Re: Telecommunication (Interception and Access) Act 1979 Review

Author: Paul Wilkins

Date: 18 June 2019

Table of Contents

I raised the point in my PJCIS submissions regarding the Assistance and Access Act, that TANs/TCNs are potentially sufficient grounds to serve as authorisation under s280/s313 and/or s177 of the Telecommunications Act, and/or under the Criminal Code Act 1995, for the access of Data Retention datasets, and so provide the necessary enabling legislation for law enforcement to institute access to metadata datastreams. Thus a consequence of the the passage of the Assistance and Access Act is that there is a now legal avenue under s280/s313 of the Telecommunications Act, and under s177 of the Telecommunications (Interception and Access) Act 1979, and under the Criminal Code Act 1995, for law enforcement to lawfully seek access to en masse surveillance metadata data streams from carriers.

Nowhere are TCN/TAN/TARs disallowed from serving as "authorisation" under s280 / s313 of the Telecommunications Act 1997, sufficient to demand mass access to carrier metadata/ metadata datastreams. There is also lawful disclosure of mass metadata under s177 of the Telecomms Interception and Access Act 1979. If the police and/or intelligence services get access to metadatastreams, they will integrate this with their other metadata projects, including CCTV and facial recognition databases. Which is obviously something some in Law Enforcement are advocating for, though I think most citizens would regard this as an alarming move towards mass surveillance and a police state.

TCNs/TANs/TARs can now be used to collect, collate, and analyse carrier metadata, for which no warrant is required. Which is a consequence of the effect of the vague and flawed drafting of the Assistance and Access Act 2018 amendment which acts concurrently with sections of the Telecommunications Act 1997, which may authorise access to carrier metadata: - under s280 and/or

s313 law enforcement has power to compel carrier disclosure, and via the Telecommunications (Interception and Access) Act 1979 s177 by which carriers may voluntarily provide metadata.

Metadata access as a compelled carrier disclosure under Telecommunications Act 1997 - s280/s313

313 Obligations of carriers and carriage service providers

(3) A carrier or carriage service provider must, in connection with:

(a) the operation by the carrier or provider of telecommunications networks or facilities; or

(b) the supply by the carrier or provider of carriage services;

give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:

(c) enforcing the criminal law and laws imposing pecuniary penalties;

(ca) assisting the enforcement of the criminal laws in force in a foreign country;

(d) protecting the public revenue;

(e) safeguarding national security.

Note: Section 314 deals with the terms and conditions on which such help is to be provided.

(5) A carrier or carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith:

(a) in performance of the duty imposed by subsection (1), (1A),(2), (2A), **(3)** or (4); or

(b) in compliance with a direction that the ACMA gives in good faith in performance of its duties under section 312; or

(c) in compliance with a direction given under subsection 315A(1) or 315B(2).

(7) A reference in this section to giving help includes a reference to giving help by way of:

(e) disclosing information or a document in accordance with section 280 of this Act.

Note: Additional obligations concerning interception capability and delivery capability are, or may be, imposed on a carrier or carriage service provider under Chapter 5 of the Telecommunications (Interception and Access) Act 1979.

280 Authorisation by or under law

(1) Division 2 does not prohibit a disclosure or use of information or a document if:

(a) in a case where the disclosure or use is in connection with the operation of an enforcement agency—the disclosure or use is required or authorised under a warrant; or

(b) in any other case—the disclosure or use is required or authorised by or under law.

The net effect of 313 combined with 280 being where carriers can be compelled to disclose metadata to give “reasonable” help to law enforcement agenices on one or more of the following premises: - to enforce the law, safeguard national security, protect public revenue, or assist in enforcing the law of another country.

So, consider the situation where the Attorney General, after considering it to be reasonable, issues a TCN that mandates carrier metadata be provided to law enforcement as a raw data stream. This would cause the carrier to be obligated to provide the metadata as a data stream. Perhaps it appears on the surface the effect of s280(1)(b) prevents this, where law enforcement should require additional authorisation, to meet the standard of "required or authorised by or under law". However the Attorney General's TCN provides the necessary requirement and authorisation that s280(1)(b) demands, even to a standard of "reasonableness", even if that is only to the Attorney General's arbitrary standard of reasonable. The only grounds for carriers to challenge such a TCN would be that the scope of data requested, or establishing a system for mass surveillance, was "unreasonable", yet the fact of the Attorney General's TCN establishes a prima facie case that the request is reasonable, if only to the Attorney General's arbitrary standard.

This is in stark contrast to current practice and expectations, where access to carrier metadata is requested on a per case basis:

> "For example, we learnt that in the last reported year more than 80 federal and state enforcement agencies requested access to historical telecommunications data under the *Telecommunications (Interception and Access) Act 1979* and that requests for such data resulted in an annual total of over 500,500 disclosures by service providers.
>
> This statistic did not include an undisclosed number of accesses by intelligence agencies – reporting as to even the number of requests by intelligence agencies is classified (secret) – or accesses by agencies exercising powers under other federal, state or territory statutes, or accesses pursuant to subpoena and other court process."
>
> https://www.gtlaw.com.au/insights/metaexercised-about-metadata

There should be provision within the exceptions of 280(1B) to include TCNs and TANs, but there isn't. This omission is either deliberate or an oversight, but either way, either deliberately or inadvertently as a result of the passage of the Assistance and Access Act 2018, there exists a direct path for law enforcement to use TCNs/TANs to institute the machinery of a police state without further legislation required, and absent of any additional oversight.

S280(1B) of the Telecommunications Act 1997 must be amended to include TCNs/TANs/TARs, so that they do not constitute requirement/authorisation under s280(1)(b). There should be specific injunctions against the use of TCNs/TANs/TARs to require provision of metadata as data streams, and checks and balances ensuring metadata access is only provided on a case by case basis.

Metadata access as voluntary carrier disclosure under Telecommunications (Interception and Access) Act 1979 - s177

Another means by which mass collection of metadata can be established is via the voluntary disclosure provision of s177 of the Telecommunications (Interception and Access) Act 1979.

Of course, where there are concurrently enabled voluntary and compulsory disclosure, Law Enforcement have a powerful means to coerce voluntary disclosure. Either provide the data voluntarily, or be compelled as a last resort.

> **177 Voluntary disclosure**
>
> ***Enforcement of the criminal law***
>
> (1) Sections 276, 277 and 278 of the Telecommunications Act 1997 do not prevent a disclosure by a person (the holder) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law.
>
> ***Enforcement of a law imposing a pecuniary penalty or protection of the public revenue***
>
> (2) Sections 276 and 277 of the Telecommunications Act 1997 do not prevent a disclosure by a person (the holder) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.
>
> Telecommunications (Interception and Access) Act 1979: Compilation No. 101, Compilation date: 18/9/18

The point is made in “The Metadata Retention Debate rages on - Peter Leonard GILBERT + TOBIN LAWYERS”
https://www.gtlaw.com.au/insights/metadata-retention-debate-rages

that current requests for metadata typically are via 313 than 177, due to liability concerns. However, where carriers are indemnified under the Act’s s317G, s177 provides a viable pathway for carriers to voluntarily provide metadata datastreams to LEAs without liability concerns.

Metadata access authorised under the Criminal Code Act 1995

It is arguable TCNs/TANs/TARs authorise the collection of metadata without judicial intervention of any kind including warrants. For example, s474.6(7) and s476.2(b) of the Criminal Code Act.

> 474.6 Interference with facilities
>
> (7) A person is not criminally responsible for an offence against subsection (5) if:
>
> (a) the person is, at the time of the offence, a law enforcement officer, or an intelligence or security officer, acting in good faith in the course of his or her duties; and
>
> (b) the conduct of the person is reasonable in the circumstances for the purpose of performing that duty.
>
> Criminal Code Act 1995: Compilation No. 123, Compilation date: 22/9/18

476.2 Meaning of unauthorised access, modification or impairment

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

Criminal Code Act 1995: Compilation No. 123, Compilation date: 22/9/18

That seems a pretty solid case that a TAN can be argued to authorise access to metadata under the Criminal Code Act, and certainly such access is not unauthorised, nor does it require judicial warrant. This then provides the necessary authorisation for metadata access either on the merits of the TAN alone, or in conjunction with s313 of the Telecommunications Act. It places the courts in a difficult position to overrule such access as unreasonable, if the Attorney General has previously given his opinion that such access is reasonable. Further, it is within the power of the government of the day to compel access to metadata streams unlawfully, if the fact of the establishment of carrier metadata datastreams is suppressed, leaving the public none the wiser that they're being surveilled en masse.

There ought to be specific legislative protections preventing Law Enforcement Agencies seeking access to metadata streams, or otherwise engaging in the en masse collection of metadata. Specific provision including that requests by Law Enforcement Agencies for access to metadata beyond a case by case basis, including provision of metadata data streams, goes beyond reasonable necessity for all purposes, including enforcement of the criminal law, provisions 280, 313 of the Telecommunications Act 1997, s177 of the Telecommunications (Interception and Access) Act 1979, and the Criminal Code Act 1995.

Authorisation for Metadata TCNs/TANs/TARs

Given that the existence of TCNs/TANs/TARs may serve to establish access to metadata datastreams, enabling mass surveillance, it remains to be show how Law Enforcement can raise the TCNs/TANs/TARs for the purpose of metadata collection and gaining access to carrier metadata streams.

This is provided under the Act's "317E Listed acts or things", covered under the definitions:

317E(1)(e) facilitating or assisting access to whichever of the following are the subject of **eligible activities** of the provider:

(v) a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service;

(vi) an electronic service;

(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

Note that a metadata datastream would meet the definition of a “service” under 317E(1)(e) subsections (v),(vi),(vii). Indeed, it’s beyond question that a metadata datastream meets the definition of ss(vii) as a service ancillary to the provision of an electronic service. Even more so if the carrier has been compelled under TCN to create such a service.

A carriers activities are **“eligible activities”** under 317C

317C Designated communications provider etc.

For the purposes of this Part, the following table defines:

(b) the eligible activities of a designated communications provider.

Item 1: **the person is a carrier or carrier service provider**

The power to issue a TCN to establish metadata datastreams then is created under the Act’s s317T Technical capability notices, where it should be apparent from the preceeding argument that on examination of the necessary condititions that all necessary conditions are met. It is interesting to note where 317T(10) excludes the “keeping” of metadata, but is silent as to the *transmitting* of metadata.

The power to issue TANs to establish metadata datastreams is created under the Act’s s317L, where it should be apparent from the preceeding argument that on examination of the necessary conditions that all necessary conditions are met.

Consequences of Access to Carrier Metadata Datastreams by Law Enforcement

It’s entirely conceivable (if not inevitable) that systems will be created for LEAs to access metadata datastreams, requiring no involvement of service providers, other than to provision access to their metadata stores. Conceivably this access could be provisioned only once, at the initiation of access for each agency, and the service provider have no further involvement. Access to service provider metadata would be ongoing under 313(3)(c) and s280(1)(b). This machinery will run with the

public mostly unawares that they're being surveilled, en masse, especially if service providers are compelled to silence as to the terms of the enabling TCNs/TANs.

Where one considers the very great use of s280 observed in a Communications Alliance submission to PJCIS, it becomes obvious that TCNs/TANs will be used by law enforcement to institute automated processes for mass trawling metadata. This process was initiated with the introduction of the Data Retention Act, and with the reach of the Assistance and Access Act, no further enabling legislation is required.

It is within the technical capability, the legal reach, and reasonably foreseeable, that at some point in the future, LEAs will use these powers to gain access to metadata data streams, and these will be merged with metadata streams from other sources (CCTV including number plate and facial recognition, public transport travel cards), to create IT systems for the automatic collection, collation, and analysis of service provider metadata all without judicial warrant or oversight. Indeed, we're already seeing efforts to track citizens via CCTV via number plate and facial recognition.

Without the necessary legislative checks on police powers, it is inevitable that there will be creeping extension of the scope of law enforcement activities, foreseeably to prosecute the criminal law to include Minority Report style metaanalysis including the following:

- tracking convoys of (possibly illegal) motorcycle enthusiast groups
- tracking weekend night movements of dance enthusiast groups
- tracking associates of journalists who have sourced leaked government documents (whether or no such leaks being in the public's interest in holding State power to account)
- prosecuting politicians use of electoral office staff for political campaigns
- prosecuting public servants committing time fraud
- identifying police frequenting criminal haunts, or with otherwise suspect behaviours/movements
- profiling and then identifying car thieves and house breakers, and other criminal activities
- tracking associates of those who attend public protests

This represents a radical departure from firstly the presumption of innocence, and secondly, from the existing standard that police require reasonable doubt before they have the right to intrude into the rights of citizens. Unfortunately, once you let the geni out of the bottle, and allow for police to track people's movements, and correlate these to social groups and behaviours, there's no telling where it may wind up. Except where history affords ample distopian object lessons. It's certainly a consequence of the legislation that would amaze the great majority of Australian citizens. Though there are signs the public is beginning to take an interest. We have seen in the public debate repeated assurance by law enforcement and the Dep't of Home Affairs that there is no need for legislative checks on current State police powers, only for the media to expose overreach of these powers. It's disturbing that certain of these instances of overreach by the State, have targeted journalists and the media who have sought to hold the police machinery to account.

Mass collection of metadata creates a powerful machine for the government of the day to engage in social engineering. In a Liberal Democracy, you are free to live as you please within the law. But if we allow governments and law enforcement to collect and collate metadata, we're moving towards Minority Report scenarios, where if you depart from your usual routine, there's an exception report generated, and overall pictures of aberrant behaviours and databases of non conformists built up. And where the police go from there is not necessarily a question of law, but can be influenced by

whoever is the government of the day, and to what populist causes they may need to pander to to remain in office.

Furthermore, if metadata is collected from service providers, and subjected to metaanalysis, under the legislative police powers, there are no restraints against law enforcement subsequently sharing this metaanlysis with other agencies.

It's certainly clear the Privacy Act 1988 never anticipated law enforcement would have access to such a mine of personal information, and is inadequate to protect citizens rights in the face of such powerful police machinery.

Consequences of Aggregation of Carrier Metadata with other Metadata Datastreams (CCTV + number plate/facial identification, Social Media etc.)

Because there are no limits under the legislation on metadata, the powers of Law Enforcement will be able to pursue collection of metadata whereever it can be found, and then combine the data streams to create correlations and metaanalysis of the movements, behaviours, and associations of citizens. Sources for metadata collection will include:

- Mobile Phones, with approximate location from towers
- CCTV (from RTA, councils) including facial recognition identifiers, and number plate matching
- Social Media - including cross referencing calendared protest events
- Public transport travel cards

It only remains for a future Home Affairs Minister to extend the reach of metadata (via TCN) to debit and credit cards, CCTV from ATMS, and CCTV number plate matching from petrol stations.

Mass collection and analysis of metadata from multiple sources lays the foundations for the establishment of the machinery of a police state. Of course, this will make prosecution of crime straightforward (the police will only need to correlate crime against a database of the public's electronic fingerprints). However, such powerful machinery can be used for oppressive purposes, and the Act is absent of the checks and balances consistent with the traditions and institutions of Liberal Democracy.