UNCLASSIFIED

AFP
AUSTRALIAN FEDERAL POLICE

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*

Submission by the Australian Federal Police

January 2015

UNCLASSIFIED

Introduction

The AFP welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security as part of its inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill)*. This submission builds on the evidence the AFP provided the Committee on 17 December 2014.

2. The AFP supports the Bill. The amendments within the Bill address critical capability requirements by updating existing data access powers to ensure that information once consistently available to law enforcement is preserved. Communications that were once limited to fixed line, single provider telephony now include multiple networks and mechanisms. Telecommunications data such as call records once retained as standard practice are becoming less relevant for current business models within the communication sector, but remain vital for law enforcement. These changes along with globalisation and technological advances mean the legislation is now inadequate. Law enforcement faces a severely degraded capacity to attribute communications to specific individuals, in support of investigations into serious criminality.

3. The Bill, if passed, will address this degradation by providing agencies prescribed under the Act with necessary surety that a defined, limited set of telecommunications data will exist into the future and will be accessible — when lawfully requested — for targeted inquiry in specific investigations into criminal activity. The AFP and other agencies need consistency in the information telecommunications service providers have available to support investigations.

4. Without the reforms proposed in the Bill, the AFP will be increasingly relying on chance that perpetrators of crime are using telecommunications providers that retain telecommunications data. Such a situation is clearly unsatisfactory when dealing with investigations into criminal matters such as child exploitation, counter terrorism or serious and organised crime.

5. The AFP notes the current Bill is consistent with many of the PJCIS' recommendations from its report on its inquiry into *Potential Reforms of National Security Legislation*, and supports the implementation of a balanced series of reforms which provide for continued access to telecommunications data for law enforcement purposes, coupled with enhanced oversight and accountability.

6. This submission seeks to address the inquiry terms of reference by:

- Outlining the operation of the existing regime for lawful access to historical telecommunications data.
- Providing examples of how the AFP uses historical telecommunications data as a critical investigative tool in a range of serious criminal investigations.

- Demonstrating how the variation in retention periods for data across providers impairs the effectiveness of the existing TIA Act provisions, preventing the AFP from identifying perpetrators of significant criminal activities.
- Describing the existing oversight and accountability measures applied to the AFP, as well as the additional safeguards and oversight mechanisms proposed to be incorporated into the existing lawful access provisions of the TIA Act.
- Discussing the financial and procedural impacts of alternatives to retention that have been raised by other parties.

Existing Powers

7. Chapter 4 of the TIA Act currently allows a range of agencies to lawfully access telecommunications data by way of authorised requests to domestic communications providers. This telecommunications data has provided information fundamental in enabling the AFP to effectively investigate and prevent crime across the full suite of the AFP's functions including counter terrorism, serious and organised crime, firearm and drug trafficking, child protection operations, cybercrime, crimes against humanity such as slavery, people smuggling and human trafficking, as well as community policing in the ACT and airports.

8. Within the AFP, authorised requests for access are made on a case by case basis according to identified operational needs. Moreover, under the existing legislative framework, agencies may only make authorisations to disclose information when information is required to:

- enforce the criminal law,
- enforce a law imposing a pecuniary penalty or,
- to locate a missing person.

9. The information returned by providers in response to authorisations forms a cornerstone of contemporary policing, enabling law enforcement to:

- identify suspects and/or victims,
- exculpate uninvolved persons,
- resolve life threatening situations like child abduction or exploitation,
- identify associations between members of criminal organisations,
- provide insight into criminal syndicates and terrorist networks, and
- establish leads to target further investigative resources.

10. The majority of all authorised requests made by the AFP are for the disclosure of ‘historic’ telecommunications data; this is the vital information that will be safeguarded through the Bill. The historical data most commonly requested relates to the basic details necessary to identify a customer or

subscriber to a service — predominantly, the type of information that would once have been available through a telephone directory such as name and address. This information, while basic, can be valuable in confirming a person's identity and linking a service or account back to a person.

11. These links are particularly vital in the modern communications environment where the number of subscriptions and services exceeds the population, with 33.05 million internet services in Australia. This figure includes mobile phone handset subscriptions, and there are an additional 9.19 million fixed line services, making for a total of more than 42 million services[1]. It is also worth noting that this figure does not include other services that may have been active at some time in the last 5 years but which are not currently in active use.

12. A further challenge for establishing the identity of a criminal is that some account details may be fictitious or based on partial or fabricated information. In this context, multiple enquiries, across a range of identifiers, may be required before a link to the real user is found. Using a range of checks, including authorisations for access to historic data to establish a verifiable identity, are vital requirements to ensure that, when used, more intrusive lawful powers such as interception or access to content (conducted under a warrant) are accurately focussed.

13. Another form of authorised request useful for investigations relates to call charge records, which show details of interaction between services including times and durations of calls. These records can then be used to map links and show connections between criminal syndicate members. It must be emphasised that such records, while highly valuable, do not provide an instantaneous result and require detailed and often time consuming analysis. Aside from the legislative prohibitions limiting access to this data, the extensive work required to extract full value from the results is another practical reason why such requests are limited to carefully chosen instances centred on defined investigative avenues and operational needs.

14. When making authorised requests for access the AFP respects privacy and adheres to both the requirements of the TIA Act and the Australian Privacy Principles. Information is only accessed when there is a genuine need and in accordance with all relevant laws. The AFP understands the importance of individual privacy and supports this as a fundamental right in Australia. We also support the important protections on privacy provided for under Australian law. However, the AFP cannot support the right to anonymity when it relates to unlawful activity.

[1] ACMA Communications report 2013–14

AFP use of historical telecommunications data

15. Access to historical telecommunications data is an elementary building block across the vast majority of AFP investigations into serious crimes. Analysis of AFP investigations commenced in the first quarter of 2014-15 confirms that telecommunications data was used in 92% of Counter Terrorism investigations, 100% of Cybercrime investigations, 87% of Child Protection investigations, and 79% of Serious Organised Crime investigations.

16. Intercepted or accessed content played a role in at least 328 convictions over the past five years. In each of these cases telecommunications data was a crucial tool to ensure that those more intrusive capabilities were appropriately targeted and deployed. This figure does not take into account current investigations, matters still before the court, or matters where data (but not content) was used to support a conviction.

17. While these figures highlight the critical role that historical telecommunications data plays in supporting investigations into matters of serious criminality, there is no way to capture how many potential leads are lost or investigations are impacted where information is not available. Indeed it is likely that the figures underestimate the potential breadth of telecommunications data's use in investigations. Firstly, the statistics account for only new investigations: in some instances it may not be until a later stage in the investigative process that lawful access to historical data will be sought. Nor do the statistics address existing and protracted investigations where there may be ongoing requests necessary for a range of reasons including the methodology of suspects churning through cheap and easily obtained 'burner' phones which are used short term and rapidly discarded.

18. Additionally, where it is known that a carrier will not possess the required information due to it being beyond their known retention period, requests will not be progressed. This means the figures referenced in paragraph 15 are indicative only and cannot be said to represent the entirety of investigations, or leads that may have been actively pursued had we been confident that the data had been retained. To mitigate this it is critical that there is a level playing field established, so that the AFP and other law enforcement agencies can be confident that all providers will retain that limited subset of highly valuable telecommunications data for two years.

19. The AFP firmly believes that the two year retention period proposed in the Bill is a reasonable and appropriate timeframe. However, from a law enforcement point of view, there is no clear correlation between the age of the information and its intrinsic value. Depending on the type of investigation, telecommunications data could be as important five years after an event as it is in the immediate aftermath. Moreover, in complex cases the value of older data may increase, particularly where physical evidence has eroded or (as in the case of cyber investigations) it is non-existent, making telecommunications data the key piece of information and evidence available.

The case for standardisation

20. As more services and subscription plans become available some providers are keeping fewer records for shorter periods of time. Additionally the increasing prevalence of encryption by criminal syndicates is resulting in a corresponding diminishment of law enforcements ability to access content thereby increasing the value of data itself. While the need for historical telecommunications data is becoming ever more pressing its availability is becoming less certain. Current retention rates vary widely across industry providers and are based on business imperatives of the provider rather than concerns for national security. The cumulative effect is an uneven playing field where law enforcement is faced with inconsistency in its ability to obtain relevant information from all providers. The AFP strongly believes that criminal investigations and national security are too important to be subject to this element of chance.

21. The amendments proposed in the Bill will address this by creating a legislated obligation on providers to keep records which they already generate and (at least fleetingly) capture in order to facilitate communications. This industry-wide obligation to retain certain telecommunications data will relate to:

- The subscriber of an account or service (including billing details);
- The source and destination of a communication;
- The type, date, time and duration of a communication; and
- The location of equipment or device used during a communication activity.

22. The Bill does not provide new powers for law enforcement. It will not lead to the creation of new or additional information being available at a lesser threshold. Rather it will simply ensure that a defined subset of telecommunications data that is already generated is retained for a known and defined period of time, allowing for the continuing effective operation of the existing provisions under the TIA Act.

23. Essentially the Bill resolves the existing incongruity within the TIA Act whereby law enforcement can legitimately ask a question but there is no corresponding requirement for carriage service providers to retain the information necessary to provide a response. The following case studies demonstrate the critical value of telecommunications data in AFP investigations.

Operation STATICE commenced in January 2007 following referrals from foreign law enforcement agencies identifying high level corruption involving a senior law enforcement officer working with a member of an international criminal enterprise. The formation of the corrupt relationship was a significant factor in a failed prosecution in 2004 allowing the enterprise to continue its global operations unfettered for a further 5 years, with Australia being their main target market.

Analysis of historic telecommunications and other records was undertaken, relating to both the alleged global trafficking of narcotics and the corrupt relationship during 2002 and 2003. This historical review involved the collection and assessment of telecommunications data dating as far back as 1999; some 8 years prior to the initial referral.

The records confirmed the criminal syndicates methodology of using many falsely subscribed pre-paid mobile telecommunications, which were easily acquired and changed frequently. Historical telecommunications data was a key tool for the investigation, not only to corroborate the evidence of the key witnesses but to corroborate the group's activities and prove key elements of the offences including date, time, place, and location of drug importations and also to establish the identity of offenders.

Historical telecommunications data was used as key evidence in the trial of the senior corrupt law enforcement officer and the committal hearing of the criminal syndicate member. The CDPP have indicated that this type of historical telecommunications data will continue to play a critical role in the upcoming trial of the syndicate member in October 2015.

The results of Operation STATICE to date, include are:

- The identification and successful prosecution of a corrupt senior Australian law enforcement officer, imprisoned for 22 years for drug trafficking and corruption;
- The arrest, extradition to Australia and ongoing prosecution of the senior syndicate member for major drug trafficking, money laundering and corruption based offences;
- The identification and restraint of some $2 million of assets, so far, which are believed to be the proceeds of crime;
- The arrest and successful prosecution of at least six senior members, including the two principals of the international criminal syndicate, significantly disrupting their ongoing criminal activities; and
- The arrest and ongoing prosecution of Europe's number one manufacturer of MDMA, whose main customers were Australian.

Operation PENDENNIS was a joint investigation between the AFP, Australian Security Intelligence Organisation (ASIO) and State law enforcement agencies in NSW and Victoria, into terrorist cells based in Victoria and NSW.

In November 2005, a total of 13 persons were charged with a variety of terrorism offences as a result of the investigation in Victoria. A further nine persons were charged with similar offences in NSW. A number of trials were held in Victoria and NSW following that date. The first Melbourne trial, which was an indictment for membership of a terrorist organisation for the entire group concluded in 2009, with seven accused found guilty, two accused pleading guilty and four accused acquitted.

Historical data was a crucial tool supporting the investigation, and was used to identify a covert phone network that was being used in NSW in an attempt to conceal illicit terrorist activities from law enforcement. Historical telecommunications data was critical to identifying and confirming communication between members of the terrorist cells, planning of covert meetings, contact made for purchasing chemicals & ammunition and to verify meetings with interstate suspects.

Analysis of data allowed authorities to identify relevant subjects, and supported applications for warrants for telecommunications interception and surveillance.

Had this data not been available, law enforcement and intelligence agencies would likely not have understood the extent of the network involved in the planning of a terrorist attack in Australia.

One demonstration of the benefits of telecommunications records relates to its use verifying the planning for, and location of, a covert terrorist training exercise conducted in rural NSW.

Subsequent to this police were able to examine the site and conduct ballistic examinations of the shell casings located to match them to a firearm which was seized by police during a search of a suspects' residence.

The investigation would never have reached that point without the use of historical metadata.

Another demonstration of the use for metadata related to Fadl Sayadi, one of the seven accused found guilty in Victoria and sentenced to a period of 7 years imprisonment. On 3 February 2011, he was released on parole and required to comply with multiple conditions including several relating to his access and use of the internet. The monitoring of Operation Pendennis parole compliance was executed by Corrections Victoria with the assistance of members of the AFP Joint Counter Terrorism Team in Melbourne.

During his time on parole Sayadi was observed to be evasive and dishonest with

both his parole officer and law enforcement authorities and was found to be non-compliant on several occasions in relation to his parole conditions. It was not possible to obtain an interception to verify his compliance with parole conditions but this violation was proven with telecommunications metadata provided in response to an authorised request served on his telecommunications service provider.

The telecommunications data whilst not providing content showed clear evidence of undeclared internet access and use contrary to his parole conditions. This data was utilised in reporting the parole breach to both the Attorney General's Federal Offenders Unit and as evidence put before the Court during the parole revocation hearing.

Operation INCA – In 2007, 4.4 tonnes of MDMA pills were seized, in the world's largest single seizure of the drug. There followed a 14 month joint investigation involving AFP, Victoria Police, the Australian Crime Commission, and the Australian Customs & Border Protection Service. During the course of the investigation there was a further seizure of 150kgs of cocaine, and a significant money laundering activity was identified along with ongoing conspiracies to import border controlled substances.

The syndicate under investigation in Operation INCA relied on substantial telecommunications contact between syndicate members and with overseas contacts to conduct its criminal enterprise. In particular, syndicate members used multiple telecommunications services (often subscribed in false details), in attempts to avoid law enforcement detection. By way of example, the syndicate principal was identified as using at least 95 mobile telephone services during the course of the investigation.

Approximately 970 requests for historic telecommunication records were made by the AFP during the operation. Lawful access to historic telecommunications data was vital as it allowed for:

- Reflective insight regarding the telecommunication linkages between syndicate members, revealing the extent of their association
- Use of historic records including cell site information and call pattern analysis to identify and confirm potential involvement with historical acts of criminality ;
- Comparative analysis between historical and recent acts of criminality to ascertain the size and scope of the syndicates criminal footprint;
- Ascertaining the syndicates method of operation through sequential data documenting telecommunication patterns and communication strategies specifically employed by the syndicate to facilitate crime and circumvent law enforcement detection;
- Trend analysis of historic telecommunication data to assist with the identification and use patterns of covert communication networks by the syndicate members, thereby confirming other operational intelligence material particularly human source intelligence; and
- Examining the historical relationship between transnational crime groups and the syndicate to assist with planning for future investigative strategies to deter or stop serious acts of criminality.

Additionally a proportion of call records were obtained after the investigation to corroborate telecommunications product already obtained through lawful interception for use in the CDPP's Briefs of Evidence to support prosecutions.

The investigation culminated in a 6 year prosecution of the 33 offenders, leading to 32 convictions and sentences totalling 300 years of imprisonment. One offender charged remains at large and is considered Australia's most wanted person. Approximately $9 million in proceeds of crime has been forfeited to the Commonwealth.

Operation DRAKENSBERG In November 2013, the AFP commenced evaluating a referral from the UK relating to the compromise of a UK based website in 2011 involving 552 Australian based internet protocol (IP's) addresses which were identified as possibly having accessed child exploitation material. In such cases, telecommunications data is the only avenue of inquiry that may establish the identity of offenders.

Of 552 IP addresses identified, 89 (16%) had to be discounted immediately, as they resolved to Internet Service Providers (ISP's) that were known not to retain any data for the relevant period of time. A further 219 were discounted as although the IP addresses had visited the site it was identified they had not undertaken any transactions.

Further analysis revealed 244 addresses were likely to have been linked to criminal offending and were the subject of requests to ISPs for telecommunications data. Of those 244 requests, another 67 were unable to be progressed further, because telecommunications data could not be obtained from the ISP.

Historic telecommunications data for the remaining 177 IPs was available and resulted in further investigations the identification of 139 persons/subscribers of interest who were referred to the AFP and State and Territory counterparts for further investigations which remain ongoing.

One such investigation led to the AFP executing warrants in Victoria, resulting in two members of the same family being arrested for Child Exploitation-related offences. Child exploitation material was located on the personal computer of one and the work computer of the other. Both were arrested and charged as a result, an outcome that would not have been possible without the availability of historic telecommunications data.

Existing Accountability and New Oversight

24. The TIA Act includes robust accountability measures to ensure that telecommunications data is accessed in a targeted manner to support investigations. The AFP also has strict internal processes to ensure the use of this power is accountably executed.

25. All authorisations for access to historic telecommunications data must be considered and endorsed by a delegated senior Authorising Officer of commissioned rank. After obtaining this approval, an authorisation is then progressed to a centralised area within the AFP, where it is triaged before being sent to a carrier. At this point, the Superintendent of the managing area can also review the authorised request prior to sending it back to the requesting officer for refinement, supporting it as is, or rejecting it.

26. The legislation further stipulates that any Authorising Officer making such a request must have regard as to whether interference with the privacy of any person is justifiable in the circumstances. The number of authorised requests made by each agency is also reported publically on an annual basis, and use of the returned data is subject to disclosure offences and strict regulation under the TIA Act and under the Australian Privacy Principles.

27. The Bill does not change or reduce these existing accountability and oversight mechanisms. Beyond maintaining the existing constraints it also proposes a number of additional safeguards, making accountabilities for data access more consistent with those applied to interception and stored content regimes. Law enforcement will not be provided with any unregulated or indiscriminate access to retained data. Access will remain limited to specific, identified operational needs and targeted requests, as is the case under current provisions of the TIA Act.

28. These expanded oversight provisions are consistent with provisions under the *Surveillance Devices Act 2004.* These measures include making explicit the Ombudsman's role in scrutinising authorised requests and associated public reporting. This will provide public assurance as to appropriate use of powers and will enhance transparency and accountability.

29. The AFP has a strong existing culture of compliance in relation to its responsibilities under legislation including the TIA Act and will proactively adapt its processes to ensure that it meets its new obligations as proposed under the Bill. The AFP's record in relation to its use of powers under the TIA Act and the *Surveillance Devices Act 2004* is demonstrated through the Commonwealth Ombudsman's frequent inspections, with the Ombudsman praising the agency's development of best practice benchmarks in relation to the AFP's use of powers.

Warrants and Preservation notices

30. Telecommunications data is often used at the early stages of investigations to build a picture of a suspect and their network of criminal associates. The AFP also uses telecommunications data, in combination with other information, to ensure that more sensitive or intrusive powers are carefully and effectively targeted. Information obtained via an authorised request is most often used as a fundamental basis to satisfy the evidentiary test to obtain an interception warrant in most situations. As described above, there are numerous safeguards, both in legislation and through the AFP's internal authorisation process, to ensure the proper and appropriate authorisations for access to telecommunications data.

31. Some parties have suggested that, should a defined period of retention for telecommunications data be enacted, a warrant regime should be imposed for access to such data. The AFP understands that part of the impetus for this arises from a misconception that what is proposed through the Bill is the extension of powers available to law enforcement and security agencies. The AFP considers that, given the existing safeguards, constraints and processes governing the authorisation regime, and the extended oversight provisions under the Bill, that a

warrant scheme for access to telecommunications data would not significantly improve accountability or transparency of the scheme. Rather, the AFP considers that such a scheme would generate unnecessary administrative burden and costs on both agencies seeking access to telecommunications data and on the issuing authority for such warrants.

32. The AFP is concerned that the time (not even counting the financial cost) required per request to prepare and progress a warrant for telecommunications data would reduce operational responsiveness in time sensitive cases and create a bureaucratic burden, diverting investigative resources from the field. The AFP conservatively estimates, based on other warrant applications that the process for preparing such a warrant would take at least 8 hours of dedicated work. Extending this to the existing rate of requests for telecommunications data, this would equate to a requirement for over 100 staff to be solely committed to warrant preparation duties.

33. A scheme requiring agencies to obtain a warrant for historical telecommunications data would also create a significant additional burden on the already stretched Administrative Appeals Tribunal and judicial system, who would be required to consider approximately 25,000 applications from the AFP alone every year. Such a process, particularly when contrasted with the Bills proposal to extend the Ombudsman's oversight of agency compliance and allow for holistic evaluation and public reporting on how agencies are executing their powers, would be resource intensive and provide limited additional surety to the community.

34. It has also been suggested that instead of a defined all-inclusive retention period for a limited subset of telecommunications data, preservation or freezing of telecommunication data could be applied following target identification. The AFP is concerned that such an approach would not provide any significant improvement on the current situation. Preservation notices could only be imposed after an offence has been committed and would only be effective if the relevant telecommunications data had been retained at the time of the preservation notice being served. Where a carrier routinely disposes of crucial telecommunications data in a short period of time, the preservation order would be entirely ineffective.

35. Indeed, to only be able to request a provider retain or preserve information after a criminal suspect has been identified or a serious criminal offence has already taken place would be ineffective and leave law enforcement at serious disadvantage as information and potential evidence will be lost. In many instances, the role that data plays in the early stages of investigations is to assist in attribution: that is, data is a crucial tool in identifying the suspect in a criminal act or event, and in clearing other persons from suspected involvement. Where this data is unavailable because it has not been retained, investigations have been unable to progress.

Conclusion

36. The AFP's advocacy for data retention has never been about an expansion of powers. The AFP's support stems from the critical need to redress an ongoing erosion of existing investigative powers, flowing from the rapid evolution of technology, the convergence of communication methods, changes in business models within the communications sector and changes in social interaction characterised by the increasing use of multiple communications services. The current environment is one where legislation allows law enforcement to ask a question but does nothing to compel carriers to preserve the answer.

37. The Bill balances this equation by ensuring a limited, but crucial, set of communications data will exist into the future and will be available when lawfully authorised for specific inquiry into serious acts of criminality whilst implementing appropriate safeguards and oversight mechanisms. Without this reform the AFP will face growing uncertainty that telecommunication carriers will retain this data and a vital investigative tool will be lost. This state of affairs is manifestly unsatisfactory when dealing with criminal matters and national security.

38. The AFP believes the data retention Bill as currently presented is a proportionate scheme that will enable the AFP to continue using existing capabilities and tools that are becoming less effective due to technological and social change.