Submission No 203

Inquiry into potential reforms of National Security Legislation

Name: K O'Callaghan APM

Organisation: Office of the Deputy Commissioner
Western Australia Police
Police Headquarters
Adelaide Terrace, East Perth WA 6004

Western Australia Police

Inquiry into Potential Reforms of National Security Legislation:

Submission to Parliamentary Joint Committee on Intelligence and Security

September 2012

OVERVIEW

Western Australia Police (WA Police) is one of eight police jurisdictions in Australia and is responsible for policing the world's largest single police jurisdiction covering 2.5 million square kilometres with a structure comprising three regions, 14 districts and 157 police stations.

Our Mission:
To enhance the quality of life and well-being of all people in Western Australia by contributing to making our State a safe and secure place.

WA Police outcomes:

- Lawful behaviour and community safety
- Offenders apprehended and dealt with in accordance with the law
- Lawful road-user behaviour

Contributing to Whole of Government Outcome:
To enhance the quality of life and well-being of all people throughout Western Australia by providing high quality, accessible services.

Community outcomes:

- Improved confidence and trust of the community
- People feeling safer at home and in the community

TELECOMMUNICATIONS INTERCEPTION

Covert or unde**c**lared telecommunications interception is an effective and highly valued tool in the investigation of serious crime. Those involved in criminal behaviour will often communicate with each other by way of telephone, whether by telephone call or SMS text message, and lawfully intercepted communications may assist in the investigation, and prosecution of a serious criminal offence.

WA Police use the powers under the *Telecommunications (Interception and Access) Act 1979* (Cth) ("the TIA Act") to lawfully intercept communications made over the telephone or internet in a covert manner.

Technological change however, has led to an increase in the way that people involved in crime communicate, and this has created new challenges for law enforcement agencies. Advancement in mobile phone technology such as the introduction of the iPhone and Smartphone and the use of highspeed internet usage has meant that the criminal element can use mutiple technologies and frequently changing methodology to communicate, so to avoid detection.

It is apparent that the current legislative framework established by the TIA Act is not sufficient to adequately deal with technological change, and the attempt by the legislature to address such advancements has resulted in an unnecessarily complicated and difficult regime, which can be confusing to follow.

WA Police supports the national reform of security legislation (interception capabilities) to meet the demands of technological change and to ensure that the lawful use of legislative powers will better assist in the investigation of serious crime.

SCOPE OF SUBMISSION

WA Police will limit this submission to matters relating to the following Acts:

- ***Telecommunications (Interception and Access) Act 1979***
- ***Telecommunications Act 1997***

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

It is recognised that the privacy protection objective is a fundamental principle which underlies the TIA Act. It is important to protect the privacy of users of telecommunications services by prohibiting covert access to communications except as authorised by the TIA Act.

WA Police is of the view that the current provisions contained in the TI Act are adequate to ensure a proper balance between the privacy of the individual who uses a telecommunications service, and the public interest in detecting and prosecuting serious offences.

For example, when applying for a warrant under the TIA Act, the issuing authority must be provided details about the likely interference of a person's privacy when intercepting a particular service. This becomes a factor which is considered by the issuing authority when determining whether the circumstances are such that a warrant should be issued.

The introduction of a privacy focus objective clause into the TIA Act is appropriate, and would ensure that privacy protection is a consideration in the interpretation and application of the law.

b) the proportionality tests for issuing of warrants

The proportionality test is viewed as the careful balancing of the public interest in the right to privacy, against the public interest in the detection and prosecution of serious crime. The weight given to each factor will be a matter of judgement for the issuing authority, as well as the ultimate decision of whether or not a warrant should be issued.

It is the view of WA Police that the current provisions of the TIA Act provide sufficient scope for the proportionality test to be properly applied.

c) mandatory recording-keeping standards

Mandatory record keeping is an integral part of oversight and governance, and is necessary to ensure that the provisions of the TIA Act are lawfully applied. Currently, the TIA Act requires record keeping and reporting on

every warrant issued to WA Police. However, the recording and reporting requirements are unduly onerous, and are administratively burdensome. In particular, the dual system of Federal and State oversight has resulted in different record keeping for content warrants as opposed to stored communications warrants.

Further, the current system results in unnecessary duplication of records, for example the requirements for interception under a service warrant, Section 46 of the Act. It is necessary to provide a faxed copy and then a hard copy of the warrant to the provider; a copy of the enabling notice to the provider and to the Attorney General; revocation notice and copy of the revocation notice to the provider and Attorney General, and then provide copies of the warrants and revocations, on a monthly basis to the Attorney General, via the Minister for Police. Further, the Ombudsman requires a screen snap shot from the interception system to prove that we have also disabled the interception on our system at the requisite time to ensure the interception was not outside the scope of the warrant.

For these reasons, WA Police supports an examination of the current mandatory record keeping standards with a view to introducing a more simplistic regime.

d) oversight arrangements by the Commonwealth and State Ombudsman

The TIA Act currently creates a system based on dual oversight by both Commonwealth and State Ombudsman. The role of the oversight body, and the scope of inspection, could be better defined within the TIA Act.

For WA Police, stored communications are inspected by the Commonwealth Ombudsman, annually. Inspections of all other TI Warrants, and the corresponding revocations, destruction of, and associated record keeping, is conducted by the State Ombudsman, on a regular basis.

On occasion, the Commonwealth Ombudsman has made comment on the content of an affidavit in support of an application for a stored communications warrant, and has questioned the appropriateness of the application. WA Police is of the opinion that the determination of the application, and the appropriateness or otherwise of the information contained in the affidavit is a matter for the issuing authority, not the oversight body. It is noted that the issuing authority has the power to receive information in both written and oral form.

An examination of the existing oversight arrangements, the clarity of the role, and the practibility of a single oversight body is supported by WA Police.

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

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

WA Police supports limiting the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so.

b) the standardisation of warrant tests and thresholds

This refers to the implementation of a standard threshold for both content (section 46 or 46A warrant) and stored communication warrants. Currently, a content warrant is limited to an offence that carries a penalty of at least 7 years imprisonment (in addition to other criteria), whereas a stored communications warrant can only be issued for an offence punishable by a maximum period of imprisonment of at least 3 years or an offence with an equivalent monetary penalty.

WA Police is of the opinion that the lesser threshold for a stored communications warrant is appropriate on the basis that the use of a stored communications warrant is less intrusive on an individual's privacy than the use of an interception warrant.

WA Police would support the standarisation of warrant tests and thresholds but does not support increasing the threshold for stored communciations warrants. Rather, it may be beneficial to explore the possibility of the lowering the threshold for interception warrants. It is noted that under the *Surveillance Device Act 1998* (WA) there is no threshold for making an application for a surveillance device warrant. This enables WA Police to make an application with respect to any offence if evidence obtained from the use of a surveillance device would assist the investigation. Although there is no minimum threshold, the issuing authority is required to weigh up the severity of the offence, as one of several factors.

At present, under the TIA Act, it is not possible to obtain an interception warrant with respect to offences which carry a penalty of less than 7 years imprisonment but which may be preparatory to more serious offending. For example, precursor or preparatory crimes could include selling unregistered firearms, pervert the course of justice or stealing a motor vehicle. The ability to intercept communications in relation to precursor offences may assist in the prevention of more serious offending.

WA Police would welcome an examination of the current definition of serious offence and serious contravention contained in the TIA Act (section 5D and section 5E). The current definition is complex and unwieldly, and requires simplification.

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

WA Police is of the view that the information sharing provisions of the current TIA Act present a barrier to effective information sharing both within the agency and between WA Police and other agencies.

Under the current provisions of the TIA Act, law enforcement agencies such as WA Police, can only obtain and use evidence in relation to the serious offence or serious contravention being investigated and for no other purpose. Once the information has been used by the agency, it must be destroyed. The current provisions of the TIA Act are too restrictive.

WA Police supports an examination of the provisions in the TIA Act that set the parameters around the disclosure and use of lawfully intercepted information.

From a policing perspective, there has, in recent years, been a shift in the nature of much offending from localised to cross jurisdictional (and international) activity. To effectively investigate, and gather evidence for the prosecution of such criminal activity, it is important that there is a focus on effective information sharing between agencies. The ability of agencies to share information for purposes beyond the serious offence that is being investigated is, at present, unclear.

Further, WA Police would support the use of lawfully intercepted information for the purpose of intelligence sharing which could ultimately result in the detection of a future unrelated serious offence.

To this end, WA Police welcomes an examination of the current definition of permitted purpose, and how this term has been interpreted and applied in practice.

b) removing legislative duplication

There have been a significant number of amendments to the TIA Act, most likely precipitated by changes in technology, and some of these amendments have caused duplication in some areas. In addition to legislative duplication, some provisions contained in the TIA Act are outdated and are difficult to apply.

In a recent District Court (WA) trial, the Judge, in relation to a number of intercept warrants ruled that in accordance with the TIA Act that both notification of the warrant and a certified copy had to be received by the carrier before any intercept was admissible. Effectively therefore, any

interceptions made before the certified copy was received by the carrier were ruled inadmissible.

This ruling is significant for WA because the provision of a certified copy to a carrier requires it to be sent interstate by way of overnight courier, and at considerable cost. Important evidence may be lost between the issue of the warrant and the receipt of the certified copy by the carrier.

WA Police supports the suggested reform of the TIA Act in its entirety, for ease of understanding and in order to remove duplication. Further, there is a need to update the content of the TIA Act to ensure that the provisions are practical and responsive.

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

a) align industry interception assistance with industry regulatory policy

WA Police understands that uniform obligation is a fairer system, however supports the concept of a tiered model, as smaller providers generally have fewer customers and therefore less potential to be required to execute an interception warrant.

b) clarify ACMA's regulatory and enforcement role

WA Police supports the concept of expanding the range of regulatory options available to ACMA and endorses the clarification of the standards within 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 creation of a single warrant with multiple TI powers would provide the flexibility to cater for future technological change by having a focus on communications made by an individual rather than the specific technology or equipment used.

WA Police is of the view that the use of a single broad based warrant would simplify an otherwise overly complicated regime. At present, the TIA Act provides for 6 different warrants (service warrant, b-party interception warrant, named person warrant, device based interception warrant, section 48 entry onto premises warrant, stored communications warrant), each of which have specific applicability. The application of the current warrant regime has the potential to cause confusion as police officers are often unsure about which warrant best suits the needs of a particular investigation.

WA Police supports the introduction of a single warrant for the purpose of lawfully intercepting a person's communications over a telecommunications network.

9) Modernising the industry assistance framework:

a) implement detailed requirements for industry interception obligations

It is the view of WA Police that the current requirement for industry to prepare and submit interception capability plans which are then assessed annually should be reviewed, and supports the inclusion of administrative specifications as part of industry interception requirements and obligations.

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

WA Police supports the inclusion of ancillary service providers to ensure jurisdictional and technical issues can be addressed.

When communication systems were conducted over telephone networks only, as was the case when the TIA Act was written, there was no question as to who was responsible for supplying the interception points. It is no longer simply the case of going to just one telecommunications provider to intercept a persons' communications. It is now quite feasible for someone to be

subscribed to one provider for their telephone traffic and another provider for their Internet. Further, other providers might provide a Voice Over IP (VOIP) telephone service which then utilises a network, or multiple networks of multiple providers to get from point a to point b.

Intercepting an individual's communications is no longer a simple exercise of only going to the major identified service providers. Regardless of the provider, it should be possible to intercept related Internet traffic for the purposes of investigating serious criminal activities.

c) implement a three-tiered industry participation model

WA Police supports the proposed multiple tier model for interception capability and reporting capability based on the volume of traffic that the provider has across their network system. The important thing is that there should be a means to enforce all service providers to have an interception capability.

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 which has a focus on intercepting equipment (service or device) has its limitations. It is the view of WA Police that the interception regime could be broadened by focusing on the interception of an individual and that individual's private conversations over a telecommunications network.

It is acknowledged that this would reflect a change in the current underpinnings of the TIA Act.

15) Modernising the industry assistance framework

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

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 is supported by WA Police.

b) institute industry response timelines

WA Police supports the introduction of industry response timelines.

It is important that telecommunication carriers are capable of dealing with urgent requests for communications data. This is particularly relevant when dealing with stored communications data. It is the practice of some carriers to purge such data after a short period of time. To ensure that evidence is not lost, carriers must have the capability of immediately responding to requests from law enforcement agencies to preserve the data, or alternatively they must have a reasonable ability to store data to until the completion of a police investigation.

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

WA Police supports this initiative to enforce the service providers to retain their data. Currently, the only retention regime in existence is what the service providers have voluntarily implemented. There is no formal period of compulsory retention, which suggests access to data is unreliable, and may impede serious investigations.

Telecommunications interception and associated data is an often utilised investigative tool, and it is important that a reasonable retention regime is put in place to enforce the service providers to not delete their data.

WA Police would applaud a regime that would enable investigators reasonable access to all telecommunications for a defined period. Due to the protracted nature of serious investigations, a minimum retention period of 2 years is considered appropriate.

Telecommunications Act 1997

16) Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

a) By instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference

Advances in technology have resulted in a greater ability for the criminal element to interfere with, and manipulate the telecommunications networks. Appropriate legislative measures should be put in place to ensure that carriers protect networks from cyber attack. WA Police supports the proposed compliance framework, which will address these vulnerabilities in the telecommunication industry networks.

b) By instituting obligations to provide Government with information on significant business and procurement decisions and network changes

This initiative is supported by WA Police.

c) Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers

In the interest of increased community security and to ensure the protection of the telecommunications industry, WA Police supports this proposal.

d) Creating appropriate enforcement powers and pecuniary penalties

WA Police supports the introduction of an appropriate pecuniary punishment framework to ensure compliace with matters of national security.

NOTE: Part 17 relates to the ASIO Act and 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, WA Police supports reform of the *Telecommunications (Interception and Access) Act 1979,* and the *Telecommunications Act 1997,* as proposed by the Government.