victoria Police accepts and welcomes the involvement of the Commonwealth Ombudsman to offer integrity to the process and provide assurance that the access and use of telecommunications material is in the public interest.

Victoria Police is afforded the opportunity to comment prior to the findings being included in the annual report by the Commonwealth Ombudsman which is provided to the Minister pursuant to section 186J of the TIA Act. The report contains recommendations and suggestions and highlights positive practices. Victoria Police remains grateful for the opportunity to receive feedback and make the suggested amendments to processes and practices with a view to achieving full compliance.

Victoria Police has not yet authorised or actioned a journalist information warrant. However, we are conversant with the process involved in obtaining such a warrant and have no concerns in this regard.

Data Security

Victoria Police has no concerns or comments to make about data security and considers that there are appropriate legislative controls in place to ensure the privacy and security of a person's data.

Consolidated Summary of Records

Under subsection 187N(3) of the TIA Act, Victoria Police is required to keep a consolidated summary of records and report on these figures to the Commonwealth Ombudsman and Victorian Inspectorate. As requested by the Committee, the attached tables at Appendix B provide consolidated figures since the data retention regime commenced, of the total number of authorisations made each year as well as each of the other items that are required to be reported on annually under sections 186(1)(e) to (k) of the TIA Act.

Appendix A

Terms of Reference

The Committee has resolved to focus on the following aspects of the legislation:

- the continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill;
- the appropriateness of the dataset and retention period;
- costs, including ongoing costs borne by service providers for compliance with the regime;
- any potential improvements to oversight, including in relation to journalist information warrants;
- any regulations and determinations made under the regime;
- the number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security;
- security requirements in relation to data stored under the regime, including in relation to data stored offshore;
- any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the Telecommunications Act 1997; and
- developments in international jurisdictions since the passage of the Bill.

Appendix B

Consolidated summary of records

ANNUAL REPORT 2014/2015

Telecommunications Data

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

1.1	**Authorisations for historical data - s178**	**Result**
1.1.1	*Total number of authorisations made for access to existing information or documents to enforce the criminal law.*	*66,633*

1.2	**Authorisations to locate missing persons - s178A**	**Result**
1.2.1	*Total number of authorisations made for access to existing information or documents to locate missing persons.*	*5*

1.3	**Authorisations for historical data — s179**	**Result**
1.3.1	*Total number of authorisations made for access to existing information or documents to enforce a law imposing a pecuniary penalty or to protect the public revenue.*	*0*

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

2.3	**Specified duration of prospective authorisations — s180**	**Result**
2.3.1	*Total number of authorisations made*	*4797*
2.3.2	*Total number of days authorisations specified in force*	*98226*
2.3.3	*Average specified duration*	*20.4765*

2.4	**Actual duration of prospective authorisations — s180**	**Result**
2.4.1	*Total number of days authorisations in force*	*43859*
2.4.2	*Authorisations discounted*	*53*
2.4.3	*Average period in force*	*9.24515*

ANNUAL REPORT 2015/2016

Telecommunications Data

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

1.1	Authorisations for historical data - s178	Result
1.1.1	*Total number of authorisations made for access to existing information or documents to enforce the criminal law.*	*82034*

1.2	Authorisations to locate missing persons - s178A	Result
1.2.1	*Total number of authorisations made for access to existing information or documents to locate missing persons.*	*1513*

1.3	Authorisations for historical data — s179	Result
1.3.1	*Total number of authorisations made for access to existing information or documents to enforce a law imposing a pecuniary penalty or to protect the public revenue.*	*0*

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

2.3	Specified duration of prospective authorisations — s180	Result
2.1.1	*Total number of authorisations made*	*6733*
2.1.2	*Total number of days authorisations specified in force*	*133316*
2.1.3	*Average specified duration*	*19.80*

2.4	Actual duration of prospective authorisations — s180	Result
2.4.1	*Total number of days authorisations in force*	*96102*
2.4.2	*Authorisations discounted*	*142*
2.4.3	*Average period in force*	*14.58*

3. Foreign law enforcement-s 186 ca 186 cb - AFP only

3.1	Foreign law enforcement-ss180A, 180B, 1800,180D	
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*	*0*

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*	*4831*	*0*	*640*
4.2	*ACC Investigation*	*0*	*0*	*0*
4.3	*Acts intending to cause injury*	*17605*	*0*	*43*
4.4	*Bribery or Corruption*	*405*	*0*	*33*
4.5	*Cartel Offences*	*0*	*0*	*0*
4.6	*Conspire/aid/abet serious offence*	*501*	*0*	*0*
4.7	*Cybercrime and Telecommunications offences*	*465*	*0*	*4*
4.8	*Dangerous and negligent acts and endangering a person*	*12269*	*0*	*1120*
4.9	*Fraud, deception and related offences.*	*1067*	*0*	*25*
4.10	*Homicide and related offences*	*10493*	*0*	*180*
4.11	*Illicit drug offences*	*2136*	*0*	*85*
4.12	*Loss of Life*	*5634*	*0*	*180*
4.13	*Miscellaneous offences*	*21559*	*0*	*2655*
4.14	*Offences against justice procedures, government security and government operations*	*20*	*0*	*0*

4.1	Offences	s178	s179	s180
4.15	*Organised offences and/or criminal organisations*	*1599*	*0*	*58*
4.16	*Other offences relating to the enforcement of a law impos*	*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.*	*5304*	*0*	*49*
4.20	*Property damage and environment pollution*	*1696*	*0*	*20*
4.21	*Public order offences*	*0*	*0*	*0*
4.22	*Robbery, extortion and related offences*	*3516*	*0*	*68*
4.23	*Serious damage to property*	*1278*	*0*	*55*
4.24	*Sexual Assault and related offences*	*2334*	*0*	*137*
4.25	*Terrorism offences*	*1702*	*0*	*60*
4.26	*Theft and related offences*	*2011*	*0*	*252*
4.27	*Traffic and vehicle regulatory offences*	*3232*	*0*	*56*
4.28	*Unlawful entry with intent/burglary, break and enter*	*5006*	*0*	*98*

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:*	*28590*	*22973*	*12592*	*10087*
		12-15 mth	***15-18mth***	***18-21mth***	***21-24mnth***
		4550	*1763*	*812*	*552*

5.1.2	*Total number of authorisations made for information or documents held for lengths of time exceeding 24 months*	*115*

6. Type of retained data covered by s178, 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)*	*60053*
6.1.2	*Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)*	*23494*
6.1.3	*Total number of authorisations relating to retained data which includes information in items 1-6 ss187AA(1)*	*83547*

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 the year*				*0*

ANNUAL REPORT 2016/2017
Telecommunications Data

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

1.1	Authorisations for historical data - s178	Result
1.1.1	*Total number of authorisations made for access to existing information or documents to enforce the criminal law.*	*82041*

1.2	Authorisations to locate missing persons - s178A	Result
1.2.1	*Total number of authorisations made for access to existing information or documents to locate missing persons.*	*1256*

1.3	Authorisations for historical data — s179	Result
1.3.1	*Total number of authorisations made for access to existing information or documents to enforce a law imposing a pecuniary penalty or to protect the public revenue.*	*0*

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

2.1	Specified duration of prospective authorisations — s180	Result
2.1.1	*Total number of authorisations made*	*7647*
2.1.2	*Total number of days authorisations specified in force*	*145424*
2.1.3	*Average specified duration*	*19.02*

2.2	Actual duration of prospective authorisations — s180	Result
2.2.1	*Total number of days authorisations in force*	*132132*
2.2.2	*Authorisations discounted*	*531*
2.2.3	*Average period in force*	*18.57*

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*	*3649*	*0*	*821*
4.2	*ACIC Investigation*	*0*	*0*	*0*
4.3	*Acts intending to cause injury*	*6800*	*0*	*268*
4.4	*Bribery or Corruption*	*304*	*0*	*5*
4.5	*Cartel Offences*	*1*	*0*	*0*
4.6	*Conspire/aid/abet serious offence*	*332*	*0*	*31*
4.7	*Cybercrime and Telecommunications offences*	*529*	*0*	*15*
4.8	*Dangerous and negligent acts and endangering a person*	*534*	*0*	*954*
4.9	*Fraud, deception and related offences*	*1264*	*0*	*89*
4.10	*Homicide and related offences.*	*12285*	*0*	*946*
4.11	*Illicit drug offences*	*11273*	*0*	*905*
4.12	*Loss of Life*	*5205*	*0*	*211*
4.13	*Miscellaneous offences*	*5532*	*0*	*393*

4.1	Offences	s178	s179	s180
4.14	*Offences against justice procedures, government security and government operations*	*535*	*0*	*37*
4.15	*Organised offences and/or criminal organisations*	*3026*	*0*	*325*
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*	*3*
4.18	*People smuggling and related*	*0*	*0*	*0*
4.19	*Prohibited and regulated weapons and explosive offences.*	*6884*	*0*	*141*
4.20	*Property damage and environment pollution*	*4900*	*0*	*48*
4.21	*Public order offences*	*0*	*0*	*3*
4.22	*Robbery, extortion and related offences*	*4155*	*0*	*417*
4.23	*Serious damage to property*	*1340*	*0*	*207*
4.24	*Sexual Assault and related offences*	*2354*	*0*	*782*
4.25	*Terrorism offences*	*453*	*0*	*168*
4.26	*Theft and related offences*	*5274*	*0*	*461*
4.27	*Traffic and vehicle regulatory offences*	*198*	*0*	*0*
4.28	*Unlawful entry with intent/burglary, break and enter*	*5214*	*0*	*417*

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:*	*61131*	*6712*	*5691*	*3497*
		12-15mth	***15-18mth***	***18-21mth***	***21-24mth***
		2579	*2486*	*1134*	*47*

5.1.2	*Total number of authorisations made for information or documents held for lengths of time exceeding 24 months*	*20*

6. Type of retained data covered by s178, 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 iteml ss187AA(1)*	*60515*
6.1.2	*Total number of authorisations relating to retained data which includes information in items2-6 ss187AA(1)*	*22782*
6.1.3	*Total number of authorisations relating to retained data which includes information in itemsl-6 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 the year*				*0*

ANNUAL REPORT 2017/2018
Telecommunications Data

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

1.1	Authorisations for historical data - s178	Result
1.1.1	*Total number of authorisations made for access to existing information or documents to enforce the criminal law.*	*90,112*

1.2	Authorisations to locate missing persons - s178A	Result
1.2.1	*Total number of authorisations made for access to existing information or documents to locate missing persons.*	*1345*

1.3	Authorisations for historical data — s179	Result
1.3.1	*Total number of authorisations made for access to existing information or documents to enforce a law imposing a pecuniary penalty or to protect the public revenue.*	*0*

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

2.1	Specified duration of prospective authorisations — s180	Result
2.1.1	*Total number of authorisations made*	*9619*
2.1.2	*Total number of days authorisations specified in force*	*384341*
2.1.3	*Average specified duration*	*39.95*

2.2	Actual duration of prospective authorisations — s180	Result
2.2.1	*Total number of days authorisations in force*	*329420*
2.2.2	*Authorisations discounted*	*1010*
2.2.3	*Average period in force*	*38.26*

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*	*4015*	*0*	*1041*
4.2	*ACIC Investigation*	*0*	*0*	*0*
4.3	*Acts intending to cause injury*	*7508*	*0*	*312*
4.4	*Bribery,or Corruption*	*238*	*0*	*11*
4.5	*Cartel Offences*	*0*	*0*	*0*
4.6	*Conspire/aid/abet serious offence*	*356*	*0*	*40*
4.7	*Cybercrime and Telecommunications offences*	*581*	*0*	*21*
4.8	*Dangerous and negligent acts and endangering a person*	*599*	*0*	*1178*
4.9	*Fraud, deception and related offences*	*1377*	*0*	*88*
4.10	*Homicide and related offences*	*13549*	*0*	*1193*
4.11	*Illicit drug offences*	*12586*	*0*	*1119*
4.12	*Loss of Life*	*5731*	*0*	*264*
4.13	*Miscellaneous offences*	*6084*	*0*	*473*

4.1	Offences	s178	s179	s180
4.14	*Offences against justice procedures, government security and government operations*	*581*	*0*	*15*
4.15	*Organised offences and/or criminal organisations*	*3324*	*0*	*425*
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.*	*7562*	*0*	*178*
4.20	*Property damage and environment pollution*	*5372*	*0*	*59*
4.21	*Public order offences*	*1*	*0*	*2*
4.22	*Robbery, extortion and related offences*	*4556*	*0*	*533*
4.23	*Serious damage to property*	*1464*	*0*	*258*
4.24	*Sexual Assault and related offences*	*2591*	*0*	*966*
4.25	*Terrorism offences*	*496*	*0*	*216*
4.26	*Theft and related offences*	*5807*	*0*	*633*
4.27	*Traffic and vehicle regulatory offences*	*0*	*0*	*0*
4.28	*Unlawful entry with intent/burglary, break and enter*	*5734*	*0*	*594*

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.**	*63108*	*7621*	*6593*	*4315*
		12-15mth	***15-18mth***	***18-21mth***	***21-24mnth***
		3565	*3497*	*1336*	*57*

5.1.2	*Total number of authorisations made for information or documents held for lengths of time exceeding 24 months*	*20*

6. Type of retained data covered by s178, 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)*	*45459*
6.1.2	*Total number of authorisations relating to retained data which includes information in items 2-6 ss187AA(1)*	*44653*
6.1.3	*Total number of authorisations relating to retained data which includes information in items 1-6 ss187AA(1)*	*0*

7. Journalist Information Warrants-s186(1)(1) 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 the year*				*0*