AUSTRALIA

ACC
AUSTRALIAN CRIME COMMISSION

AUSTRALIAN CRIME COMMISSION

Submission to Parliamentary Joint Committee on Intelligence and Security Inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*

Introduction

The Australian Crime Commission (ACC) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) Inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Bill).

This submission is unclassified and may be published in the public domain. It addresses the Bill introduced in the House of Representatives on 30 October 2014 and further focuses on the ACC's need for telecommunications data retention in the course of investigating serious and organised crime. The ACC recognises the need to provide a clear evidence base for requiring the retention of historical telecommunications data and has included a number of de-classified case studies in this submission.

The Bill

Access to telecommunications data is not a new power for law enforcement and security agencies, including the ACC. This Bill will create consistency in the storage provisions for data that law enforcement and security agencies, including the ACC, already request and use.

The ACC supports the proposed Bill and has contributed to its development, in collaboration with the Attorney-General's Department, Department of Communications, Australian Federal Police, Australian Security Intelligence Organisation and industry participants.

The ACC consulted with, and represented the interests of, its state and territory law enforcement Board member partners throughout the drafting and consultation process. The ACC Board is both supportive of mandatory data retention and the data set outlined in the Bill[1].

Data set

The ACC is supportive of the proposed data set outlined within the Bill and the subsequent amendments outlined in the Final Report of the Data Retention Implementation Working Group[2]. It is important to note, however, that this data set is a compromise with industry participants on what law enforcement and intelligence agencies would like to be retained to aid their investigations. This data set captures the basic categories of telecommunications data critical to many ACC investigations that provide the foundation for other investigatory techniques, such as telecommunications interception or physical surveillance, that allow the ACC to combat serious and organised crime.

[1] At its meeting in November 2013, the ACC Board recognised the importance of the retention of telecommunications data to law enforcement and noted its support for a mandatory data retention regime.
[2] Provided to the PJCIS on 16 December 2014.

Oversight and access

The ACC supports the concept of restricting the range of agencies that can access telecommunications data under the proposed retention regime. The ACC considers that the sensitivity of telecommunications data should be restricted to agencies that play a key role in combating serious criminal activity and national security threats, such as ACC Board members and anti-corruption agencies. The ACC also supports the proposed additional oversight regime by the Commonwealth Ombudsman. The Commission maintains stringent accountability and oversight mechanisms to provide assurance that the access and use of telecommunications material is used appropriately and is in the public interest. Both the restriction of agencies and the oversight mechanisms are important safeguards that go towards the reasonableness and proportionality of the data retention regime as a whole.

Retention period

Currently, the differences in what is retained and the absence of standard retention periods affect the ACC's ability to detect and understand the scope and nature of serious and organised crime, as valuable telecommunications data is not always available when needed. The ACC notes that some sectors, such as the banking and financial sector, have significant existing data storage requirements, enabling them to provide assistance to the ACC with requests for data up to seven years old.

The telecommunications data requested by the ACC is restricted by the retention periods the telecommunications service providers are known to have in place. As a matter of practice, the ACC will not ordinarily seek historical data where it is known that the data for that period would have already been destroyed by the carrier or unable to be retrieved. Presently, the majority of the telecommunications data sought and used by the ACC is subscriber information (including service and carrier status enquiries) and telecommunications service histories (such as call records) less than three months old.

The Commission is supportive of a retention period of a minimum of two years due to the advantage it would provide in investigating serious and organised crime. The ACC recognises the need to appropriately balance the rights to privacy of an individual with the investigatory needs of law enforcement and intelligence agencies and is of the view that a retention period between two and five years achieves that balance.

A minimum legislated two year period would assist with ACC projects, which are currently authorised by the Board for up to three year periods. For example, if a criminal offence which occurred in 2012 was to come to the attention of the ACC, the Commission would have significant difficulty in investigating that offence without access to retrospective telecommunications data. If a consistent retention regime across service providers does not exist, serious and organised criminals will exploit this vulnerability to their advantage.

How the ACC uses telecommunications data

Serious and organised crime groups continue to deliberately impede the ACC's intelligence and investigatory activities. New technologies and counter-measures employed by these groups are

increasingly making it difficult for the ACC to discover and understand organised criminal activity using other investigatory methods. Telecommunications data provides a common source of truth that helps mitigate these challenges.

Telecommunications data is an essential resource in the ACC's role of discovering, understanding and responding to serious organised crime. Inherent in this crime type are complex communication webs which are often only able to be discovered through retrospective analysis of criminality which may span many years. Telecommunications data is both the foundation of, and one of the least intrusive sources of information for, the ACC's other investigative techniques. It enables the ACC to establish the time, general location, and participants involved in telecommunications activity. It is critical for determining the parties involved in serious and organised crime activities, eliminating innocent parties from our investigations and identifying those who may be victims of serious and organised crime.

CASE STUDY – ELIMINATING A PERSON OF INTEREST USING TELECOMMUNICATIONS DATA

An ACC money laundering project identified an active money laundering syndicate controlled from another country. The Australian member of this syndicate was told by his overseas controller to contact an Australian mobile number to collect criminal proceeds. However, the number provided by the overseas controller was incorrect. The Australian syndicate member made contact with the Australian phone number, and on initial examination the communication appeared to be suspicious. A check on the subscriber of the Australian phone and collection of call associated data of the number provided by the overseas controller was conducted. The subscriber check showed that the Australian phone number was subscribed to a person with legitimate details who was not involved with drug distribution or money laundering suspects. Based on this information, the ACC could identify that the user of this service was not likely to be involved in criminality and they were excluded from further enquiries in the investigation.

CASE STUDY – IDENTIFYING A VICTIM OF SERIOUS AND ORGANISED CRIME

The ACC-led Taskforce Galilee was established in 2011 to examine serious and organised investment fraud conducted by offshore boiler rooms. It found that more than 2600 Australians lost in excess of $113 million to serious and organised investment fraud, but it is believed there is a high level of under-reporting and the actual amount is far greater. Telecommunications data was fundamental in detecting the victims of this crime. The ACC was able to acquire telecommunications data related to communications conducted by those offshore boiler rooms through international telephony gateways. This data assisted in identifying Australian citizens who had been in contact with these boiler rooms, and had purchased non-existent or worthless shares and other securities. The ACC was able to inform these individuals of the criminal activity and prevent further financial losses. However, the ACC's ability to identify additional victims of this crime is impeded by the absence of a mandatory data retention regime.

UNCLASSIFIED

CASE STUDY - USE OF TELECOMMUNICATIONS DATA TO IDENTIFY PREVIOUSLY UNKNOWN CRIMINAL ENTITIES

In early 2014, an ACC project identified a transnational criminal syndicate operating a multi-million dollar money laundering scheme. The ACC used telecommunications data to identify members of the syndicate. Firstly, the ACC requested call charge record data for a period of three months relating to the service used by the syndicate leader already known to the ACC. This data provided a history of calls, in addition to the time, date, location and duration of those calls. The ACC then conducted a range of analysis on this data that allowed the ACC to identify other syndicate members and also to discount some persons from the investigation, on the basis that that their connection with the syndicate leader was assessed as legitimate, and not for criminal purposes. As a result of this process, the ACC built a picture of the criminal syndicate's membership, including a greater insight into its composition and hierarchy.

Pursuant to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), each request to access telecommunications data is carefully considered by an Authorised Officer who must be satisfied that the disclosure of the information is reasonably necessary for the enforcement of the criminal law. The ACC also ensures that each request includes the reason for accessing the data and relates to the ACC's mandate in countering serious and organised crime.

Once granted authority to access material under the TIA Act, the ACC has very stringent oversight and accountability arrangements that govern the access, storage and use of that material. The ACC is of the view that the existing authorisation arrangements under the TIA Act establish lawful access to telecommunications data and provide the appropriate balance between protection of privacy and the ability of the agency to conduct its investigations effectively.

Should agencies be required to obtain warrants for telecommunications data?

The ACC is not supportive of having to obtain a warrant for telecommunications data. The imposition of a requirement for the ACC to obtain a warrant to access telecommunications data would have a significant impact on the activities of the agency. The impact would be felt across numerous functions, including administrative, financial and operational.

Interception warrants rely on information obtained from telecommunications data, e.g. subscriber names, evidence that the service is active etc. The ACC would have difficulty meeting the existing warrant threshold to obtain access to content if the agency could not initially refer to findings from telecommunications data. This would necessitate the need for more intrusive and costly techniques, such as physical surveillance, the use of covert human sources and coercive examinations, in order to provide some of the substantiating evidence required to obtain a warrant.

Each application for telecommunications data is evaluated as to the relevance and effective contribution it will likely make to an investigation. However, the consistent use of

telecommunications data in investigations demonstrates its intrinsic and unique value to understanding and responding to serious and organised criminal activity.

It is highly unlikely that using physical surveillance and covert human intelligence sources will provide the ACC with all the information that is currently required to obtain a warrant. The ACC needs service details that are only available from the telecommunications carriers (e.g. subscription details) before it can obtain a warrant.

Warrant applications are resource intensive, both for the ACC as an applicant and for the issuing authorities hearing the applications. A warrant regime for telecommunications data would have the potential to divert issuing authorities from their primary focus of hearing and deciding cases, to being officers of the executive whose primary function is to process large numbers of information requests.

Defining telecommunications data

The ACC supports the drafting of the legislation in its current form and is not supportive of including a definition of 'telecommunications data' within. The ACC's preference is for the Bill to remain neutral in terms of technology and terminology to account for the rapid technological changes the world is experiencing.

Organised criminals now have a diverse array of telecommunications technologies with which they can communicate regarding illicit activity and that are not always able to be intercepted and processed by law enforcement. The environment has changed entirely since the introduction of the TIA Act; organised crime groups no longer rely solely on landline telephone communications to organise and support their activities.

Today, consumers and criminals have an almost unlimited choice of telecommunications service providers, access points to connect to the internet, devices that can be used to communicate and applications to facilitate communication. For example, to communicate using a smartphone, a criminal can use a number of different methods, including but not limited to, traditional mobile telephony, text and instant messaging, voice over internet protocol (VoIP), mobile and VoIP applications, video calling, social networking and email.

Changes in the way communications technology is delivered and used continue to erode the ACC and its partners' capabilities to lawfully intercept the full range of communications, devices and applications used by criminals. This is a gap that can be partially mitigated through the access to, and use of, telecommunications data.

Telecommunications data retention legislation must be sufficiently flexible to ensure data from new, emerging or unknown future technologies that can assist investigations is also able to be retained. Without this flexibility, technology will continue to outpace the legal framework under which the ACC and its partner national security and law enforcement agencies operate.

Cost of data retention

The ACC recognises storage of telecommunications data will impose additional costs on both government and industry, and acknowledges the need for balancing law enforcement needs and the onus placed on industry through the introduction of a mandatory data retention regime. Under the current arrangements, telecommunications service providers use cost recovery means to service law enforcement requirements, covering both access to telecommunications data and warranted interception. The ACC is supportive of continuing these arrangements to ensure it is able to access the information required for investigations, however it is not in a position to fund capital costs that may be incurred by industry.

Conclusion

The ACC supports the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* in its entirety and welcomes the changes to the TIA Act that would support the Commission's mission to discover, understand and respond to serious and organised crime and emerging threats facing the Australian community. The ACC considers its current oversight and compliance regimes to be rigorous, comprehensive and to appropriately balance representing the rights of privacy to the individual with the agency's investigatory needs.