



Western Australia Police

Inquiry into Potential Reforms of
National Security Legislation:

Recommendations from the Parliamentary
Joint Committee on Intelligence and
Security:

Submission to Legal and Constitutional
Affairs Reference Committee

February 2014

Submission by Western Australia Police

OVERVIEW 3
SCOPE OF SUBMISSION 5
CONCLUSION 8

Submission by Western Australia Police

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

Submission by Western Australia Police

TELECOMMUNICATIONS INTERCEPTION

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 communicate, and this has created new challenges for law enforcement agencies. Advancement in mobile phone technology such as the introduction of the iPhone and Smart phone, and the use of high speed internet usage has meant that people can use multiple 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 to address such advancements has resulted in a complicated regime, which sometimes 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.

Submission by Western Australia Police

SCOPE OF SUBMISSION

WA Police will limit this submission to discussion and comment relative to the recommendations of the Parliamentary Joint Committee on Intelligence and Security *Inquiry into Potential Reforms of National Security Legislation* report, dated May 2013. This submission relates only to the following Acts:

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

Submission by Western Australia Police

The Parliamentary Joint Committee on Intelligence and Security *Inquiry into Potential Reforms of National Security Legislation* report, dated May 2013, has been considered by WA Police, who are supportive of the 42 recommendations of the inquiry, in the context of:

- The need to ensure that intelligence, security and law enforcement agencies are equipped to effectively perform their functions and cooperate effectively in today's and tomorrow's technologically advanced environment;
- The desirability of comprehensive, consistent and workable laws and practices.

This submission provides further comment on 7 of those recommendations.

Recommendation 2:

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; nonetheless we would support a review of this area.

It is considered that applying one proportionality test across all applications within the TI act seems inappropriate. Data Applications and Stored Communications Warrants currently only require a "serious contravention" as defined by the Act (i.e. 3 years imprisonment), however to obtain a TI Warrant the investigation of a "serious offence" (i.e. 7 years imprisonment) is necessary.

WAPOL believe the degree of proportionality should reflect the seriousness of the offence and the subsequent application within the act. It is considered that the application of a single consistent proportionality test across Interception, Stored Communications and Communications Data would not be able to be appropriately applied across the three areas which have significant differences in levels of intrusion of privacy of an individual.

Recommendation 3:

WA Police suggest that reporting requirements as set out in sections 94(2), 94A & 94B of the Act, be amended to include an evaluation by the investigator relative to the effectiveness of the interception, including whether the privacy intrusion was proportionate to the public outcome sought.

Recommendation 4:

WA Police supports a review with intent to simplify the oversight arrangements to ensure accountability and compliance under the TI Act. At present the State Ombudsman has oversight for TI warrants, the

Submission by Western Australia Police

Commonwealth Ombudsman for Stored Communications warrants, and little or no oversight in regards to Data Applications (both historic and prospective).

An examination of the existing oversight arrangements, the clarity of the role, and the practicality, consistency and continuity of an inspection regime administered by a single oversight body is supported by WA Police.

Recommendation 6:

WA Police considers that the current thresholds for access to content of communications for serious offences and serious contraventions are sufficient. The current thresholds applied to Interception and Stored Communications are suitable and relevant to the degree of intrusion of each type of access.

WA Police would support the standardisation of warrant tests and thresholds but does not support increasing the threshold for Stored Communications warrants.

Recommendation 7

WA Police supports the recommendation that interception be conducted on the basis of specific attributes of communications (i.e. specifying a particular email address or account within an entire IP flow.) We also support the ability to vary the attributes within the course of the investigation, similar to the existing named person warrant model, although at present it appears that neither the carriers or WAPOL have the ability nor the technology to be able to isolate or deliver only the identified attribute.

If this technology is not available and a warrant is obtained and served on a carrier for an identified attribute, it is unclear if the requesting agency would be entitled under warrant to receive/be in possession of all communications and data whilst “sorting through” the data to locate and extract the desired attribute.

Further, should an agency be required to ingest and store all data in order to isolate and extract a specified attribute, a specific storage and destruction regime be considered for implementation, and the relevant oversight body allocated responsibility to provide guidance and ensure compliance.

Should a recommendation evolve from this review, WA Police and other agencies may require time to engage our interception system vendors to ensure our systems are capable, compatible and compliant with the amended legislation in this area.

Submission by Western Australia Police

Recommendation 10:

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 supports the recommendation to develop a single warrant regime. The support is predicated on the basis that a single threshold is lowered to cover “serious contravention” applications, not raised to the threshold for “serious offences” applied to all applications.

Recommendation 42:

WA Police fully supports the introduction of a mandatory data retention regime as this would provide consistency across all telecommunication providers when accessing stored data to assist during investigation of serious offences.

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 ensure service providers do not delete 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. Due to the protracted nature of serious investigations, a minimum retention period of 2 years is considered appropriate.

Consideration would need to be given to the cost impact on Law Enforcement Agencies, should the cost to reimburse the providers be passed on to the interception agencies as part of a cost sharing agreement.

CONCLUSION

For the reasons stated in this submission, WA Police supports reform of the *Telecommunications (Interception and Access) Act 1979*.