Submission No 156

Inquiry into potential reforms of National Security Legislation

Organisation: Corruption and Crime Commission of Western Australia

CORRUPTION AND CRIME COMMISSION

Inquiry into Potential Reforms of National Security Legislation:

Submission to Parliamentary Joint Committee on Intelligence and Security

August 2012

CORRUPTION AND CRIME COMMISSION

186 St Georges Terrace
PERTH WA 6000
PO Box 7667, Cloisters Square
PERTH WA 6850

Telephone: +61 8 9215 4888
Toll Free: 1800 809 000
Fax: +61 8 9215 4884
info@ccc.wa.gov.au
www.ccc.wa.gov.au

Table of Contents

INTRODUCTION

The Corruption and Crime Commission of Western Australia ('the Commission') was established on 1 January 2004 to *'combat and reduce the incidence of organised crime; [and] to reduce the incidence of misconduct in the public service'*. In order to perform these functions significant powers have been afforded, including the authority to apply for Telecommunications Interception ('TI') warrants issued under the *Telecommunications (Interception and Access) Act 1979 (Cth)* ('TIA Act'). The Commission is a declared Agency under the TIA Act for the purposes of obtaining TI warrants and operates equipment to facilitate the lawful interception of communications by virtue of such warrants.

Lawful interception and access to telecommunications data offer an effective investigative instrument that supports and complements Commission operations and investigations. The Commission supports the primary objective of the current legislation, which seeks to protect the privacy of individuals who use the Australian telecommunications system, understanding the need for this to be balanced against Australia's law enforcement and national security interests.

The advancement of technology has seen a shift in how people interact and communicate. The original TI Act of the 1970s was aimed principally at intercepting wired voice telephone communications. In 1982 the Internet Protocol Suite encompassing TCP/IP was standardised and the concept of a worldwide network of fully interconnected computers, the Internet, was introduced. Reform to the TIA Act over the years by way of amendments has been necessary but that has unfortunately resulted in duplication and complexity that makes the TIA Act difficult to interpret and implement.

The Commission supports potential reforms of national security legislation and having reviewed the Government's discussion paper "Equipping Australia against Emerging and Evolving Threats" agrees with the broad concepts outlined within the paper and fully supports the requirements for holistic reform to the TIA Act.

SCOPE OF SUBMISSION

The Corruption and Crime Commission of Western Australia ('the Commission') seeks to limit its response contained in this submission to matters relating to amendments pertaining to the following act:

- *Telecommunications (Interception and Access) Act 1979*

Where responses are provided in these sections they support the proposed amendments unless specifically noted to the contrary. Where the Commission has not provided a specific response this is to be considered as general support for the proposed amendments.

RESPONSE TO PART-A – GOVERNMENT WISHES TO PROGRESS THE FOLLOWING PROPOSALS

Telecommunications (Interception and Access) Act 1979

1) Strengthening the safeguards and privacy protections under the lawful access to communications regime in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This would include the examination of:

a) the legislation's privacy protection objective

The Commission supports the primary objective of the TIA Act which seeks to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act does this by making it an offence to intercept communications passing over the telecommunications system. However this needs to be balanced against Australia's law enforcement and national security interests. The TIA Act specifies the circumstances in which it is permissible for law enforcement agencies, including the Commission, to intercept communications under the authority of a warrant, subject to reporting and communications requirements within the Act.

The rapid advancement in telecommunications technology, since the enactment of the legislation in 1979, has seen change not only in the equipment, but also in people's use and expectations of this technology. The Commission supports the proposed legislative amendments accepting that privacy protection objectives could be enhanced with the proposed simplified warrant regime that focuses on better targeting the characteristics of a communication therefore enabling it to be isolated from the communications that are not of interest.

The Commission takes seriously its consideration of its obligations under the TIA Act when executing warrants and lawfully accessing communications. The Commission supports strong penalties in relation to the unlawful access, use or disclosure of private communications or information derived from private information and supports amendments for this improved model.

b) the proportionality tests for issuing of warrants

Strong justification is needed for the interception of private conversations however the TIA Act recognises that there are circumstances where it is appropriate to allow law enforcement or security organisations to intercept telecommunications. In these cases the TIA Act provides a suitable regulatory scheme that ensures any interception of private telecommunications is necessary due to the seriousness of the offence being investigated. The Commission believes that the current arrangements

linking the eligibility of warrants to an appropriate threshold for serious offences provides a simple but fair approach for both agencies and issuing authorities.

c) mandatory recording-keeping standards

The Commission fully supports a robust regime of mandatory record-keeping standards for agencies exercising powers under the TIA Act. The Commission acknowledges that effective oversight of agencies' use of these powers requires appropriate record-keeping standards sufficient to show compliance with the legislation. However it is the view of the Commission that many of the requirements of the current Act create unnecessary duplication of records and the creation of further records which no longer serve the original purpose of ensuring compliance with the Act and the creation of a robust compliance regime. The Commission welcomes enhancements to streamline and reduce the complexity in the law and believes that a review of records necessary to provide a tangible benefit in ensuring a robust regime should be part of any reform to the TIA Act.

d) oversight arrangements by the Commonwealth and State Ombudsman

The Ombudsman has statutory responsibility for inspecting the records of law enforcement and other enforcement agencies in relation to the use of covert powers. Current oversight by the Ombudsman on the Commission's use of powers is split between the Commonwealth and the State Ombudsman. The State Ombudsman inspects the records of the Commission in relation to telecommunications interception, whilst the Commonwealth Ombudsman inspects the records of the Commission in relation to stored communications. The State Ombudsman's Office has demonstrated its capability to maintain a rigorous and professional oversight regime of the Commission's records. The Commission welcomes an intrusive oversight regime to its use of these powers.

2) Reforming the lawful access to communications regime. This would include:

a) reducing the number of agencies eligible to access communications information

The Commission supports the principles outlined in the discussion paper under *'Reforming the lawful access regime'*.

The Commission holds the view that content communications accessed via interception or via the stored communications warrant represent a similar intrusion into privacy and therefore should be captured under the same offence provisions and thresholds.

The Commission does not wish to comment on which agencies should be entitled to access stored communications or intercepted communications. The Commission understands that the serious offence threshold may preclude certain agencies utilising these powers, however the Commission's view is that the content of communications, be it stored or intercepted live, represent differing levels of intrusion into privacy and therefore should command similar thresholds.

The Commission supports the concept of a higher threshold for accessing data associated with communications traffic as opposed to a lower threshold for subscriber information associated with user accounts and services.

The Commission supports the authorisation of this access for the investigation of relevant offences applying to both telephony based and internet protocol based communications.

b) the standardisation of warrant tests and thresholds

The Commission strongly supports the standardisation of warrant tests and thresholds. Eligible offences and thresholds have been somewhat complicated under the current regime. The Commission supports a simplified regime where relevant offences are clearly defined by way of penalty units and sentences as a way of simplifying the warrant process. Similarly, access to telecommunications data should be simply defined with appropriate thresholds to avoid ambiguity in determining the threshold.

3) Streamlining and reducing complexity in the lawful access to communications regime. This would include:

a) simplifying the information sharing provisions that allow agencies to cooperate

The Commission firmly supports reform to the information use and disclosure rules of the TIA Act due to the convoluted nature of the current information sharing provisions.

b) removing legislative duplication

Change in technology has seen many amendments in the current TIA Act. This in some cases has resulted in duplication and complexity that makes the Act difficult to follow. The simplification and removal of legislative repetition will assist with the interpretation of the Act. The Commission supports the suggested reform of the TIA Act with a holistic approach in order to remove this duplication.

4) Modernising the TIA Act's cost sharing framework to:

a) align industry interception assistance with industry regulatory policy

The Commission supports the concept of a tiered model, understanding that the current model was predicated on the existence of only Carriers and Carriage Service Providers all with similar resource backing and generally a large customer base. The reality is that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant. Whilst the Commission understands that uniform obligation is a fairer system, the reality is that the majority of intercepts are executed through the major telecommunications carriers and supports a cost neutral environment for carriers.

b) clarify ACMA's regulatory and enforcement role

The Commission supports the concept of expanding the range of regulatory options available to ACMA and clarifying the standards with which the industry must comply as described in the discussion paper.

NOTE: Parts 5 to 7 relate to the Australian Security Intelligence Organisation Act 1979 and/or Intelligence Services Act 2001 and are outside the scope of this submission

RESPONSE TO PART-B – GOVERNMENT IS CONSIDERING THE FOLLOWING PROPOSALS

Telecommunications (Interception and Access) Act 1979

8) Streamlining and reducing complexity in the lawful access to communications regime. This would include:

a) creating a single warrant with multiple TI powers

The current TIA Act requires various types of warrants to access communications lawfully. Additional types of warrants have been created over the years in response to changes in methodologies and technologies. The resultant system is complex requiring detail to be interpreted by agencies, issuing authorities, oversight bodies, and courts. The Commission supports the concept of a single simplified warrant. The relevant thresholds and privacy intrusions are essentially the same where communications are accessed via service device be they stored communications or intercepted in transit.

9) Modernising the industry assistance framework:

a) implement detailed requirements for industry interception obligations

The current regulatory regime for industry interception obligations is administratively burdensome for both industry participants and the regulatory agency. The current requirement of industry to prepare and submit interception capability plans which are then assessed annually should be reviewed.

The implementation of detailed requirements for industry interception obligations may assist in clarifying requirements and account for technical complexities. The Commission endorses the inclusion of administrative requirements as part of industry interception requirements. In many cases, difficulties or delays in interception are due to administrative, as opposed to, technical limitations.

b) extend the regulatory regime to ancillary service providers not currently covered by the legislation

As communications migrate to IP networks and applications, the lawful access to such communications to investigate serious offences has become more complex and challenging. Communications to further criminal activity are now taking place across

a myriad of ancillary service providers including offshore web based email and social networking applications. The migration of offending behaviour across these networks or applications mirrors the general uptake of these technologies by the Australian public. However, it is often the case that offenders will attempt to use means of communications which they believe are secure or enable them to avoid interception to further criminal activity. In the modern communications environment it is vital that the legislative regime covers the new forms of IP based communications otherwise the ability of law enforcement agencies to investigate serious crime and to adequately protect the public will degrade over time. The Commission supports the inclusion of ancillary service providers to ensure both jurisdictional and technical issues can be addressed.

c) implement a three-tiered industry participation model

The Commission acknowledges that the modern telecommunications industry environment is complex and dynamic and that applying a regulatory regime across such an industry requires some flexibility. The Commission believes that a three-tiered industry participation model could provide scope for a reasonable and more equitable system of industry participation based on the level of assistance required by agencies.

The Commission believes that all service providers should be obliged by law to provide reasonable assistance. Larger providers that are more likely to receive warrants should support a higher capability for support and response.

The Commission believes that a three-tiered model should not be based solely on market share or company size. The Commission would endorse an avenue for agencies to have input into the classification of providers within the tiers under such a model.

NOTE: Parts 10 to 13 relate to the Australian Security Intelligence Organisation Act 1979 and/or Intelligence Services Act 2001 and are outside the scope of this submission

RESPONSE TO PART-C – GOVERNMENT IS EXPRESSLY SEEKING THE VIEWS OF THE COMMITTEE ON THE FOLLOWING MATTERS

Telecommunications (Interception and Access) Act 1979

14) Reforming the Lawful Access Regime

a) expanding the basis of interception activities

The current regime of identifying communication based on services or devices for interception can be restrictive. In the modern telecommunications environment communications can be associated with or described by various identifiers which can be more clinically targeted than by simply specifying device or service identifiers. By expanding the basis of interception activities the Commission believes that better targeting communications associated to particular offending behaviour can be achieved providing greater operational effectiveness and reducing the level of privacy intrusion. Being able to identify particular communications within the service, for example, may allow agencies to exclude or include particular communications through relevant identifiers. For example, if an internet based interception were to be conducted on a user's account the agency may only be interested in particular communications such as those linked to an email address or internet chat protocol. By expanding the basis for interception activity, agencies may be able to exclude other communications thereby better targeting the communications of interest and providing greater privacy protection by excluding other content.

15) Modernising the industry assistance framework

a) establish an offence for failure to assist in the decryption of communications

The Commission supports the establishment of such an offence. Where communications are accessed by agencies lawfully under warrant, and decryption assistance is required the legislation should enforce the provision of assistance and an offence regime for non-compliance.

b) institute industry response timelines

The facilitation of lawful access to communications in most instances is time critical. Where vital evidence needs to be captured immediately due to circumstances, the lack of timeliness for lawful assistance can jeopardise investigations. In the

Commission's experience lawful access can in many cases be instant or in other cases take up to several weeks. The Commission believes that reasonable obligations addressing response timelines is highly desirable within the TIA Act.

c) tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts

Telecommunications data is a fundamental investigative tool within many investigations. Carriers retain some data sets currently for commercial purposes (i.e. call charge records relating to telephony services). There is no requirement for carriers to retain data should their business practices no longer require it. The Commission notes with concern that the discussion paper states that "*some carriers have already ceased retaining such data for their business purposes and that it is no longer available to agencies for their investigations*".

In simple investigations telecommunications data is used to provide information or evidence directly related to the investigation.

In complex investigations telecommunications data is used to build a picture of suspected offences by identifying participants, establishing relationships and levels of contact. The use of telecommunications data to identify methods of communication is a crucial investigative tool.

Agencies will face many challenges as telecommunications technologies migrate to IP networks. Investigations across almost all serious crime types including corruption, counter-terrorism and homicide rely significantly on telecommunications data. Without legislated data retention obligations the degradation of investigative capability will be significant.

NOTE: Part 18 relates to the Intelligence Services Act 2001 and is outside the scope of this submission

CONCLUSION

For the reasons stated in this submission, the Corruption and Crime Commission firmly supports holistic reform of the *Telecommunications (Interception and Access) Act 1979* as proposed by the Government.