AFP
AUSTRALIAN FEDERAL POLICE

AFP Response to Questions from the Parliamentary Joint Committee on Intelligence and Security

1. *In each of the last five years how many times has the AFP sought a stored data warrant?*
2. *In each of the last five years how many times has the AFP obtained a stored communications warrant?*

There are no provisions in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) which allow specifically for stored data to be accessed. Stored Communications may include content, and need to be considered separately from authorised requests for telecommunications data, which cannot include content.

Stored data where it relates to and/or includes content would be sought under Part 3.3 of the TIA Act which allows for warrants to be issued for Stored Communications. These warrants are issued to allow agencies to obtain information which have passed over the telecommunications system, and are accessed with the assistance of a telecommunications carrier without the knowledge of one of the parties to the communication for the investigation of a serious contravention (as defined under the TIA Act).

In the last five years the AFP has sought and been issued with 225 stored communications warrants.

YEAR	Stored Communications Warrants Sought	Stored Communications Warrants Obtained
08/09	41	41
09/10	39	39
10/11	25	25
11/12	76	76
12/13	44	44
TOTAL	225	225

3. *In each of the last five years how many times has the AFP sought authorisations for historical telecommunications data?*

YEAR	Pecuniary Penalty	Criminal Offence	Missing Person	TOTAL
08/09	549	16 492	N/A [1]	17 041
09/10	267	20 869	N/A	21 136
10/11	359	22 992	N/A	23 351
11/12	101	22 900	N/A	23 001
12/13	99	25 582	45	25 726
				110 255

The AFP sought 110,255 authorisations between 08/09 and 12/13.
It is important to note that this figure does not necessarily relate to 110,255 individual people. These authorisations relate to services and/or records such as device identifiers or call charge records, and multiple authorisations may be sought in relation to a single person. This is increasingly becoming the norm, with persons of interest seeking to evade law enforcement detection through the use of multiple services (such as the use of 'burner phones').

The ACMA Communications Report 2013–14 states that, as at June 2014, there were 33.05 million internet service subscribers in Australia. This figure includes mobile phone handset subscribers. In addition, the report notes an additional 9.19 million fixed line telephone services, for a total of more than 42 million services. This figure does not include other services that may have been active at some time in the last 5 years but are no longer active.

4. *For each of the last 5 years, what percentage of historical telecommunications data for which access was sought was:*

   - *Less than three months old;*
   - *Three to six months old;*
   - *Six to nine months old;*
   - *Nine to 12 months old;*
   - *More than 12 months old.*

5. *For each of the last 5 years, what percentage of historical telecommunications data was actually used by the AFP in its operation was:*

[1] The provisions for 178A which allow for access to telecommunications data to assist in locating missing persons were introduced under the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2010 (TIISLA)* which was incorporated in 2011.

- *Less than three months old;*
- *Three to six months old;*
- *Six to nine months old;*
- *Nine to 12 months old;*
- *More than 12 months old.*

In relation to questions 4 & 5, there are a number of reasons that prevent us from accurately quantifying the age of requests for historical telecommunications data within the current timeframe.

AFP systems are not configured to capture this information, and extraction of this information from historical records would require significant resources to manually review.

The AFP also notes that the frequency of requests for historical telecommunications data of different ages may not be the most relevant way of considering the value of that telecommunications data. The nature of criminal investigations means that the bulk of matters subject to investigation relate to relatively recent conduct. However, where those investigations relate to historical events, the investigation will likely be more complex, relate to more serious conduct, or both. While the volume of requests for telecommunications data beyond 12 months old is likely to be lower than for more recent data, the relative value of that data is likely to be more significant.

An example of historical events that may be the subject of investigation are international child protection operations, where information on Australian IP addresses are identified. This process may take a significant amount of time, meaning that data could be more than a year old before it becomes available to Australian authorities. Delays in the provision of information may relate to:

- Lack of control over prioritisation or legal processes in foreign partner agencies;
- Administrative processes associated with international cooperative arrangements;
- Establishment of coordinated international operational activity;
- Technical difficulties in analysis of source data.

Without a 2 year data retention period, the AFP is concerned such investigations, which rely heavily on telecommunications data, will continue to be frustrated by inconsistency in the retention of data by Australian service providers.

6. *In approximately how many cases over the last five years did access to historical telecommunications data accessed by the AFP assist in preventing a serious crime from occurring?*

   - *If historical data was useful in preventing crimes from occurring please provide examples which illustrate the use to which historical data was put (without identifying specific individuals involved)*
   - *If historical data was useful in preventing crime from occurring how old was the specific data that was of use in those instances?*

7. *In approximately how many cases over the last five years did access to historical telecommunications data accessed by the AFP assist in preventing a terrorist act from occurring?*

   - *If historical data was useful in preventing a terrorist act from occurring please provide examples which illustrate the use to which historical data was put (without identifying specific individuals involved)*
   - *If historical data was useful in preventing a terrorist act from occurring how old was the specific data that was of use in those instances?*

It is not possible to approximate with any degree of certainty how many criminal actions, including terrorist acts, have been averted as a direct result of the use of telecommunications data.

Telecommunications data, including historical data, plays an important role in nearly every organised crime, counter-espionage, cyber security, child protection and counter terrorism investigation. Historical telecommunications data can also serve to support contemporaneous criminal investigations. For example, data linked to historical child exploitation material can assist in identifying persons of interest who may be currently involved in further undetected offending, such as live grooming of minors, contact offending or travel for the purposes of child exploitation tourism. Historical telecommunications data could also assist in identifying previously unknown persons of security concern, through analysis of historical radicalisation materials, and support current investigations that may reveal and aid to disrupt contemporary terrorist threats. Historical data may also provide the support necessary to meet the thresholds to obtain search warrants or provide access to other investigative tools.

Metadata is crucial and used in all counter terrorism investigations to determine associations between groups and identifying individuals in the physical world, who are behind anonymous activity. The analysis of telecommunications data is a key component in the overwhelming majority of serious investigations and consistently provides to be an invaluable intelligence capability, including helping identify individuals of concern without having to resort to more privacy instructive measures such as interception of communications.

Telecommunications data played an important role in the investigation and prosecution of suspects in Australia's two largest counter terrorism investigations—Operation Neath and Operation Pendennis. Data was used in these investigations to identify persons of interest and map networks, as well as identifying international links and patterns of communication.

Access to telecommunications data has been instrumental in providing law enforcement and intelligence agencies information necessary to manage specific terrorist risks, and has played an important role in assisting law enforcement agencies to prevent terrorist attacks in Australia.

Telecommunications data also assists in the elimination of suspects from investigations without having to resort to more privacy intrusive measures such as interception of communications.

8. *In approximately how many cases over the last five years did access to historical telecommunications data accessed by the AFP assist in securing a criminal conviction?*

   - *If historical data was useful in securing a criminal conviction provide examples which illustrate the use to which the historical data was put?*

Historical communications data is a fundamental building block of most investigations. However, it is not possible to precisely report on how many cases assisted in securing a criminal conviction.

What can be unequivocally stated is that where stored communications and interception warrants have been used in evidence and led to a conviction a request for historical data will also have occurred. Principally, this data is used to confirm the identity of subscribers or other identifying information. This information can provide the evidence necessary to satisfy an issuing authority prior to a stored communications or interception warrant being obtained.

The approximate number of convictions using intercepted or accessed content is reported on annually. The following table provides a breakdown of convictions of this type between 2008/09 and 2012/13, with a total of 328 convictions.

YEAR	TI/SC Convictions
08/09	29
09/10	31
10/11	20
11/12	45
12/13	203
TOTAL	328

The true figure will be much higher than this, noting that not all historical requests lead to a warrant being sought, and noting the wide use of historical telecommunications data across the range of AFP investigations.

9. *Please describe in detail the use made of historical telecommunications data (as distinct from surveillance material and stored data obtained under warrant) in the investigation and prosecution of suspects in the following investigations:*

   - *Holdsworthy Barracks (Op Neath)*
   - *Benbrika and others (Op Pendennis)*
   - *Lodhi and Willie Brigitte*

Metadata is crucial and used in all counter terrorism investigations to determine associations between groups and identifying individuals in the physical world, who are behind anonymous activity. The analysis of telecommunications data is a key component in the overwhelming majority of priority investigations and consistently provides an invaluable intelligence capability, including helping identify individuals of concern without having to resort to more privacy instructive measures such as interception of communications.

Holdsworthy Barracks (Op Neath)

Operation NEATH was a 2009 investigation into a planned terrorist attack against Holsworthy Army Barracks in New South Wales. In 2010, the five suspects were tried in the Supreme Court of Victoria for conspiring to undertake acts in preparation for, or planning a terrorist act contrary to section 11.5 and section 101.6 of the Criminal Code Act 1995.

Telecommunications data was crucial to the AFP and its partner agencies identifying and understanding the network of people that were involved in the planning of a terrorist attack in Australia.

An analysis of telecommunications data showed an identified individual had dialled a range of numbers known to be linked to individuals engaged in extremist activity.

This information, and the context derived from analysis of telecommunications data, was then able to be further developed through intelligence and investigative techniques to provide the basis for a more comprehensive investigation. This investigation revealed a dedicated terrorist cell in Australia which had intentions to conduct a terrorist act in Australia. The group and their planned action was effectively disrupted.

In December 2010, three of the five were found guilty and sentenced to 18 years imprisonment, to serve 13.5 years.

Benbrika and others (Op Pendennis)

Operation Pendennis utilised both telecommunications interception powers and surveillance devices. Historical telecommunications requests were fundamental in substantiating information in affidavits to support the issue of the telecommunication interception and surveillance device warrants by establishing the identity of implicated individuals. Historical telecommunications data (2003 to 2005) were used in the investigation and the prosecution to show communication between the local individuals, planning of covert meetings, purchasing chemicals/ammunition and meeting with interstate suspects.

Lodhi and Willie Brigitte

Historic Call Charge Records (May 2003 to November 2003) were used in the investigation and the prosecution to show communication between the individuals, purchasing chemicals and overseas Lashkar-e-Tayyiba (LeT) contacts. It is assessed that the arrest of BRIGITTE & LODHI prevented a terrorist act.

Willie Brigitte was taken into Immigration custody (breach of visa) and was returned to France. He was subsequently convicted in France of terrorist training (LeT Pakistan) and acts in preparation & planning a terrorist act in Australia (based on Australian evidence).

Mr Lodhi was sentenced to 20 years imprisonment after being found guilty of planning a terrorist attack against Australia's electricity grid, with one of the alleged targets believed to be the Lucas Heights nuclear reactor in Sydney.

10. *Why is there a significant discrepancy in the number of authorisations to access telecommunications data reported annually to the Parliament under the Telecommunications (Interceptions and Access) Act 1979 in contrast to the figure reported to the Australian Communications and Media Authority?*

There is a difference in the numbers reported in the two documents, as they report on different matters.

The number provided in the annual report to the Parliament under the *Telecommunications (Interception and Access) Act 1979* relates to Authorisations. The AFP's Authorisations may relate to several services or devices linked to a particular person or persons of interest in an investigation.

The figures detailed in the ACMA report includes the number of resulting disclosures made by industry, which may be larger than the number of Authorisations. The ACMA report may also include activities undertaken in accordance with the Telecommunications Act 1997, which are not included in the *Telecommunications (Interception and Access) Act 1979* Report.