Submission No 147

Inquiry into potential reforms of National Security Legislation

Organisation: Queensland Crime and Misconduct Commission

Crime and Misconduct Commission

SUBMISSION TO PARLIAMENTARY JOINT COMMITTEE ON PROPOSED INTELLIGENCE AND NATIONAL SECURITY REFORM

Inquiry into potential reforms of National Security Legislation

August 2012

Contents

1 Introduction

The Queensland Crime and Misconduct Commission (CMC) was created with the enactment of the *Crime and Misconduct Act (Qld)* 2001. The CMC was declared an eligible authority within the meaning of the *Telecommunications (Interception and Access) Act 1979 (Cth)* 1979 (the TIA Act) on 8 July 2009. It was at this time that the CMC was first able to apply for telecommunications interception warrants to assist in the investigation of a serious offence.

The activities of the CMC are unique in that they are the oversight body of the Queensland public service and may also investigate major crimes referred to the CMC under one of its general or specific referrals.

The use of telecommunications interception under the TIA Act remains relevant in the ongoing investigation of CMC official misconduct, organised crime and criminal paedophilia investigations.

In responding to the invitation for submissions, our comments are restricted to those areas where the CMC has expertise by virtue of its jurisdiction and investigative experience. In this context, the operational, intelligence and research activities of the CMC are concentrated on state legislative matters as opposed to those matters controlled by Commonwealth legislation.

We have chosen not to comment specifically on some of the terms of reference. In particular, it is our view that other Commonwealth and State based agencies such as the Australian Security and Intelligence Organisation (ASIO) are better placed to provide comment on the proposed reforms to the *Telecommunications Act 1997*, *Australian Security Intelligence Organisation Act 1979* and *Intelligence Services Act 2001*.

2 Interception and the TIA Act

Access to telecommunications remains an important tool in the detection, investigation and prosecution of criminal activity by the CMC. In particular, it is a cost effective investigative tool that supports and complements information derived from other sources.

Both lawfully intercepted information and telecommunications data present a unique and invaluable picture of the associations of a person of interest and often enable law enforcement agencies to secure arrests in circumstances where traditional law enforcement techniques alone would be insufficient.

3 Interception and the TIA Act - Comment

Rapidly emerging technology necessitates urgent reform to the interception regime to ensure agencies operate within a framework that is responsive.

The current interception regime does not seamlessly support the interception of emerging technologies without the need for further legislative amendment. For telecommunications interception to continue to be a useful investigative tool, a framework is needed which focuses more on the interception of telecommunications data.

To achieve a framework that continues to meet the needs of interception agencies, the CMC supports the concept of an attributes based system. The use of an attributes based system will enhance the privacy of users of the Australian telecommunications system by increasing the likelihood of intercepting only that information which is relevant to an investigation. For more detail, please see 3.2.

The CMC faces many challenges maintaining operational effectiveness in lawful telecommunications interception, particularly the challenges posed by rapidly emerging technologies and a significant increase in the use of data communications. These challenges include but are not limited to:

- Rapidly Increasing Data Volumes
- Use of Multiple Data Capturing Devices
- Increasing use of Sophisticated Encryption
- Inconsistent Data Retention Regimes by ISPs and Carriers
- Increasing use of Web Based Software Applications
- The Limitation of a 7 year Offence Threshold
- Information Sharing with Other Agencies and use in Other Proceedings
- Current access/use of Darknets/Anonymisers

3.1 Rapidly Increasing Data Volumes

Data allowances for both home and mobile devices are increasing significantly, as is the speed of those services. Reform which allows for law enforcement to target the type of internet content they wish to intercept will result in less content being intercepted with a higher relevance to law enforcement agencies.

In some investigations for example, the CMC is interested in certain types of internet traffic only (for example, file sharing of child exploitation material). The CMC welcomes reform which envisages the CMC being able to limit its interception to only those file types that are relative to its investigation. The CMC could then avoid having to intercept, process and monitor the irrelevant components of the target's internet traffic.

The CMC can provide detailed examples of the challenges faced by rapidly increasing data volumes *in camera.*

3.2 Use of Multiple Data Capturing Devices

Many of the CMC's targets utilise multiple communication devices or multiple internet connections. Trying to obtain a complete understanding of a target's communications framework can therefore be challenging. In particular, the use of data services over multiple devices and multiple points of connectivity (for example, 3G, 4G and public or private WIFI services) makes the task of law enforcement increasingly complex. TIA Act reform which enables law enforcement agencies to more clearly and flexibly define the telecommunications they wish to intercept by referencing a greater range of attributes would allow for a more complete picture of the communications to be captured.

3.2.1 Example – Use of Multiple Data Capturing Devices

In a recent CMC operation targeting an illicit drug distribution network, the CMC recovered a total of 62 handsets subscribed in false names with interchangeable SIM cards across the life of the 18 month investigation. Twelve of these handsets were recovered from the principal target of which 5 handsets were dual-sim enabled, meaning that the single phone could be used as two distinct services. This methodology was utilised by the principal target and the principals target's associates in an effort to defeat the attention of law enforcement.

The ease with which the principal target and the principal target's associates were able to acquire numerous telecommunications devices significantly impacted on the investigation. In particular, it resulted in significant costs and analytical resources being expended to determine

the true identity of the user of the telecommunications device and to identify new replacement telecommunication devices.

TIA Act reform which allows for more streamlined and efficient identification of new telecommunication devices used by targets would be welcome. This might include being able to identify communication devices by additional attributes (for example, a file type being shared, emails being sent to and/or from a particular email address in addition to a particular handset or internet modem being used).

The CMC can provide more detailed examples of the challenges faced by multiple data capturing devices *in camera.*

3.2.2 Example – Access to Telecommunications Data where Multiple Data Capturing Devices used

If it were proposed to introduce a requirement that telecommunications data retained by a Carrier (for example, call charge records) be available only by warrant, this would result in vital evidence not being identified until well after an offence has occurred where the target is using multiple data capturing devices. It would also result in intelligence gathering being significantly delayed as the warrant application process can take several days to a week to complete.

Having regard to the frequency with which such information is sought to progress investigations, and the speed at which targets can change their data capturing device (for example, a mobile phone service), the introduction of a warrant issued process would also have significant time and human resource implications for the CMC, potentially the Public Interest Monitor and the Issuing Authority.

3.3 Increasing use of Sophisticated Encryption

The increased use of sophisticated encryption presents challenges to the CMC. Internet service providers (ISPs) as well as application service providers (ASPs) are increasingly providing end to end encryption. The fact that ASPs can be located anywhere in the world can make it extremely difficult to seek assistance in the decryption of content that may be vital in an investigation. TIA Act reform that envisages law enforcement agencies being able to request decryption assistance where possible from ISP's, Carriers and ASPs, would potentially allow for greater access to critical evidence.

The CMC can provide examples of the challenges created by encryption *in camera.*

3.4 Inconsistent Data Retention Regimes by ISPs and Carriers

The CMC welcomes TIA Act reform that requires the type of information retained by Carriers and ISPs to be consistent. The CMC also supports reform that ensures consistent information be retained for clearly defined periods of time. There is currently no consistency between ISPs and Carriers with respect to what information they retain and for how long.

3.4.1 Example – Stored Communications – Differing Retention Periods

The stored communications regime is integral for law enforcement agencies to obtain telecommunications evidence proactively. However, the regime is complicated by a lack of consistency between Carriers, for example, the major Carriers currently delete stored communications data on their network between 24 hours and 90 days after being generated by the customer, depending on the Carrier. This can mean that by the time valuable evidence being stored by a particular Carrier is discovered, that Carrier may have already deleted the data. This is particularly problematic in the investigation of Queensland state offences of unlawful trafficking in dangerous drugs and money laundering which are continuing offences that may be charged over a broad date range.

3.4.2 Example – Critical Data not Retained

In some cases Carriers are unable to provide law enforcement with information critically needed to progress investigations. For example, the CMC recently identified significant on-line sharing of child exploitation material by the principal target who declared that he was abusing children. The principal target was based in Queensland. The investigative team provided information to the ISP identifying the internet service being used. The Carrier was unable to advise the CMC of the subscriber details for the principal target, despite the on-line sharing of child exploitation material being less than 24 hours prior. This resulted in the CMC not being able to identify the principal target's precise location or true identity. The CMC estimates that the inability to identify targets for this reason occurs in approximately 1 in every 5 investigations, and the rate at which this is occurring is increasing. From a child protection perspective, this is an unacceptable outcome.

While recognising that telecommunications networks are very complex and contain vast volumes of data, CMC investigations in these types of areas can be frustrated because of a Carrier's or ISP's inability to retain certain types of information. Clearly defined data

retention periods are welcomed by the CMC for the identification of subscribers who use the telecommunications network in furtherance of their criminal activity.

The CMC can provide more detailed examples of the challenges created by inconsistencies between ISPs and Carriers *in camera.*

3.5 Increasing use of Web Based Software Applications

The proprietary formats used by ASPs can make the analysis of the content intercepted from such providers difficult to analyse without assistance from the ASPs. These providers can be located anywhere in the world and assistance is rarely forthcoming. The CMC welcomes TIA Act reform which envisages decoding assistance from ASPs as this would potentially allow for greater access to critical evidence.

The CMC can provide examples of the challenges created by the increasing use of web based applications *in camera.*

3.6 The Limitation of a 7 year Offence Threshold

The 7 year offence threshold does not currently allow the CMC to lawfully intercept communications made in connection with offences of a lesser maximum imprisonment term. This includes most of our criminal paedophilia investigations. For example, in Queensland it is an offence to share child exploitation material or to use the internet to procure a child to engage in a sexual act. Both these offences are liable to a maximum imprisonment term of 5 years which fall below the existing threshold. These are offences however which are carried out over the telecommunications network and create a market for the creation and uploading of images which depict children being sexualised, indecently dealt with or engaged in sexual intercourse.

The CMC welcomes TIA Act reform which reduces the threshold maximum imprisonment term for a serious offence from 7 years.

The CMC can provide examples of the challenges created by the limitation of a 7 year offence threshold *in camera.*

3.7 Information Sharing with Other Agencies and use in Other Proceedings

Being able to share intercepted information with other interception agencies, especially in an emergency, and the use of lawfully intercepted information or telecommunications data in disciplinary proceedings has significant limitations under the current regime.

3.7.1 Example – Information Sharing with Other Interception Agencies

The TIA Act does not currently recognise a mechanism whereby interception agencies can communicate lawfully intercepted information (LII) to another agency or person in the event of a time sensitive emergency or where it is justified in the public interest.

A mechanism whereby interception agencies may communicate LII in the event of a genuine emergency, that is, one that constitutes a serious threat to life or property, would better ensure a real time response to the threat is able to made. Threats to life or property commonly arise in criminal investigations where pre-existing instances of child exploitation, domestic and/or general violence and/or mental health issues exist.

3.7.1 Example – Information Sharing with Non-Interception Agencies

Because of the complex means by which crime is conducted and the lengths to which targets attempt to legitimise their criminality, an investigation may uncover evidence of wrongdoing outside of the scope of the CMC's statutory powers. A mechanism whereby interception agencies may communicate LII or telecommunications data to another person where it is justified in the public interest is therefore welcomed by the CMC.

For example, during an investigation involving the use of peer to peer networks to distribute child pornography material, intelligence may be gathered regarding the target's employment. In the event the target is employed to care for children (for example, a teacher), the CMC is currently unable to share interception information with the Queensland Department of Education, Training and Employment for them to take appropriate industrial action in relation to that employee's continued employment.

3.7.2 Example – Use of Telecommunications Data in Disciplinary Proceedings

It is common for CMC Misconduct Operations to analyse telecommunications data during investigations of misconduct which involve criminal offences. At times, the investigation does not result in sufficient evidence being obtained to commence a criminal proceeding, but

there is sufficient evidence to refer the matter back to an agency to commence disciplinary proceedings. The gravity of the disciplinary matter may be very serious and could lead to the demotion or termination of the officer's position.

As the means by which the CMC can communicate telecommunications data analysed by the CMC to another agency is currently limited to the protection of the public revenue or the enforcement of the criminal law or a law imposing a pecuniary penalty, the analysis could not under the TIA Act be communicated to another agency for the purposes of a disciplinary proceeding. The desired ability to communicate telecommunications data analysis to other agency would enhance the CMC's ability to perform its statutory Misconduct function.

By comparison, the TIA Act provides for the communication of LII back to an agency to commence disciplinary proceedings.

The CMC can provide more detailed examples of the challenges faced by information sharing with other interception agencies and use in other proceedings *in camera*.

3.7.3 Example – Use of Information in Disciplinary Proceedings against Former Officers

In Queensland it is possible for public servants and police officers to have 'disciplinary declarations' made against them after they have resigned from their position. A disciplinary declaration is a finding that, but for the officers resignation, a finding of misconduct would have been made. Police officers and public servants may therefore be the subject of a 'disciplinary declaration' where, but for their resignation, their conduct was serious enough that it may have resulted in their demotion or their dismissal.

Following a Misconduct investigation it is common practice that the officers subject of the investigation are interviewed regarding their conduct. Often it is possible to interview officers under a 'disciplinary interview' during which the officers must answer questions put to them or they may be subject to further disciplinary proceedings. It has been the experience of the CMC that where an officer is faced with strong evidence, including LII, of serious misconduct they will often refuse to participate in the interview and offer their resignation prior to a finding of misconduct being made against them. The current TIA Act does not allow LII to be used by the relevant agency to determine whether a disciplinary declaration should be made. This means officers can leave their employment without a formal record of misconduct having been made against them.

The CMC welcomes reform which would allow LII to be used by agencies to determine whether a disciplinary declaration should be made. This would assist agencies in avoiding employing/re-employing persons who do not have a suitable work history.

3.8 Current access/use of Darknets/Anonymisers

The CMC's Applied Research and Evaluation Division has undertaken an extensive examination of "Darknets" and online market places advertising illicit commodities like the "Silk Road".

The CMC invites the Committee to include Senior Commission Officers to discuss this particular subject *in camera*.

4 Conclusion

We commend the Committee for examining legislative reform to the national security framework in Australia, particularly in response to calls for reform to the TIA Act.

The CMC supports a detailed examination of different legislative options for the strengthening of national security in Australia.

We invite the Committee to include Senior CMC Officers in the public hearings consultation phase of its inquiry into potential reforms of national security legislation.