NSW Police Force
www.police.nsw.gov.au

16 February 2015

Mr Dan Tehan MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Sir

Provision Of Further Advice to the Parliamentary Joint Committee On Intelligence & Security (PJCIS) in Relation to the *Telecommunications (Interception & Access) Amendment (Data Retention) Bill 2014.*

I write to you following the joint appearance of representatives of Victoria Police, South Australia Police and New South Wales Police before the PJCIS on 30 January 2015 in relation to the *Telecommunications (Interception & Access) Amendment (Data Retention) Bill 2014.*

As a result of evidence provided on 30 January 2015, the PJCIS invited the three agencies present to canvass the unrepresented law enforcement agencies with a view of providing a consolidated response and clarification in relation to two issues – firstly, extending the retention period for three defined sets of metadata from the proposed two years to seven years and secondly, removing the proposed exemption for certain WI-FI providers from retaining metadata.

This is a response comprising the agreed position of all State and Territory jurisdictions being Victoria Police, South Australia Police, Western Australia Police, Northern Territory Police, Queensland Police, Tasmanian Police and New South Wales Police.

Enclosed are the responses received from those agencies commenting on specific recommendations. It should be noted that due to the short time frame not all agencies were in a position to provide more detailed responses. The recommendations are:

Special Services Group
Building 1 Level 1
30 William Holmes Street POTTS HILL NSW 2143
Telephone 02 9780-0300 Facsimile 02 9780-0306 ENet 73300 EFax 73306 TTY 9211 3776 (Hearing/Speech impaired)
ABN 43 408 613 180

1) **That all police jurisdictions support a uniform Data Retention Bill enforcing the retention of metadata for a period of two years for the majority of data sets (please see point 2).**

The Data Retention Bill will ensure access to specific telecommunications data from all Carriers is consistently held for periods of up to two years.

2) **That police jurisdictions support an extended data retention period of seven years for access to particular data sets comprising CCRs, RCCRs and subscriber information.**

The combat of serious and organised crime along with national security investigations requires access to telecommunications data both for an immediate response and from a historical perspective. Police jurisdictions have provided commentary and case studies demonstrating the need to retain telecommunications data for periods much beyond two years for certain data sets.

The New South Wales Police Force has tabled evidence to the PJCIS on 30th January 2015 which outlined the need to access telecommunications data for periods in excess five years. These crimes involved unsolved homicides, historical sexual assault and child abuse matters, armed robbery and kidnapping investigations to name but a few. Further evidence from Victoria and Queensland's Police responses is provided for the information and consideration of the PJCIS (as enclosed).

It is submitted that these crimes are relevant to all police jurisdictions and are complex and significant crimes to investigate necessitating access to relevant telecommunications data. Further, the data sets sought are currently available to law enforcement for periods up to 7 years with certain carriers and this is of great assistance to law enforcement. Any period of less than 7 years for those data sets would potentially be a retrograde step for law enforcement and impact on the success of criminal investigations.

3) **That police jurisdictions support the proposition that Wi-Fi providers should not be exempted from retaining data under the provisions of the Data Retention Bill 2014.**

In Australia, the rate of publically available free Wi-Fi spots has increased significantly over the past few years. Wi-Fi zones now exist in a number of City Council public spaces such as pedestrian malls, parklands and also on entire public transport networks. These locations are in addition to single access Wi-Fi locations such as restaurants, libraries, higher educational institutions and sporting stadiums.

The increased availability of free network access poses obvious risks in terms of being able to solve crimes that are facilitated or committed using telecommunications devices roaming and operating on these Wi-Fi networks.

There are numerous instances in which police agencies have been unable to identify offenders who have utilised insecure Wi-Fi networks to exchange peer to peer child

exploitation material and to groom children using social media. These instances have occurred using insecure private Wi-Fi networks and in internet cafes. Whilst the security protocols of most corporate or government operated Wi-Fi networks afford a level of protection over some of these offences being able to be committed, it would be naïve to assume that exploitation of these networks is not possible, especially as technology advances, software becomes readily accessible and security flaws can be exploited. (Sourced from Queensland Police submission)

4) **That all police jurisdictions support their current oversight and compliance frameworks.**

Currently, the dual oversight role involving Commonwealth and State Ombudsman over telephone interception and stored communication records under the Telecommunications (Interception and Access) Act 1979 has caused duplication, some confusion and complexity with agencies compliance and internal practices regimes. A more pragmatic and consistent approach would be to have a single oversight authority perform the compliance role in each jurisdiction.

Due to the sensitivity of some of the case studies provided by Victoria Police and Queensland Police we would be grateful if you could treat these as "confidential" and not released publicly.

If you require any further information involving this consolidated response, could you please contact Detective Superintendent Arthur Kopsias APM, Commander Telecommunications Interception Branch, New South Wales Police Force via email to

Yours faithfully,

M. A. Lanyon APM
Assistant Commissioner
Special Services Group
New South Wales Police Force

PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

SUBMISSION 202

THE COMMITTEE HAS RECEIVED ADDITIONAL MATERIAL FROM STATE AND TERRITORY POLICE FORCES.

CONTENTS OF THESE DOCUMENTS ARE CONFIDENTIAL TO THE COMMITTEE