# Table of Contents



Supplementary Submission
Author: Paul Wilkins
Date: 24 November 2018

> "Because this encryption bill really is crucial to giving police and ASIO and other intelligence agencies the tool they need to disrupt and deter these activities."
>
> Home Affairs Minister, Peter Dutton

Dutton's argument is premised on a false equivalence.

It's perfectly possible to protect against terrorism and serious crime without throwing out the baby with the bathwater, kicking doors in on data centres and imposing warrantless mass surveillance.

# Introduction

Home Affairs put up this Bill on the premise it's needed to fight terrorism and serious crime in the context of increasing use of encryption. Unfortunately, this isn't that bill. It should be returned to Dep't Home Affairs for a complete rewrite, with the direction that the new Bill meet the stated goals of protecting the nation from terrorism and serious crime in the context of increasing use of encryption, subject to provisions for necessary and proportionate interference with the rights to privacy and rights to private property, consistent with democratic traditions and institutions of Liberal Democracy and the rule of law, to include necessary checks/balances and accountability for the use of highly intrusive police powers, and to ensure judicial appeal for all interested parties is an included part of the process.

This additional to previous submissions examines the following matters:

1 - The Bill establishes the machinery of mass surveillance. Existing legislation is quoted extensively to demonstrate that under this Bill, metadata can be lawfully collected from multiple sources, without the requirement for warrants or any other authorisation from the courts.

2 - Examination of the consequences of the collation of metadata from multiple sources (mobile telephone towers, CCTV, social media…). The ability of Law Enforcement to collate and cross reference metadata institutes the machinery of a police state.

Where the function of Law Enforcement is reduced to an algorithm, and law breaking is detected by matching behaviours/movements/associations to a database of the public's electronic signatures, you have the machinery of a police state. Without accountability and checks and balances on its use, this machinery could be used by Law Enforcement or by the government of the day to persecute and oppress minorities as easily as it can be used to prosecute the law.

3 - Advantages of centralisation in a single agency. My previous submission makes the case for economy and data security. This submission explores advantages of governance and accountability of a single agency approach.

4 - A body no less august than the Internet Architecture Board in their PJCIS submission makes the compelling argument the bald fact of the Bill creates systemic weakness in the Internet. The PCI framework is a security framework widely relied upon to audit and ensure the integrity and security of ecommerce IT systems. This submission examines the case of PCI accreditation as an example, of where the existence of powers under the Bill, to alter codebase, to change security architectures, to suppress pertinence governance details, will undermine the strength and confidence in the security of the PCI framework.

5 - A series of pertinent questions that go to the unpreparedness and inadequacies of this Bill.

6 - Analysis of these same questions through the prism of one agency to demonstrate the merits of the one agency approach including data security, economy, governance, accountability, and the checks and balances and accountability for the exercise of police powers consistent with Liberal Democracy.

# The Bill Establishes the Machinery of Mass Surveillance

Both the Department of Home Affairs and its Minister have suggested, incorrectly, that powers under the Bill are limited by the necessity for a warrant for data access. This is either deeply disingenuous or overlooks where TCNs/TANs/TARs can be used to collect, collate, and analyse carrier metadata, for which no warrant is required. This is a consequence of the effect of the vague and flawed drafting of the Bill concurrent with existing legislation, including provision in the Telecommunications Act 1997 under s313 to compel carrier disclosure, provision in the Telecommunications (Interception and Access) Act 1979, s177 by which carriers may voluntarily provide metadata, and elsewhere where the fact of TCNs/TANs/TARs will meet requirements for authorisation of metadata access under existing legislation, including the Criminal Code Act 1995.

## Metadata access as a compelled carrier disclosure under Telecommunications Act 1997.

**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 of carriers consequent to the carriage of this Bill, 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 the present situation, 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

It it were the intent of this Bill, that TCNs/TANs not consitute a s280(1)(b) requirement/authorisation, there would be provision to amend the exceptions of 280(1B) to include TCNs and TANs. This omission is either deliberate or an oversight, but either way, leaves one deeply suspicious of this Bill, where either deliberately or inadvertently it can be made to serve as a trojan horse for the mass collection of carrier metadata.

**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.

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.
>
> 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 Bill's s317G, s177 provides a viable pathway for carriers to voluntarily provide metadata datastreams to LEAs without liability concerns.

Consequently, this Bill gives law enforcement a two phase approach for the establishment of carrier metadata data streams, request voluntary compliance under TCN under s177 of the Telecommunications (Interception and Access) Act 1979, with s313 of the Telecommunications Act 1997 as a last resort.

## Metadata access authorised under the Criminal Code Act 1995

Because either by oversite or deliberate attempt by drafters of the Bill to obfuscate the true extent of embodied police powers to collect metadata en masse, the Bill contains other obfuscated means by which 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

The Criminal Code as amended under new sections 474.6(7)(7A) and 476.2(4)(b)(iii) of this Bill would authorise action that:

> (a) is in accordance with a technical assistance request; or
> (b) is in compliance with a technical assistance notice; or
> (c) is in compliance with a technical capability notice.

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. The Bill nowhere is explicit that such access is unreasonable. 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. Which is to

say, should this Bill pass, the public will henceforth be in the dark as to whether or not the state is mass surveilling its citizens.

**There ought to be specific protections in the Bill against Law Enforcement Agencies seeking access to metadata streams, or otherwise engaging in the en masse collection of metadata. The Bill should make specific provision 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 of 313 of the Telecommunications Act 1997, and s177 of the Telecommunications (Interception and Access) Act 1979.**

**The Bill needs to make provision for checks and balances, accountability, and transparency for disclosures of metadata to Law Enforcement made under TCNs/TANs/TARs.**

## 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 Bill'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 Bill'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 Bill'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 the 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 Bill, no further enabling legislation is required.

It's highly improper where the Home Affairs Minister has represented to the House that this is not a Bill for mass surveillance. The Bill in fact establishes these very powers. It's of deep concern that either the Minister brings to the House a Bill of which he is unaware of the import of its provisions, or more alarming is the possibility he has chosen to misrepresent the import of the Bill he has commended to the House.

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.

Consequently, should this Bill pass, police will be able to widen their attempts 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
- prosecuting politicians using electoral office staff for political campaigns, where they're canvassing/letter dropping when they're supposed to be at work
- prosecuting public servants committing time fraud
- identifying police frequenting criminal haunts, or with otherwise suspect behaviours/movements
- identifying car thieves and house breakers
- 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 if the Government were to consider this move to a police state reasonable or proportionate.

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 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 this legislation 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 Bill is absent the checks and balances consistent with the traditions and institutions of Liberal Democracy.

If one were cynical you might think the Bill's outrageous overreach is deliberate, a Trumpist ploy to enrage the unthinking. And when we see critics of the Bill slandered for being weak on terrorism, maybe not so wide of the mark or so cynical.

**There need to be protections for confidentiality, and limits of necessity and proportionality, on the sharing of any metaanalysis of metadata, including with other government agencies, government service providers, or in fact transfers of the metaanalysis within the agency who conducted the metaananalysis.**

Where governments are increasingly reluctant to be held accountable and impose secrecy on government documents, journalists are increasingly being criminalised for protecting free speech and for holding the government of the day to account, where they cannot do their job without access to documents deliberately classified as secret for no other reason than the government wishes they remain outside the view of the public.

The powers within this Bill will, as drafted, will provide a powerful tool for pursuing journalists who receive leaked documents and those who provide the leaked documents, and while government will benefit from the reduced incidence of leaking, the net effect will be increasing opacity of the workings of government and consequent obstruction for government employees, journalists, media organisations, and the public, to hold the government of the day to account.

**The Bill ought to be specific as to the standard of serious crime. The bar ought to be significantly higher than as currently drafted. Media organisations ought to have standing and opportunity to mount a public interest defense against the issue of TCNs and TANs.**

## The Bill creates systemic weakness in the Internet - Case Study - PCI Framework

It is of course outrageours, that the Bill should seek to empower Law Enforcement to intrude without limitation into the private domain of service providers, without limitations that ensure changes are consistent with established business and security practices. Under the Bill, there are no limitations under the Bill on uncontrolled changes by Law Enforcement across established business practices, architectures, and security controls, including powers to compel:

- alterations to codebase, including inclusion of non standard, non audited, untested, or unsupported code
- modification of security architectures, including departures from existing security controls

- creation of alternate data flows, including flows beyond the enterprise security perimeter
- suppression of pertinent governance details

Now this is all very interesting in the context of 317ZG, where all the above create systemic weakness. But there is a real problem, where all intrusions into service operations by a third party, can be argued to represent a systemic weakness, especially where:
agents of the third party are both unfamiliar and unconstrained by established governance, process, and security controls, do not have intimate understanding of the service provider environment, architectures, coding standards, security policies, and where the intervention is not required to conform to release procedures, quality and testing controls, and where after the fact, there is no one responsible for the artefacts introduced into the service provider environment. CIOs and corporate boards are to be held accountable for maintenance of service standards, including those subject to TCNs/TANs/TARs, but without the ability to enforce or attribute responsibility by Law Enforcement.

The Internet Architecture Board in their PJCIS submission make the same point. They go further, to point out that such interventions weaken confidence across the entire internet.

Question: Is it possible to pass a PCI audit, while potentially bound to silence regarding:

- source integrity
- secret functionality
- undisclosed 3rd party end points

If consequent to TCN/TAN, the control plane function extends beyond the security perimeter to third parties, that right there makes the architecture non PCI compliant.

It places PCI auditors in the curious position, where reports will need to qualify their reports that PCI compliance of mandated TCNs/TANs are beyond the audit scope, potentially invalidating the compliance of the entire environment. This specific example highlights the need for clarity regarding the vague protection of 317ZG and the meaning of "Systemic Weakness".

The situation is further complicated, where Law Enforcement have the power to compel silence as to the existence of TCNs/TANs. This presents PCI auditors with an impossible situation, where either they cannot vet the TCN/TAN mechanisms, or if they can, they cannot report their findings. Consequently *all* PCI reports issued within Australia should come with a rider that no TCN or TAN subject to non disclosure can be reported. Consequently all PCI accreditation issued within Australia becomes suspect.

Given the IAB's position that all currently known Exceptional Access methods create security weaknesses, presumably that can be relied on as authority for the argument that 317ZG offers immunity against all TCN/TAN requests.

## A series of open questions to consider in assessing Bill

1 - Why is there no judicial oversite of these sweeping police powers?

2 - Scope of powers go beyond terrorism and serious crime when it's not supposed to.

3 - It supports the establishment of the machinery of mass surveillance when it's not supposed to.

4 - It weakens the Internet's security, when it's not supposed to.

5 - Why are there no limits to ensure issue of TCNs/TANs/TARs are necessary and proportionate to the human right to privacy, unrevokeable per the Declaration of Human Rights.

6 - Why the deliberate exclusion/incompatibility of the provisions of the Privacy Act 1988?

7 - Why are there no limits to ensure issue of TCNs/TANs/TARs are necessary and proportionate to service providers rights to private property, unrevokeable per the Declaration of Human Rights?

8 - When Police Powers lie with the States, what constitutional head of power supports the Bill's scope, without enabling legislation from the States conferring power? The Constitution confers national security powers, but the scope of the Bill's police powers exceeds this remit.

9 - Why has the Bill overlooked the obvious alternative of powers spread across a dozen Law Enforcement Agencies, which is to centralise in one single agency, providing for greater data security, governance, efficiency, and accountability?

10 - Why the lack of provisions for accountability for the exercise of police powers, and checks and balances commensurate to the reach of sweeping police powers, quite incompatible with the democratic institutions and traditions of Liberal Democracy?

11 - Why the deliberately curtailed public consultation process and attempt to ambush both the public and government with this Bill by Dep't Home Affairs, and representations of public and industry consultations as being timely and adequate, incompatible with the facts on the public record and the express concerns of the public, human rights groups, and industry?

12 - Why the absence of recompense for injury to reputation or to service providers' business, or other injury consequent to police malfeasance or misfeasance? The Bill's protections are not comprehensive, and where they make provision, go only as far as to establish lack of liability for unlawful disclosures.

13 - Why has the government of the day referred this deeply flawed Bill to the PJCIS, PJCHR, and the SSCSB, for review wasting public time and money, rather than sending it back to Dep't Home Affairs for a complete overhaul of it's scope and objectives?

## Analysis of these same questions through the prism of a single agency

1 - Why is there no judicial oversite of these sweeping police powers?

Arguments by the Dep’t Home Affairs notwithstanding, there is no real impediment to ensuring TCNs/TANs/TARs require judicial authorisation before they have the force of law. A judicial forum would afford stake holders a forum (before the fact) to challenge the intent or specifics of a notice.

Where the Dep’t Home Affairs has a point, is that having a dozen agencies all needing access to the judiciary to gain approval, creates difficulties, but this difficulty is largely due to the way the Bill itself is framed. If a single agency were responsible for issuing TCNs/TANs/TARs, then they would have a well established internal processes for developing TCNs/TANs/TARs. There would be solid governance for engagement with service providers. They could liaise with media organisations as necessary where access to journalist metadata is sought. Consequently, a great deal of the judicial

burden in assessing TCNs/TANs/TARs would be absorbed in the agencies internal processes, and resulting in TCNs/TANs/TARs of a uniformly high standard which would keep judicial involvement in the process to a minimum.

2 - Scope of powers go beyond terrorism and serious crime when it's not supposed to.

Apart from the obvious advantages of improved governance and established framework of a single agency, there is the additional advantage that the volume of notices processed will create an established process. Rather than a dozen different agencies all with differing ideas of what's considered necessary and proportionate, having one agency means the corner cases will have been resolved and hopefully corporate memory retained in operational standards to preserve the lessons learnt.

3 - It supports the establishment of the machinery of mass surveillance when it's not supposed to.

Again, the establishment of an agency with a mission to serve the warrant/notice network will result in improved governance and public accountability.

4 - It weakens the Internet's security, when it's not supposed to.

Certainly, where in this submission, and the IAB have pointed out, where the very fact of the existence of police powers to compel actions under TCN and TAN results in systemic weakness, the proposed framework goes further, where the systemic weaknesses created are then to be multiplied across a dozen different law enforcement agencies.

5 - Why are there no limits to ensure issue of TCNs/TANs/TARs are necessary and proportionate to the human right to privacy, unrevokeable per the Declaration of Human Rights.

See #1 and #2.

6 - Why the deliberate exclusion/incompatibility of the provisions of the Privacy Act 1988?

See #1 and #2.

7 - Why are there no limits to ensure issue of TCNs/TANs/TARs are necessary and proportionate to service providers rights to private property, unrevokeable per the Declaration of Human Rights?

It's quite improper that the Bill should empower law enforcement as the decision makers on choices of the use of force, including kicking in data centres, surveilling the populace, and inserting random code into the private property code base of service providers. The framework as proposed guarantees intrusion by law enforcement will be neither necessary nor proportionate. Further, that over a dozen different agencies may choose to impose their own conditions is of itself unnecessary and disproportionate.

8 - When Police Powers lie with the States, what constitutional head of power supports the Bill's scope, without enabling legislation from the States conferring power? The Constitution confers national security powers, but the scope of the Bill's police powers exceeds this remit.

If the Government takes the necessary step, and returns the Bill to Dep't Home Affairs for a complete rewrite, and as part of that process establishes a new agency to act as warrant/notice clearing house, it can take the opportunity to seek the necessary enabling legislation from the states for the establishment of the new agency.

9 - Why has the Bill overlooked the obvious alternative of powers spread across a dozen Law Enforcement Agencies, which is to centralise in one single agency, providing for greater data security, governance, efficiency, and accountability?

A single agency acting as a clearing house for TCNs, TANs, TARs, would ensure proper governance for the exercise of highly intrusive police powers. More importantly, a separate agency acting as clearing house for warrants and notices, would ensure separation between evidentiary approvals (up to and including the use of force), and the police task forces seeking these powers. Indeed the lack of this separation in the current Bill is a glaring governance gap, and if enacted as is, will ensure a great many unhappy if not unlawful outcomes.

10 - Why the lack of provisions for accountability for the exercise of police powers, and checks and balances commensurate to the reach of sweeping police powers, quite incompatible with the democratic institutions and traditions of Liberal Democracy?

11 - Why the deliberately curtailed public consultation process and attempt to ambush both the public and government with this Bill by Dep't Home Affairs, and representations of public and industry consultations as being timely and adequate, incompatible with the facts on the public record and the express concerns of the public, human rights groups, and industry?

That the Bill could have progressed to this stage, and have soaked up the time and energy of not only the government (including PJCIS, PJCHR, and the SSCSB), but also the public and industry in attempts to putting this bad Bill to rights certainly deserves censure. It’s quite deplorable the Bill should have reached this stage with such an oversite in the framework as to have overlooked the possibility of centralising powers in a single agency clearing house.

12 - Why the absence of recompense for injury to reputation or to service providers' business, or other injury consequent to police malfeasance or misfeasance? The Bill's protections are not comprehensive, and where they make provision, go only as far as to establish lack of liability for unlawful disclosures.

Again, a single agency acting as a clearing house for TCNs, TANs, TARs, would ensure proper governance and accountability. It would also provide for accountability and responsibility for the use of these powers, and consequently should carry the onus of responsibility and liability of the Crown for malfeasance/misfeasance.

13 - Why has the government of the day referred this deeply flawed Bill to the PJCIS, PJCHR, and the SSCSB, for review wasting public time and money, rather than sending it back to Dep't Home Affairs for a complete overhaul of it's scope and objectives?

It’s a moot question how Dep’t Home Affairs could have got this far down the road, and poured in such public resources as necessary to get to this stage, when the fundamental framework is so obviously flawed. Unfortunately this fundamental flaw fails to get the warranted attention, because of the Bill’s many other inadequacies and the limited window afforded for public and industry consideration and discussion of the Bill.