Police Federation of Australia
The National Voice of Policing

ABN 31 384 184 778

Level 1, 21 Murray Crescent
GRIFFITH ACT 2603

Tel: (02) 6239 8900
Fax: (02) 6239 8999

19 January 2015

Chairman
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

dataretention@aph.gov.au

POLICE FEDERATION OF AUSTRALIA SUBMISSION:
TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014

The Police Federation of Australia's submission on this important Bill follows. We have no objection to our submission being published by the Committee and are prepared to give evidence if that is your Committee's wish.

INTRODUCTION

The Police Federation of Australia (PFA) represents the nation's 58.000 police officers in each of the States and Territories and the Australia Federal Police. We believe it is in the interests of those officers, and the Australia community they serve, to have the most effective law enforcement tools and capabilities possible to ensure public safety.

In the case of the data retention regime the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Data Retention Bill) aims to put in place, the PFA is convinced that the proposals are essential and urgent.

TELECOMMUNICATIONS CONTENT IS DIFFERENT

It is important first to distinguish access to metadata, from access to telecommunications **content** such as telephone conversations or email exchanges and text messages, which in virtually all cases require a warrant from a Judge or Magistrate or nominated AAT member (i.e. interception (real time surveillance) and stored communication warrants). A warrant is required in such cases because access to private communications between people in a democracy like ours is an intrusive measure. It intrudes on the privacy of the individuals concerned, their views, their ideas, and their conversations. Because it is such an intrusion,

special safeguards have been put in place in the law to ensure this power is not misused or abused. The warrant system is an important and central safeguard, but it must be recognized that it is time consuming and expensive for police services to operate under, making the cost of such surveillance techniques an increasing burden on police budgets.

The Attorney-General's Department **Annual Report for 2012-13 on the *Telecommunications (Interception and Access) Act 1979*** shows that the recurrent cost to Australia's police agencies of telecommunications interception warrants in that year was around **$50.9 million**. This does not include the cost to agencies of stored communication warrants, or the costs incurred by the judicial system. Of that $50.9 million, more than **$8 million** was paid to the telcos for access.

The warrant system for limited law enforcement access to the **content** of communications remains unchanged.

In the PFA's view access to metadata, and data retention by telecommunications companies to enable that access, is quite different.

WHY IS DATA RETENTION ESSENTIAL?

State and Territory police services are by far the most extensive users of the metadata held by telecommunications companies. They request access to that data, **case-by-case in a targeted manner**, on a daily basis in their law enforcement work and criminal investigations.

The Annual Report referred to above shows that law enforcement agencies accessed metadata relating to existing information (as distinct from prospective data) 312,929 times in 2012-13. The greatest use was by the NSW Police which accessed data under 119,705 authorisations. The AFP, a much smaller force, had 25,582 authorisations. Of the total Australia-wide in 2012-13, 895 authorisations were in relation to missing persons. These statistics demonstrate how important data access is to law enforcement.

Contrary to claims by some commentators, the authorities do not simply have carte blanche to track the metadata of Australian residents willy nilly, nor would they have the time, the funds or the inclination to do so. It is worth reminding those making such claims that each request to the telcos for metadata access, costs the police services real scarce funds. It is estimated that metadata from one cell site for one hour from a telco costs between $30,000 and $50,000.

Access to metadata is an essential policing tool. On the one hand it is frequently used to eliminate people from ongoing investigations because the data demonstrates that the person concerned was not, at the relevant time, in the relevant place or did not communicate with the suspect. Thus it narrows the field of suspects.

On the other hand it assists police to establish people involved in a particular incident, relevant connections between individuals involved, the movement of people at particular times, and the incidence of communications between such people.

Access to metadata is critical in cases such as missing person investigations, fraud and corruption, illegal drug and firearms investigations, pedophilia, sexual slavery and child abuse and child pornography inquiries, cybercrime offenses, murder cases, serious and organized crime investigations and terrorism incidents.

It is used both as a vital investigatory tool in the preliminary stages of a suspected offence (and to support subsequent warrant applications) and an evidentiary aid in prosecutions for such offences. It has proved important in both emerging criminal cases and in "cold cases" being further investigated which is why data retention for at least two years, preferable five years, is so important. Many highly complex cases are resolved using metadata going back some five to seven years according to senior police and ASIO officials so limiting data retention to two years is shortsighted in our view.

As AFP Commissioner Andrew Colvin reported in evidence to your committee, metadata was "used in 92% of counterterrorism investigations, 100% of cybercrime investigations, 87% of child protection investigations and 79% of serious organized crime investigations". ASIO reported that metadata "has been critical in the disruption of terrorist attacks in Australia" in Melbourne in 2005 and Sydney in 2006 resulting in 18 men planning mass casualty attacks being convicted of terrorism offences. Similarly, it was vital in relation to the Holsworthy army base planned assault in Sydney in 2009. ASIO said that "the consequences of not having communications data available to support ASIO and police would have been disastrous". Lack of access as, AFP Deputy Commissioner National Security Michael Phelan said, would take policing back to the "Dark Ages".

The Australian Crime Commission tabled 10 case studies demonstrating the vital importance of metadata access. NSW Police Commissioner Andrew Scipione said "There's not a terrorism investigation since 9/11 that hasn't relied on metadata".

"The Secretary of the Victorian Police Association, Ron Iddles said the number of requests (for metadata access) currently being made by Victoria Police officers was reasonable, equating to about one per detective per week. Without that information, some of the serious crime wouldn't be solved and in particular the case of Jill Meagher would not have been solved without this data. We were able to track a particular phone which was contrary to the account which was given by the accused. We were able to track Jill Meagher's phone through this data to where her location was, to where she was buried, and show that only one phone came back. If the public don't want us to have (metadata access) then the crime solvability rate will definitely go down" (ABC News report, 14 January 2015).

Without guaranteed access to metadata, Australia's police services will be crippled. Their capacity to do the vital work in enforcing the laws of the nation passed by our Parliaments will be severely hampered.

Our police services have had access to metadata under telecommunications legislation since **1991** and no systematic abuse of that access has been evident in **23 years** despite comprehensive public reporting requirements on an annual basis. Open slather surveillance of citizens for improper purposes, or for no purpose at all, by police or security and

intelligence agencies has simply not occurred. There is no sound reason to think that this will change.

As the 2012-13 Annual Report under the Act says, access to metadata is "significant in assisting agencies to safeguard national security, enforce criminal and other laws and to protect the public revenue. Data authorisations are also vital for agencies to obtain the information necessary to apply for telecommunications interception or stored communication warrants."

The Data Retention Bill will ensure that that access can continue and obliges telecommunications companies to retain the metadata for a minimum of two years. As we said above, the PFA believes this should be five years.

In relation to prospective data, authority to access that data is limited to investigations for an offence punishable by imprisonment for at least three years. Therefore there can be no suggestion that such data is accessed for minor offences like "unpaid rego" as one commentator claimed. Authorisation applies for 45 days or less.

The safeguards and checks and balances which govern metadata access were well explained in the Parliamentary Committee hearings on 17 December 2014 (see transcript) so we will not repeat them here except to say that improper access to metadata by police and security services is a criminal offence. That should be reassurance to the Australian public that misuse is most unlikely.

PROPOSALS TO EXTEND THE WARRANT SYSTEM TO METADATA ACCESS

The PFA is most alarmed about the suggestion by some, including the Law Council of Australia, that the system of warrants for access to **content** should be extended to metadata. This sounds like a bonanza for lawyers of course. More importantly, it would cripple law enforcement and public safety in this country at the very time when we need our police forces and security and intelligence agencies operating at their very best – effectively, efficiently, with maximum agility, flexibility and speed.

The Police Federation of Australia believes that requiring warrants for access to metadata would seriously jeopardise public safety and law enforcement in this country.

In many cases metadata access is time-critical, for example during an abduction. The process of obtaining a warrant could actually put the life of a victim at risk. In offences such as homicide, missing persons where there is a suspicious death, abduction and kidnapping police need the data immediately. From the data police are able to identify who the person last spoke to, where they were, and especially if the phone is still on, up-to-date information.

In a recent Victorian case, a woman went missing. Police obtained data from her phone and then tracked her phone. On arrival at a house, police looked over the back fence and observed the offender digging a grave while the woman was tied up. An hour later and she would have been dead.

Introducing a warrant system would mire police services in bureaucracy, paperwork, delay, and huge extra costs which none are equipped to bear. The ACC estimates the average cost of an interception warrant (for telecommunications content) is $34,055. The AFP Deputy Commissioner estimated that requiring warrants would consume 20% of the AFP's investigatory capacity and cost around $25 million a year. ASIO Director General said "the whole system would come to a halt".

The system of warrants for access to telecommunications **content** is already under immense strain. For example the PFA is informed by NSW Police that currently only two telephone interception warrant applications will be dealt with by the courts on any one day because of the shortfall in judicial officers available to deal with warrant applications.

The alternative suggestion of a system of **generic warrants** is nonsense and would achieve nothing in terms of added privacy protection, increased transparency or additional accountability. It looks like an attempt by critics to find some amendment they can pursue so they can be seen to be doing something to change the Bill, but it is a desperately hollow proposal.

The Police Federation of Australia urges all Members of Parliament and the Senate to resist the proposal for warrants for metadata because it would make policing in this country unworkable. Remember that access to metadata is commonly the first and urgent step in finding criminals. Imposing a warrant system would certainly aid any budding terrorist.

CONCLUSION

We agree with the view of Attorney-General Senator George Brandis that passage of this Bill is an urgent priority because increasingly telecommunications providers are not retaining metadata so vitally important to policing and national security.

The PFA would be pleased to appear before the Joint Committee if that would assist in considering these important issues.

M A Burgess

Mark Burgess
Chief Executive Officer