# *New South Wales Police Force*
# *Submission to the PJCIS.*
# *Review of the Mandatory Data Retention Regime*

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

30 July 2019

Committee Secretary,
The Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Committee Secretary,

***PUBLIC SUBMISSION BY THE NEW SOUTH WALES POLICE FORCE***

***TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY***

***'PUBLIC SUBMISSION'***

The New South Wales Police Force welcomes the invitation to respond to the Parliamentary Joint Committee on Intelligence and Security (*'PJCIS'*) into review of the mandatory data retention regime proscribed by Part 5-1A of the Telecommunications *(Interception and Access)* Act 1979 *('TIA Act')*.

As part of this review, the New South Wales Police Force Executive corporately approved an internal working group of senior and experienced investigators and stakeholders from specialised units to share their views, and to build case examples to assess the appropriateness of the data sets provided under Section 187AA of the *'TIA Act'*. The working group also reviewed the appropriateness of a mandatory data retention period pursuant to Section 187C of the *'TIA Act'*. From that review, the working group found that without doubt, a mandatory data retention is required from a law enforcement perspective.

In this respect, a specific major investigation will be referenced to provide supporting evidence for the retention of the data. Any conclusion drawn for the value of data retention will rely only on the factual evidence provided herein for the consideration of the *'PJCIS'*.

In response to this review, the submission will incorporate responses within its terms of reference. In particular, this Agency will respond to the following *'PJCIS'* references:

Part 1: The appropriateness of the dataset and retention period;

Part 2: Statistical evidence of the NSWPF for the purposes of Section 187N of the *'TIA Act'*.

# *New South Wales Police Force*
# *Submission to the PJCIS.*
# *Review of the Mandatory Data Retention Regime*

## ***PART 1: THE APPROPRIATENESS OF THE DATA SETS AND RETENTION PERIOD.***

*Introduction and Overview*

During the 2017-2018 financial year there were **2608** evidentiary certificates requested by NSWPF for Meta Data requests pursuant to the *'TIA Act'*. From the introduction of the retention period, it was calculated that between October 2015 and June 2018 there were **18,269** Evidentiary Certificates requested for Meta Data by NSWPF. I

It is acknowledged within this organisation that the facilitation of this type of evidence is an important corroborate tool in proof of the offence prosecuted. Records of this agency show that between October 2015 to June 2018 there were a reported **300,000** requests for meta data. The data aged **over two years amounted to 2755 requests**.

*A summary of the usefulness of 'Meta Data'*

As an overview, the NSWPF respectfully submits that the usefulness of Data Sets pursuant to Section 187N of the *'TIA Act'* can be summarised as follows:

1) *In numerous cases, the use of Meta Data becomes the first point of call for the commencement of an investigation;*
2) *The data provides independent corroboration of witness accounts (ie an independent account for presence at the scene of the crime). This is an important tool when investigating matters such as historical sexual assault matters and other serious offences;*
3) *The 'meta data' is a tool to provide for further investigative opportunities to corroborate 'presence' before, during and or after the crime. Ie Telecommunications Records show a route of travel by a known target. Further analysis may show presence in a location overnight (R v Holdom). Further opportunities then arise to ascertain visitation to local motels/hotels, and CCTV footage;*
4) *The data is an independent and highly reliable form of evidence in judicial proceedings;*
5) *The data can refute alibi evidence. This particularly applies when an accused gives their version for the first time in proceedings after delay in offering an alibi between arrest and trial;*
6) *The data is an investigative tool to use in active surveillance operations in the gathering of evidence of the commission of the offence;*
7) *It is an investigative tool which can be used in the arrest of known offenders;*
8) *It is an investigative tool that can be used in the identification of other unknown offenders in the commission of serious crime;*
9) *The data can then be used as evidence that supports application for search warrants, telephone interception and other surveillance opportunities for further investigation.*

### ***Presence of Meta Data for investigative purposes***

The value of meta data cannot be overstated in the investigation of serious offences conducted by this agency. A case on point is *R v Holdom.*

# *New South Wales Police Force*
# *Submission to the PJCIS.*
# *Review of the Mandatory Data Retention Regime*

*Case Example Number 1: Strike Force Malaya. Offence - Homicide*

On 29 October, 2010 skeletal remains were located on the Red Arm Creek fire trail in the Belanglo State Forest, NSW. Forensic examination identified that the remains were that of a female aged between 13 and 25 years at the time of her death. It was determined that the remains could have been in the forest for between 6 months and 10 years. The victim had suffered numerous broken ribs.

On 15 July, 2015 skeletal remains were located in a suitcase on the side of the Karoonda Highway about 1.5 kilometres west of Wynarka in South Australia. The remains were identified as being that of a young child and were located with various clothing items.

In October 2015, Investigations confirmed the identity of both sets of remains through DNA. Strike Force MALAYA was established by the NSW Police Force Homicide Squad to further investigate these matters in conjunction with the South Australia Police Major Crime Investigation Branch Task Force MALLEE.

The discovery of the identity of the victim turned the focus of the investigation onto Daniel HOLDOM, the previous partner of the older deceased person.

Enquiries into the victims established the woman and her daughter were reported missing by the woman's mother in the Northern Territory on 4 September 2009. However, it was Identified through various other records that the woman left the ACT in December 2008 and there were no records of her being seen since that date.

*Significance of telephone records in establishing victim/offender activity*

In October 2015, phone records were obtained for both the victim and target's mobile phone services. By this stage of the investigation it was almost seven years since the date of the disappearance of the two victims.

The victim and offender's phone activity and cell tower activations were crucial to this investigation.

Critically, the phone records were able to establish the following;

- *Both the victim and target's phone showed travel from the ACT to Sutton Forest on 15 December 2008. Sutton Forest is directly adjacent to the Belangalo State Forest, therefore, placing both phones in the vicinity of the crime scene where the first body was discovered.*

- *The target's movements were then traced back to the ACT where he picked up the second victim, being the daughter of the first victim. From there his cell tower activations showed travel to South Australia. The route of travel was able to be mapped through the cell tower activations, enabling investigators to identify further locations to extend their canvas. These records together with financial records helped identify a Motel in Nerrandera where the target took the child. This motel is believed to be the location where the child was murdered. Physical evidence was located at this site, linking it to the crime scene where the child's body was discovered.*

- *The target and victim IMEI and SMS records also provided evidence of the target using the victim's phone after the murders to give the impression that both victims were still alive. The target used the deceased woman's mobile phone to send text messages to members of her family, including her mother. A flurry of SMS records were identified, in particular just after police made contact with the target, during the missing person investigation in September*

*2009. The victim and target's phone records also showed that the target's handset was used to send messages from the victim's number. Furthermore, on occasions, location data showed that both the victim and target's services were in the same locations at the time the victim's service made contact with her family.*

*The Outcome*

On 28 October 2015, Daniel James HOLDOM was charged with the murder of the woman. HOLDOM was later charged on 15 December 2015 with the murder of the woman's daughter.

HOLDOM pleaded guilty to the homicide offences one week prior to the commencement of the trial. HOLDOM received two life sentences for the murders.

On the basis of this evidence, telecommunications data was obtained over approximately seven years. The use of telecommunications data played a crucial role in the investigation, prosecution and conviction of HOLDOM.

This agency can provide numerous examples of the value of the use of 'meta data' and its value in the prosecution of serious criminal matters.

*Case Example Number 2: Unsolved Crime: Forensic Evidence & Technical Services Command*

The NSWPF uses the National Automated Fingerprint Identification System (NAFIS), which is a fingerprint and palm print database and matching system, used by police agencies to help solve crime and identify individuals by establishing a person's identity from fingerprint and palm impressions. NSWPF adopted the NAFIS in 2001, with previous prints since the 1980s being transferred over to NAFIS.

As of November 2018, NSWPF have reported **377,300** criminal cases for which fingerprints and palm impressions have been obtained with no profile matches to date. Nationally **1,420,549** criminal cases remain outstanding. The criminal offences relate to volume and major crime which date back to the 1980s.

These unmatched profiles may relate to a number of serious investigations that are suspended until further evidence is obtained. It may take a number of years before a match is made, and the investigation can progress. Telecommunications data becomes of significant value to assist in corroboration of the evidence on hand. That is, the movement of the offender before, during, after the offence, and their network etc.

Basically, at an unknown point in time, a NAFIS match can be made, requiring Telco data to corroborate evidence to assistance in the prosecution of the offender.

A case illustration is that when DNA Evidence is obtained, a common issue is the point in time that the offender attended the scene e.g. Break Enter and Commit Serious Indictable Offence as alleged by the prosecution. Meta Data may provide that key as to the person's presence within that area at the time of the commission of the offence. It may also refute evidence of alibi given in this respect at trial.

*New South Wales Police Force*
*Submission to the PJCIS.*
*Review of the Mandatory Data Retention Regime*

*Case Example Number 3: Missing Persons*

The NSW Police Force currently has **202** recorded long-term missing persons between 2012 and 2018 (long term being longer than three months). Of these, eight are flagged as suspicious with another 17 listed as possible homicides. Additionally, 17 cases are flagged as potential suicides (no body recovered). A spreadsheet of those 202 missing persons can be provided.

Due to the historical nature of these matters, meta data is crucial in the further investigation of offender and victim movements at the time a victim goes missing. Persons may also be ruled out of the investigation through this process.

Since the introduction of the retention period, there were 99 requests for meta data relating to serious criminal investigations involving Homicide (and related offences) and 29 requests for meta data concerning Sexual Assault (and related offences).

*Conclusion of the NSWPF Working Group*:

A review of the statistical and information holdings of this agency reveals that historical metadata has in fact been requested for up to a period of 14 years from the requested date of application.

**Attached to this submission is the NSW Police Force, 2015/16 Financial Year, 2016/17 Financial year and 2017/18 Financial Year records in compliance with S187N(3) of TIA Act and section 186(1)(e) to (k).**

We respectfully thank the Committee Secretary and The Parliamentary Joint Committee on Intelligence and Security for considering this submission.

Yours faithfully,

**Arthur KOPSIAS APM**

**Detective Superintendent**

**Chair: NSW Police Force**

**Data Retention Working Group**