SUBMISSIONS OF THE POLICE INTEGRITY COMMISSION

TELECCOMMUNICATIONS AMENDMENT (GET A WARRANT) BILL 2013

THE BILL

The Bill proposes to vary the present framework of the *Telecommunications (Interception and Access) Act 1979* ("the TIA Act") in respect of access to "telecommunications information" by law enforcement agencies. "Telecommunications information" refers to information held by carriers, carriage service providers, number-database operators, emergency call persons and their respective associates that is prohibited from disclosure by sections 276, 277 and 278 of the *Telecommunications Act 1997* but able to be released under Divisions 3, 4 and 4A of the TIA Act. It comprises information relating to:[1]

- carriage services supplied, or intended to be supplied, to another person by a carrier or carriage service provider; or
- the affairs or personal particulars (including any unlisted telephone number or any address) of another person

but expressly excludes:[2]

- information that is the contents or substance of a communication; or
- a document to the extent that the document contains the contents or substance of a communication.

In short, it is best described as information about communications and not the communication itself. In the main, the telecommunications information actually obtained by the Commission under Division 4 of the TIA Act comprises information such as the names and addresses of the subscribers to specified telecommunications services, the use of specified telecommunications services such as calls made, their duration, the services involved in the call and, where a mobile telecommunications device is used, the location of that device.

[1] Sections 276(1)(a)(iii) and (iv), 277(1)(a)(i) and (ii), and 278(1)(a)(iii) *Telecommunications Act 1997.*
[2] Section 172 *Telecommunications (Interception and Access) Act 1979.*

ACCESS TO TELECOMMUNICATIONS INFORMATION

The Commission relies upon either section 178 or 180 of Division 4 of the TIA Act to authorise access to telecommunications information for its investigations.

Section 178 permits the disclosure of specified telecommunications information in accordance with an authorisation issued by an authorised officer of the Commission. It is limited to historical telecommunications information, being information in existence before notification of an authorisation. An authorised officer must not issue an authorisation under this section unless satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

Section 180 permits the disclosure of prospective telecommunications information in accordance with an authorisation issued by an authorised officer of the Commission. Prospective telecommunications information is specified information that comes into existence during the period of authorisation. It may also authorise the disclosure of telecommunications data in existence before the date of the authorisation.

An authorised officer must not issue an authority under section 180 unless satisfied that the disclosure is reasonably necessary for the investigation of:

- a serious offence;[3] or
- an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least three years (thus excluding all summary offences).

An authorised officer for the purposes of sections 178 and 180 must hold a management office or position within the Commission,[4] and is designated as such only if the Commissioner for the Police Integrity Commission considers that that office or position is appropriate to assessing and issuing such authorisations. Such positions within the Commission are generally held by officers with extensive policing and investigations backgrounds.

In granting an authorisation, authorised officers must turn their minds specifically to privacy considerations. Section 180F requires authorised officers to have regard to:

> ... whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters:
>
> (a) the likely relevance and usefulness of the information or documents;
> (b) the reason why the disclosure or use concerned is proposed to be authorised.

[3] Defined in section 5D of the TIA Act.
[4] Section 5AB(1) TIA Act.

RATIONALE FOR THE BILL

In his Second Reading speech to the Bill,[5] the Honourable Senator Ludlam stated that the purpose of the Bill was to:

> ... reinstate the balance between national security and privacy and treats Australians as citizens first with basic rights and protections, and not merely suspects.
>
> This Bill seeks to ensure that Australians are protected from indiscriminate monitoring by law enforcement agencies.

It would do so by:

> ... [strengthening] the rules about collecting data about Australians. It returns us to the normal warrant procedures where a law enforcement agency is required to obtain a warrant before accessing a person's private data.

It proceeds on the basis that amendments to the *Telecommunications Act* and the *Telecommunications (Interception and Access Act)* in 2007 had the effect of:

> ... normalis[ing] warrantless surveillance, radically and unnecessarily privileged national security concerns over the privacy and civil liberties of Australians.

As a result, there were concerns that those amendments gave rise to the potential for unjustified and arbitrary intrusions into the privacy of telecommunications information:

> ... Australian law enforcement agencies (other than ASIO) are able to access vast amounts of private data without getting a warrant ... Australian citizens have a legitimate expectation that the government will defend their democratic right to privacy, freedom of expression and freedom from arbitrary acts of state surveillance or coercion.

Nonetheless it was said that the Bill was not intended to prevent law enforcement and intelligence agencies from accessing telecommunications information. Rather, the proposed amendments would *"simply require that law enforcement agencies obtain a warrant prior to accessing the information."*

SUBMISSION

The Second Reading speech set out two principal areas of concern:

- the extent to which telecommunications information disclosed private information about a particular person, and whether that ought to be permitted without the rigour of external oversight by way of warrant.

- the extent to which agencies presently access telecommunications information, which is thought might well be indicative of indiscriminate and unjustified access to large volumes of private information for no good purpose (by which it is presumed to mean for purposes that the Act does not permit).

---

[5] 2nd Reading Speech to the *Telecommunications Amendment (Get A Warrant) Bill 2013*, The Hon Senator Robert Ludlam, Parliamentary Debates (Official Hansard), Commonwealth of Australia: Senate, 18 June 2013, p 3225.

The contents/substance warrant framework

It is submitted that the proposal to simply impose the warrant requirements of the stored communications regime to the regime for access to telecommunications information is a blunt and unsatisfactory means of dealing with the balance between the public interest in criminal investigation and individual privacy interest. In particular, it does not adequately consider the lesser privacy intrusion occasioned by access to telecommunications information nor the fact that such information is almost always sought at the start of an investigation when the agency may not have sufficient corroborative information to ground the necessary suspicion for a warrant.

The TIA Act draws a bright line between information relating to the contents and substance of telecommunications and telecommunications information. Warrants are required in order to access the former. That is of course unsurprising. Quite clearly, there can hardly be anything more intrusive than law enforcement agencies accessing the contents or substance of what is assumed to be a private communication. By comparison, the intrusion occasioned by the disclosure of information able to be obtained under sections 178 and 180 is of a far lesser order. It is suggested that that difference is the very reason why the legislature considered that access to telecommunications information might be authorised by a suitably senior position within an agency.

To the extent that there appears to be specific concerns about the potential use of telecommunications information for surveillance purposes, such as in tracking the location of a mobile telecommunications device, the imposition of a warrant requirement would be inconsistent with surveillance requirements generally at the Commonwealth level. The Commonwealth *Surveillance Devices Act 2004* provides that law enforcement officers may be authorised by an appropriate authorising officer of their agency to use a tracking device: section 39 *Surveillance Devices Act 2004.*

Disclosure/use framework

In assessing whether or not the present framework adequately balances privacy interests in how it permits access to telecommunications information, it would an error to focus only upon the operation of sections 178 and 180. That is because those provisions take their place in a larger framework that also protects privacy by regulating the use and further of such information in the form of Division 6 of the TIA. The provisions of Division limit the purposes for which such information may be used and further disclosed.

In the Commission's submission, when those provisions are taken into proper account, it can be seen that the present framework provides a multilayered approach that protects the privacy of such information and is designed to prevent the misuse of such information.

Requirements for granting authorities

The concern that telecommunications information is being accessed indiscriminately and arbitrarily does not appear to take proper account of the requirements of section 178 and 180. Under those provisions, it is simply unlawful for an authorised officer to purport to authorise access to telecommunications information absent the necessary state of

satisfaction or due regard to the matters that she or he is directed by law to consider. In light of the matters that an authorising officer must be satisfied of before issuing an authority, it is plain that the TIA Act does not permit indiscriminate or arbitrary access.

It will also be noted that authorisations pursuant to sections 178 and 180 are for the disclosure of "specified information or documents". This means that authorities must identify what is required with some precision. In practice, all authorities issued will specify a person or telecommunications service of interest or both in order to properly specify what is required by an authority. As such, it would never be the case that authorisations are issued requiring information that does not relate in some real way to a person or telecommunications service of interest in an investigation.

To the extent that there are concerns that authorisations are potentially being granted in breach of the law, there seems little evidence to show that has or may be occurring. The Commission is not aware of any evidence that the present system is or has been so abused as to justify so significant a change as proposed in the Bill. For its part at least, the Commission would reject any suggestion that its exercise of those powers is or has been anything other than lawful, reasonable and with good cause.

There are also practical considerations that should allay concerns about indiscriminate or arbitrary access to telecommunications information. It requires significant resources to properly assess and make use of telecommunications data. Like all other law enforcement agencies, the Commission has limited investigative resources at its disposal. It is hardly the case that the Commission would –or could- devote its limited resources to obtaining telecommunications information absent a soundly based belief that that information can reasonably advance its investigation in some way. Quite simply, it would be a waste of its times and resources for it to do otherwise.

IMPACT UPON INVESTIGATION

The Commission is concerned that the proposed amendments sought by the Bill will unnecessarily impact in a very real way on the capacity of the Commission to effectively conduct its investigations. Telecommunications information is vital to the conduct of its investigations particularly at the outset of a criminal investigation. The information that can be gleaned from telecommunications information about persons of interest, their associates, and activity patterns is of great assistance in assessing whether allegations have any substance as well as developing and refining investigative lines of inquiry. Such information can and has enabled the Commission to rule out allegations against a particular person at an early stage.

More importantly, telecommunications information is critical in advancing an investigation to the point where the accessing of stored communications or the interception of relevant telecommunications services is a viable option. This is because such information assists in properly identifying the relevant telecommunications services. Commission investigations would be far less effective if its ability to do so were impeded.

Unfortunately, the Commission is of the view that the Bill has the potential to do precisely that.

Without being able to first obtain telecommunications data to the extent that it presently does, it would become far more difficult for Commission investigators to identity the relevant telecommunications services being used by a person of interest or who the person is in contact with regarding the commission of relevant offences. This is not least because the subject of an investigation may well use multiple telecommunications services, often subscribed to under a false identity, or simply use the telephone of an associate.

Absent certain knowledge of the services used, investigators would be unable to proceed to the step of seeking warrants for access to stored communications or the interception of those services. In effect, Commission investigators would never get past first base, such is the importance of access to telecommunications information as the precursor to seeking more textual information from specified telecommunications.

While it is claimed that the Bill will not prevent the present level of access to telecommunications information by law enforcement, it will nonetheless have a very real impact on the extent of access to telecommunications simply because of the additional procedural steps that would be required. At the least, it would require the diversion of significant resources to prepare and make formal applications for warrants to obtain the telecommunications information required. Moreover this would only be possible where the Commission had sufficient other information to ground a warrant. It is anticipated that it would necessarily mean curtailing its investigations or foregoing what might otherwise have been productive lines of inquiry.

CONCLUDING REMARKS

In the Commission's submission, the present framework strikes the proper balance between the public interest in the efficient investigation of criminal activity on the one hand and the protection of individual privacy interests on the other.

At the least, it is submitted that the amendments proposed by the Bill ought be considered as part of the broader inquiry into Australia's national security legislation. As the Committee will be aware, the Parliamentary Joint Committee on Intelligence and Security recently published its *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. As that inquiry examined, among other things, access to telecommunications information, it would seem inappropriate for the Bill to proceed independently of the process commenced by the Joint Committee touching on the very same area.