AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Submission to the Parliamentary Joint Committee on Intelligence and Security Review of Mandatory Data Retention

July 2019

Introduction

The Australian Criminal Intelligence Commission (ACIC) welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) regarding the Committee's Review of the Mandatory Data Retention Regime (the Regime) as prescribed under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979 (TIA Act).* The ACIC has also welcomed opportunity to provide information to the Committee via the Home Affairs Portfolio submission.

The significance of access to telecommunications data remains critical to the ACIC. Since implementation in 2015, the Regime has proven effective in balancing the ACIC's vital need for timely and consistent access to telecommunications data, with the need for firm accountability mechanisms to ensure access remains proportionate and transparent. The ACIC has been a proactive user of the Regime, accessing a variety of data types across the mandated data sets.

ACIC role

The ACIC is Australia's national criminal intelligence agency, uniquely equipped with intelligence, investigative, and information delivery functions. These functions help to identify new and emerging serious and organised crime threats and criminal trends, to create a national strategic intelligence picture across the spectrum of crime, to fill intelligence and knowledge gaps and to share information and intelligence holdings to inform national and international responses to crime.

The Transnational, Serious and Organised Crime threat

The adaptable and complex nature of contemporary serious and organised criminality represents a continuing challenge for the ACIC. ACIC intelligence indicates that up to 70 per cent of Australia's serious and organised criminal threats are based offshore, or have strong offshore links. In addition to the unquantifiable damage done to the well-being of Australia, transnational, serious and organised crime (TSOC) is estimated to cost Australia up to A$47.4 billion annually.

Organised crime in Australia is proficient and enduring. It is transnational in nature, technology enabled and increasingly functions as a business: employing professionals; outsourcing key activities such as money laundering; diversifying into multiple criminal markets; and developing strong, consistent revenue streams through involvement in comparatively low-risk activities.

Geographic boundaries no longer contain criminal networks. Increasing access to and uptake of the internet and technology provides serious and organised crime groups with the ability to target thousands of Australians simultaneously from anywhere in the world. Transnational organised crime groups continue to be attracted to and target Australia's lucrative illicit drug market.

The highest threat targets have the skills, knowledge and resources to remain insulated from law enforcement and intelligence efforts and are increasingly aware of or hold a well-founded suspicion about investigations being conducted.

ACIC use of Telecommunications Data

The access to retained telecommunications data afforded by the extant Data Retention Regime is a vital part of the ACIC's day-to-day activities in combatting TSOC. It is a power proportionate to the scale of the threat TSOC poses to Australia. Telecommunications data is both the foundation of, and one of the least intrusive sources of information for, the ACIC's other investigative techniques. Access to telecommunications data is complementary to other legislative tools available to the ACIC, such as those

available under the recently enacted *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.*

The ACIC notes prior to the implementation of the Regime, there were existing requirements for telecommunications data to be disclosed for lawful purposes if it was retained by a provider. The Regime has helped standardise how data is stored, for how long, as well as the process for accessing it. The data the ACIC can access has therefore become more consistent and reliable which has proven critical to investigations. Additionally, by clarifying what is expected of industry, the Regime has improved the efficiency of the ACIC's relationships with industry providers.

Since the Regime came into effect in 2015, ACIC has made approximately 20,000 requests to industry providers to access retained telecommunications data. The majority of these requests have related to data aged three months old or less due to the ACIC's common need to access subscriber information followed by Call Charge Records, although requests have been made for data across the mandatory retention period. For example, in the last year, the ACIC substantially increased its access to telecommunications data retained for a period between six and nine months. A contributing factor to this increase has likely been the growing prevalence of encryption services, which has reduced the utility of other technical capabilities and in turn made access to retained data a larger part of ACIC's activities than was the case in 2015. Instances like this demonstrate that the two-year mandatory retention has provided the ACIC with the capacity to adapt its usage of retained data to respond to changing criminal behaviour.

Access to the telecommunications data mandated in the data set has provided several benefits to ACIC investigations including:

- Providing a powerful tool for identifying and understanding linkages across complex criminal networks. For example, telecommunications data has allowed for the identification of persons performing enabling roles, such as lawyers, accounts and encrypted communications vendors, to multiple criminal networks.
- Assisting to determine peripheral activities to an identified location at a specific time. For example, telecommunications data has been used to gain an understanding of the activities of associates of the person of interest (POI) around the time of the alleged criminal activity.
- Assisting to exclude an individual as a suspect. For example, a suspect who can be identified as being at a different location, using located-based services data, at the time of specific events may be excluded from suspicion.
- Identifying common locations and behaviours. However, due to the increasing adaption of encryption, telecommunications data is also commonly used to identify normal behaviours and events which are out of character.

The benefits of access to retained telecommunications data, as outlined above, have allowed the ACIC to verify existing intelligence, establish new leads of inquiry and uncover new evidence to help counter and disrupt the highest TSOC threats impacting on Australia.

The data set and mandatory retention period

The ACIC is satisfied with the scope of data made available under the Regime and the retention period currently imposed upon telecommunications providers. The data set captures the basic categories of telecommunications data critical to many ACIC investigations that provide the foundation for other investigatory techniques, such as telecommunications interception or physical surveillance, that allow the ACIC to combat serious and organised crime.

The Regime has facilitated access to a greater depth of telecommunications data, however, the uptake of encryption over the same timeframe through use of applications and over-the-top providers such as Facebook and WhatsApp, has confronted law enforcement and intelligence agencies with additional challenges. Further, new technologies entering the Australian market, particularly 5G, will likely give consumers more options to achieve digital anonymity, which will create further significant challenges for intelligence and law enforcement agencies.

Noting this, access to telecommunications data, which enables the ACIC to establish the time, general location, and participants involved in telecommunications activity, is even more critical to determining the parties involved in serious and organised crime activities, eliminating innocent parties from investigations and identifying those who may be victims of serious and organised crime.

The ACIC is mindful that the criminal enterprise is highly adaptive and creative in the adoption of new technologies meaning that the operating environment for Australian intelligence and law enforcement agencies is dynamic and unpredictable. The ACIC notes future reform to legislative frameworks may be required to ensure Australia's Regime remains effective against TSOC and other threats into the future.

Oversight and access

The ACIC considers its current oversight and compliance for use of the Regime to be rigorous, comprehensive and to appropriately balance representing the rights of privacy to the individual with the agency's investigatory needs. The ACIC notes that no recommendations by the Ombudsman have been made to the ACIC since the Regime commenced as a result of any inspections, indicating the ACIC's use has been measured and appropriate.

The ACIC notes a key facet to the benefit of the Regime is in the ability for data to be accessed under an authorisation, providing vital, timely access. This remains appropriate and on balance with protecting privacy. The ACIC notes that any access to the content of a communication must be obtained under a warrant, outside the scope of this Regime, which is reflective and appropriate noting the more intrusive nature of the power.

The ACIC notes that since the establishment of the Regime in 2015 that the ACIC has become part of the National Intelligence Community and as a result, should the proposed *Integrity Measures Bill* pass, will be subject to additional oversight by the Inspector-General of Intelligence and Security. This will add to existing accountability already applied to ACIC's activities, including access to telecommunications data.

Conclusion

The ACIC notes the original need for the Regime was based on the increasing importance of access to telecommunications data, a decline in the availability of lawfully accessed telecommunications data and an increasingly high-risk operational environment. These key facets have not diminished since the Regime's implementation in 2015 and it remains equally critical, if not more so.

The ACIC believes that since the Regime's inception that it has proven to be effective at regulating access in a manner that has not undermined the utility of the data, nor imposed on the privacy of the Australians we seek to protect.

The ACIC notes that the Regime has provided a vital investigative tool which has enhanced the agency's ability to investigate and respond to serious and organised crime threats. A reduction in either the scope of the data sets or retention time would impede the ACIC's ability to maintain pace with serious and organised criminals.

The ACIC notes the operating environment for Australian law enforcement and intelligence agencies is highly dynamic and subject to unpredictable changes as a result of technological evolution. As such, the ACIC notes there may be a future need to adapt the legislative framework to suit the modern operating environment and to continue to provide critical access to telecommunications data.