Table of Contents

Re: The Assistance and Access Bill 2018

Author: Paul Wilkins

Date: 9 October 2018

Introduction

It’s been said before that there are two things the public should never see, the making of legislation, and the making of sausages. With regards The Assistance and Access Bill 2018, it is perhaps more curate’s egg than sausage, or perhaps a curate’s sausage. It bears all the hall marks of an ambit claim by law enforcement agencies, with little consideration given to either the rights of the public to protection of their privacy and their right to control dissemination of their private information. But less regard still given to the needs of service providers on whom the costs and legal onus of compliance with directions that will be issued by law enforcement. Conspicuous in its absence is adequate protection for service operators against arbitrary, high handed, ill prepared and/or ill considered actions by Law Enforcement causing disruption to their business in overriding established business practices for risk management, security, and change control procedures of the IT systems that form their core business.

The Bill in its present form doesn't deserve to pass, because it's not ready, and will lead to unhappy outcomes, particularly for service providers. There are evident deficencies of the Bill across the spectrum of its goals and provisions, which go to the lack of preparedness of the Bill, and the inadequacy of the Bill to either achieve the proposed aims, or to be compatible with the standards of accountability and transparency of exercise of power expected within a liberal democracy. Evident deficiencies include:

1 - The multiplicity of agencies and agents who can authorise TANs and TARs.

1a - Warrant data and service provider data will reside with the issuing agencies.

Hence, the government needs to reconsider the whole approach, and instead, have one agency act as a clearing house for TCN/TAN/TARs, and act as custodian of warrant data and service provider confidential data.

2 - The lack of civil appeal process against TCN/TAN/TARs.

Grounds for appeal to either refuse or delay assistance should include:

Cost, security management, risk management, business management processes, disruption to business, disparity of TCN/TAN/TAR with Privacy Act 1988 and other legislation or common law duties, or the public interest.

2a - Suppression of the existence of TCN/TAN/TARs should be subject to the same appeals process on the same grounds (preferable would be to have the power to suppress lie with the judiciary, predicate to the warrant process, and not lie with Law Enforcement at all)

2b - The real possibility TAN/TARs will be used by Law Enforcement to coerce unlawful access/disclosure.

3 - The low bar required to issue TCN/TAN/TARs. The government's case for these powers is serious crime and terrrorism. However, "serious crime as defined under the Crimes Act" sets a 2 year sentence as the threshold, and is not in fact not of the seriousness as to justify the sweeping exercise of police powers the Bill envisages, and goes well beyond the public's expectation these powers are restricted to serious crime and terrorism. Powers that enable Law Enforcement to issue imperious directions within data centres under pain of criminal sanctions, or to declare martial law within a data centre, one would expert would attach only to criminal offences attracting sentences of say 20 years to life.

3a - the extraordinarily wide net of "service providers" all of whom can be targeted for investigation on the basis of this 2 year threshold.

4 - The lack of accountability. The reporting requirements are a rubber stamp, and leave the public none the wiser how these powers are being used, whether they're successful, and to what ends they're exercised. They will of course be used by the AFP to pursue journalist sources of government leaks. I'm not sure it's clear all leaks are against the public interest. There's that problem where the government's interests, and the public interest, are not always the same thing.

4a - There needs to be specific details as to the use of the power to enforce silence as to the existence of TCN/TAN/TARs. I'm thinking this power to suppress shouldn't lie with Law Enforcement at all, but should rather form part of the terms of the accompanying computer/data warrants.

5 - The Emergency provisions make the police a power answerable to themselves for 48 hours. The provision is tantamount to authority for the police to declare martial law within a data centre. Any imposition of an Emergency regime should require Ministerial authorisation with judicial approval.

5a - The combination of both Emergency powers, and the power to suppress reporting of the fact of the use of those powers, poses a serious danger where these powers can be exercised unilaterally by Law Enforcement, without the accountability and transparency to be expected consistent with the institutions of a liberal democracy.

5b - The combination of Emergency powers, the power to suppress reporting of the fact of the use of those powers, and that these powers can be exercised verbally, poses a serious danger where the rule of law can be suspended by Law Enforcement, and Australia's democratic institutions can be deliberately undermined. The combination of these powers is what one would expect of a tin pot dictatorship.

6 - The definition of "computer" which extends to any data held on any computer connected on "the same network" - which can be read as extending to the internet and anything that connects to the internet.

7 - The drafting is flawed, where TCN/TAN/TARs restrict themselves to a target computer. the Bill doesn't extend to compelling access to ancillary computers/network devices, needed to extract data from the target computer.

8 - The provision where evidence gathered unlawfully is legally admissible be removed, as offering too great an incentive for Law Enforcement to circumvent due process, with no countervailing deterrence.

8a - Evidence gathered must be only for which TAR/TAN has been issued, and for relates to the same offense for which data/computer warrant is in effect.

8b - Because computing histories now cover all aspects of a person's life, there must be a statutory limitation to the scope of evidentiary data. Data older than a statutory period (perhaps 7 years or some equally arbitrary period of time) must be put beyond the reach of legally admissible evidence. Or alternatively, restrict the admissability of evidence extracted under TCN/TAN/TAR to the offence for which the order was issued.

> The current drafting, allows Law Enforcement once they hold a warrant, to trawl a person's entire online life history for wrong doing. Allowing Law Enforcement to effectively go on a fishing expedition constitutes an unnecessary and arbitrary invasion of privacy, contrary to the Declaration of Human Rights.

This submission, discussing the objectives and provisions of The Assistance and Access Bill 2018, is divided into 4 parts, where is discussed:

1 - The framework under which the bill will be administered. The bill envisages a regime for data retrieval that parallels the existing warrant regime for search and seizure of the physical domain and of physical assets. This fails to reflect the complexity and business processes of service providers, who under the bill, have little scope to protect their interests or the interests of their customers, should law enforcement exceed their remit. There ought to be scope for a negotiated framework for the exercise of Assistance Notices that allows for service providers to comply in a manner consistent with established risk management, security, and change management processes. The author suggests an alternative framework that would better meet the needs of service providers, and reduce the possibility of adverse consequences for service providers arising as a consequence of their forced compliance under the bill.

The problem being where a diversity of agencies all have power to authorise and execute Assistance/Capability Notices. This should instead be managed through a single agency, that serves as the interface for the purposes of the bill, between law enforcement, and service providers. This is the only way to ensure a standard capability for intelligence gathering across agencies, smooth administration of justice and execution of Assistance/Capability Notices, and mitigates the vulnerability that arises from over a dozen different agencies and their agents all with access to service provider networks and services. This one agency should work as a clearing house for Assistance/Capability Notices, for disseminating gleaned data to client agencies, and for ensuring the protection of warrant data and service provider confidential information.

2 - Deficient public and industry consultation. Regardless of a very great public and industry outcry against the legislation, Dep't Home Aaffairs have moved the Bill from public consultation to the PJCIS in a period under 2 weeks (consultation closed 10th September, Bill was before PJCIS 20th September). This makes a mockery of the consultation process, and treats the public and industry with contempt. With under 2 weeks between closure of submissions and transfer to PJCIS, how could they have even read all submissions, let alone given them due consideration? The putative amendments between the exposure draft and the first reading are in substance equivalent to typographical corrections.

Nothing in the amendments suggests Dep't Home Affairs have absorbed the public and industry response, or given due consideration to the systemic problems evident in a rushed and dangerously flawed piece of legislation. Flawed from the perspective of protection of democratic traditions and institutions, the right to privacy, and the best interests of industry. There is not evident in this obtrusive Bill the necessary and proportionate balance of the interests of Law Enforcement.

There is a fantastic irony where the Minister for Home Affairs represents to the House that the Bill's powers are "reasonable, proportionate, practicable and technically feasible". Yet in the provisions, it lies within the remit of the Attorney General to decide what's "reasonable, proportionate, practicable and technically feasible", so disregarding established democratic tradition for transparency and accountability, and rather settles for a standard that is arbitrary and beyond review. It is of course no accident the proposed framework guarantees an arbitrary standard that answers to the government, rather than an independent and object standard managed by the judiciary.

3 - The Bill's objectives. The author is sympathetic to the argument that it is necessary to extend judicial writ from the physical realm to the cyber domain, however the provisions under the bill go well beyond this. There is absent the checks and balances needed to protect the public's right to privacy from unnecessary intrusion, and the interests of service operators from arbitrary and undue interference and disruption. Accountability for the exercise of these new powers is inadequate in the provisions, where there is the literal bare minimum reporting, not such as would provide for democratic oversite and accountability for the exercise of unprecedentedly intrusive police powers.

> "The bill requires that any obligations within a technical assistance notice and technical capability notice are reasonable, proportionate, practicable and technically feasible. We are not in the business of asking industry to do the impossible."
>
> Minister for Home Affairs - Speech to Parliament 20 Sept 2018

Unfortunately for the Minister, no one making submissions during the public consultation phase of the Bill appears to be making the case that Notices will be "reasonable, proportionate, practicable and technically feasible". Rather, the very great bulk of submissions point out the lack of provisions for transparency and accountability needed to achieve this outcome.

4 - An examination of those provisions of the bill that struck the author as of salient interest.

Framework

The bill anticipates a new regime for search and seizure, where Capability and Assistance Notices facilitate the examination and extraction of data under Data Warrants and Computer Warrants. The

Bill appears to have been drafted on a presumption that this new regime would overlay the existing warrant regime for search and seizure of physical property and physical assets. This does a grave disservice to the interests of service providers, where the commercial value of processes for risk management, security, and change management are given scan consideration, the possible impacts to the technical environment is gravely misrepresented, and where service providers can be put in a position of having little or no time to plan, test, stage and deploy changes within complex environments, with possibly gravely adverse consequences to their services, their customers, and their business. Quite possibly they may be compelled to silence, other than “something broke”, for which they will simply have to wear the reputational damage.

Issuing of Warrants & Assistance Notices

The Bill empowers a swathe of law enforcement agencies and their agents to issue Data/Computer Warrants and Assistance Notices. It goes further to extend this power to Senior Officers, which at the end of the day is probably several thousand individuals entrusted to exercise these powers in the interests of Law Enforcement, with no obligation to balance their actions against the interests of service providers, their customers, or the public’s democratic rights of privacy and free speech.

Access to Service Provider Networks

The Bill envisages a swathe of agencies that potentially will either have access, or be empowered to compel access, to service providers’ computer networks and data centres. This presents obstacles and considerable cost and risk for service providers to establish the credentials and authority every time an officer seeks to serve a warrant/notice.

If the access is to be provisioned as a permanent connection between the service provider and the agency, this will require them to reproduce the effort for every agency requesting access.

Custody of Warrant Data

The Bill envisages that warrant data will be in the custody of the agency (and officers) who issued the warrant/notice. Consequently custody of warrant data will be spread widely across a swathe of agencies. The replication multiplies the number of targets for would be hackers, and consequently multiplies the risk of warrant data leaking.

Custody of Service Provider Confidential Information

One can easily anticipate that in the process of preparing Capability Notices, a great deal of a service provider's intellectual property, internal process and security documentation, and other confidential information will gravitate towards a multiplicity of agencies. There is nothing specifica within the Bill as to ensure the protection of such information. Presumably the Privacy Act 1988 would apply, but the bill provides little in the way of incentive or compulsion for agencies to go to take pains to protect this information. Custody of this information across multiple agencies multiplies the risk of this confidential information leaking.

The author had anticipated that the exercise of the far reaching powers granted uner the Bill would lie only in the hands of at least Deputy Commissioners of Police (or equivalent). However we find that in fact these powers will extend to anyone of "authorising officer" rank as defined under the Surveillance Devices Act 2004, to include the following:

- 5(c) - a senior executive AFP employee the chief officer authorises undersubsection (5)10(c)
- 10c - a staff memberof ACLEI who is an SES employee the chief officer authorises undersubsection (5)5(c)
- 15(b) - an executive level member of the staff of the ACC the chief officer authorises under subsection (5)
- 5(c) a state or territory police Superintendent or a person holdingequivalent rank10(d)
- 10(d) an executive level officer of ICAC whom the chief officer authorises undersubsection (5)15(b)
- 15(b) - an executive level member of the Staff of the NSW Crime Commission the chief officer authorises undersubsection (5)20
- 20 - executive level member ofstaff of the LECC NSW (within the meaning of thatAct),
- 22(d) - an executive level sworn IBAC Officer (within the meaning of that Act) the chief officer authorises under subsection (5)
- 25 - a CCCQ senior executive officer (within the meaning of that Act)
- 35 - an ICAC SA executive level member of the staff of the Commissioner the chief officer authorises under subsection (5)

Surveillance Devices Act 2004 - Authorising Officers - 6A

Disproportionate Costs of Proposed Regime

The framework the Bill proposes is fatally flawed, where service providers will be compelled to engage with multiple agencies, (over a dozen), leading to duplication. This will result in wasted expenditure for both government and service providers, both in the sunk costs of infrastructure, in a confusing (and at times inconsistent and contradictory) requirements across different agencies complicating system design and delivery. There is no mechanism that will allow conflicting requirements of different agencies to be resolved.

Cost analysis suggests that the following sunk costs against the number of agencies a service provider must engage with. (The exponential ramp up of sunk costs is due to the way scale up happens, larger businesses (with larger capital costs) will engage with larger numbers of agencies).

Operator	Number Agencies	Avg Annual Requests TCN / [TAN/TAR]	Capital Costs	Annual Operating Cost	Annual Cost - (Proposed Framework)	Annual Cost - (1 Agency Model)	**% Cost Differential**
Service Provider	1	0.5 / 0.6	$355,000	$50,000	$406,000	$397,000	**2 %**
	1.5	0.7 / 1.5	$536,000	$77,000	$613,000	$422,000	**45 %**
	2.25	1.1 / 3.8	$817,000	$119,000	$937,000	$469,000	**99 %**
	3.375	1.7 / 9.8	$1,264,000	$188,000	$1,452,000	$563,000	**157 %**
	5.0	2.6 / 26.6	$2,003,000	$310,000	$2,313,000	$776,000	**197 %**
	7.5	4.3 / 75.7	$3,322,000	$547,000	$3,870,000	$1,310,000	**195 %**
	10	7.1 / 227	$5,534,000	$1,019,000	$6,553,000	$2,790,000	**134 %**
	10	12 / 719	$9,967,000	$2,163,000	$12,131,000	$7,300,000	**66 %**
	10	20 / 2415	$24,594,000	$6,035,000	$30,630,000	$22,237,000	**37 %**
Software Developer	1	0.5 / 0.6	$634,000	$81,000	$716,000	$699,000	**2 %**
	1.5	0.7 / 1.5	$969,000	$127,000	$1,096,000	$791,000	**38 %**
	2.25	1.1 / 3.8	$1,508,000	$207,000	$1,715,000	$965,000	**77 %**
	3.375	1.7 / 9.8	$2,417,000	$355,000	$2,773,000	$1,329,000	**108 %**
	5.0	2.6 / 26.6	$4,073,000	$663,000	$4,737,000	$2,167,000	**118 %**
	7.5	4.3 / 75.7	$7,442,000	$1,381,000	$8,824,000	$4,308,000	**104 %**
	10	7.1 / 227	$14,623,000	$3,216,000	$17,839,000	$10,334,000	**72 %**
	10	12 / 719	$33,126,000	$8,582,000	$41,709,000	$28,865,000	**44 %**
	10	20 / 2415	$95,057,000	$26,605,000	$121,663,000	$90,603,000	**34 %**

An Alternative - A Central Agency as Warrant/Notice Clearing House

Preparation of the Bill appears to have overlooked the obvious alternative, where the enforcement regime is managed through one central agency. This single law enforcement agency would be entrusted to manage the warrant/notice regime, with a mandate to create the processes and systems needed to support the regime, and be entrusted with the responsibility to protect the custody of both warrant information and service provider confidential information.

This agency could act as a clearing house for warrants/notices, and for the dissemination of warrant data to client agencies. It would need to be resourced to support the processes and systems facilitating access to service provider networks and data centres.

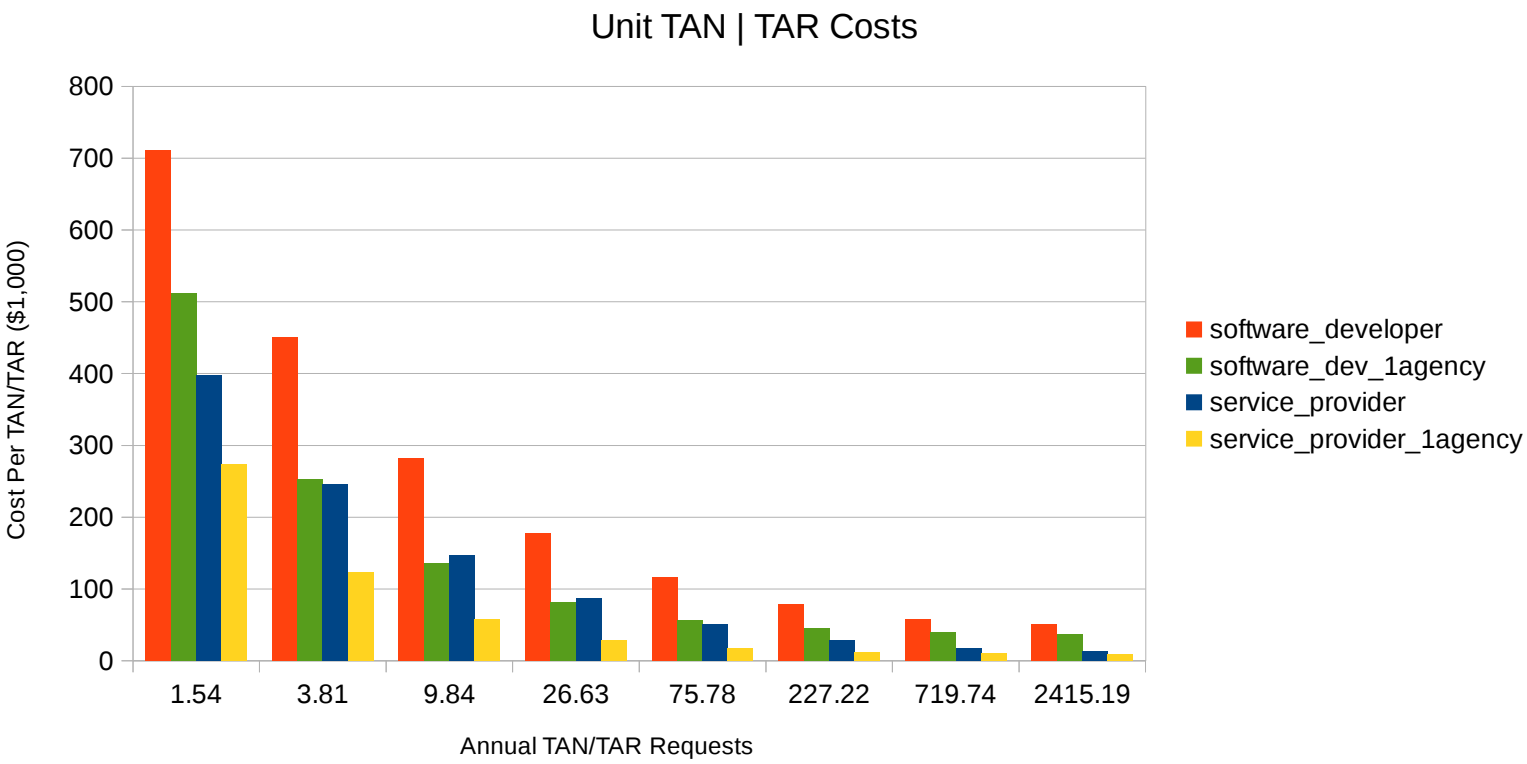
This approach is clearly preferable from a system's architecture perspective. By consolidating all the functions within a single agency, there are cost savings in eliminating the multiplication of effort, but more importantly, the multiplication of security risks across agencies is eliminated. By investing this agency with a mission to protect warrant data and service provider data, ensures that there is both accountability and resourcing for these such as would meet the public's expectation of government for protection of privacy.

Centralisation of data gathering with a single agency would greatly improve the effectiveness of the warrant/notices regime, where establishing and maintaining information capability with service providers was core business, and where establishing secure mechanisms and processes for information sharing across agencies was also core business.

Further, this would provide the opportunity to create information systems specifically designed for the protection and dissemination of warrant information across agencies. One example serves to illustrate the possibilities: it is the case that the SSL certificate has a field that allows for the certificate to be identified with a particular purpose, the Alternative Name field, where it supports an Object ID. Where a warrant was issued an Object ID, a unique SSL certificate could be allocated to a specific warrant/notice. All data subsequently collected within the purview of that warrant could be encrypted with the SSL's private key, providing a security layer that would encapsulate all data pertaining to the warrant. Service provider confidential information could be similarly protected, with a unique SSL certificate issued for each service provider. These certificates would be issued by the agency acting as a Certificate Authority. Service providers on uploading warrant data would need look no further than the certificate used for uploading the warrant data to ascertain the validity of the warrant. Client agencies would access the data through the same SSL certificate. One might hope that where separation of warrant data gathered under different warrants was cryptographically maintained would create more confidence with the public and service providers that the government was treating with private rights and privacy with the consideration they deserve.

Cost Comparison of Bill's Framework vs Centralised Agency

The following graph represents the unit cost of a single TAN/TAR as the size of the business, and the number of agencies it must engage with, scales up.



From the graph we can make the following observations:

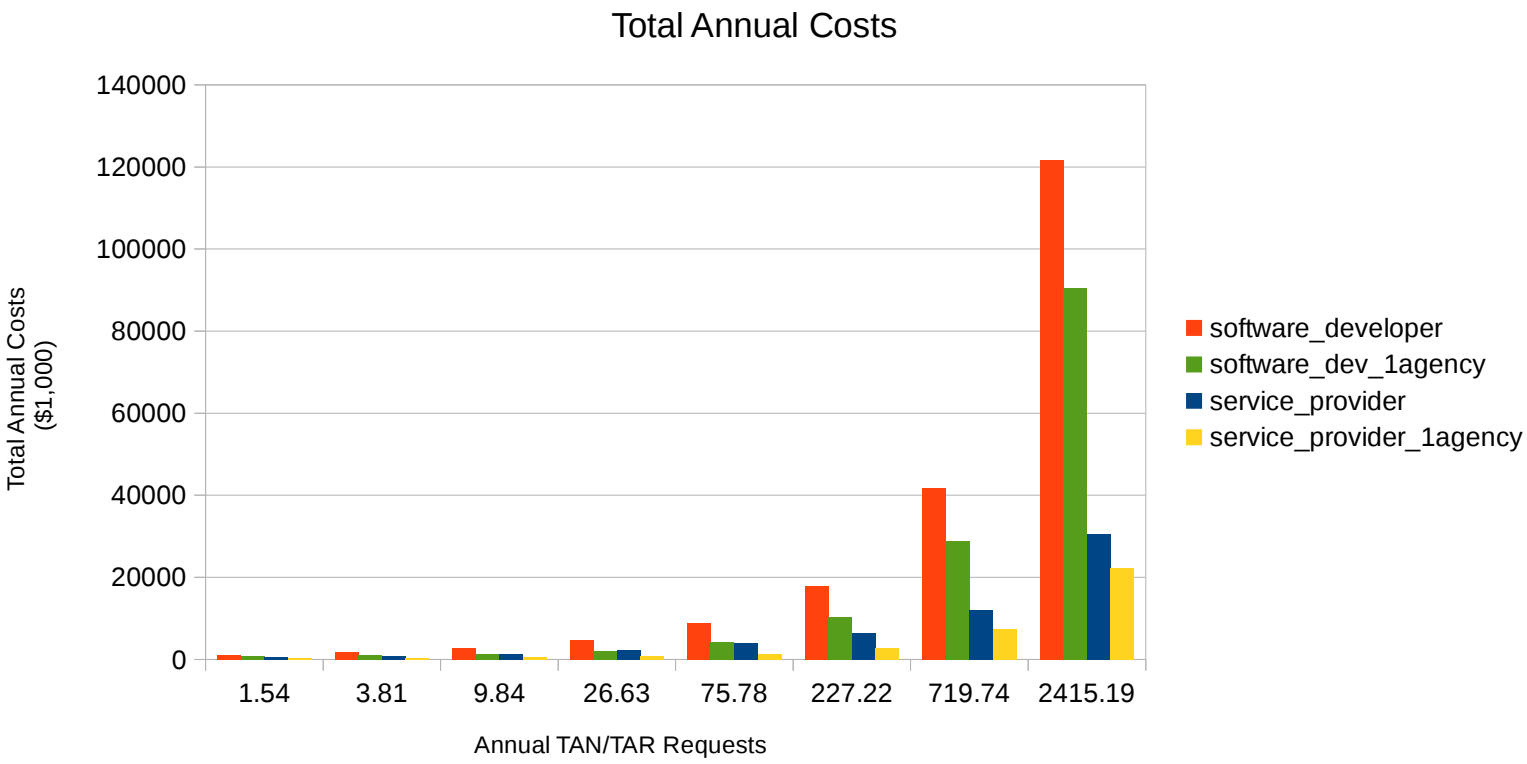
1 - As the size of the business/number of TANs/TARs received annually scales up, the unit cost of a TAN/TAR diminishes, providing an order of magnitude economy of scale. Small operators could face unit costs per TAN/TAR Request of $1,096,000 / $620,000 (respectively service providers / software developers). For very large operators, the costs drop to $50,000 / $12,000 respectively.

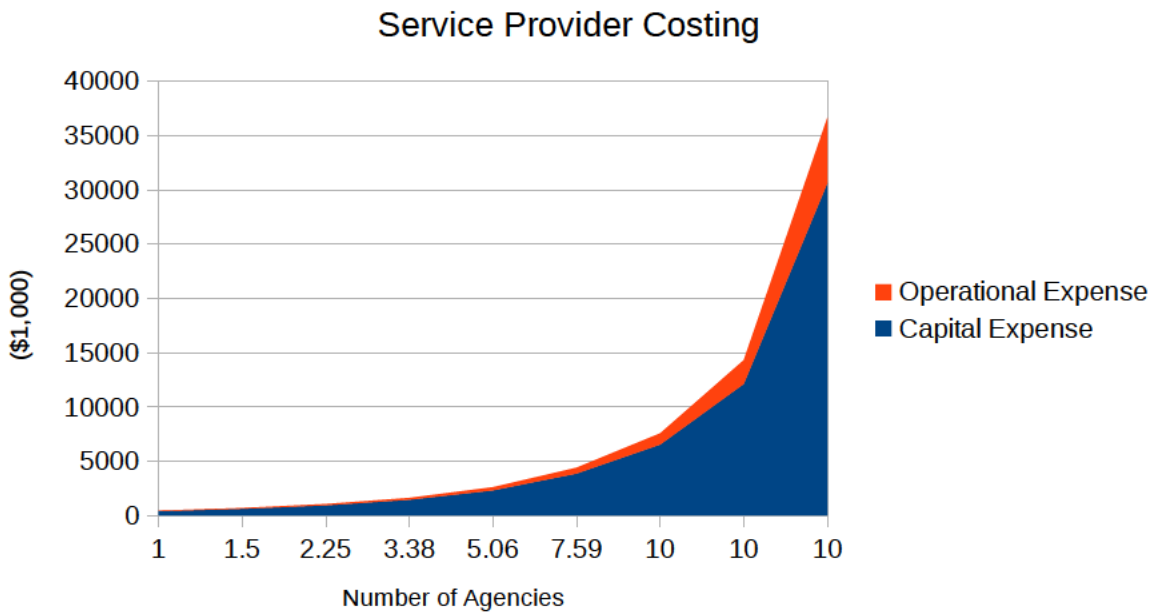
2 - The very considerable reduction in costs across the range for a centralised regime versus the regime proposed. Those who would benefit most from a centralised regime are medium scale operators, large enough that they need to sporadically engage with multiple agencies, but not so large that engagement where they regularly engage with all agencies. For example, software developers who engage with 5 different agencies would have their unit costs drop from $177,000 to $81,000, for a saving of 118%.

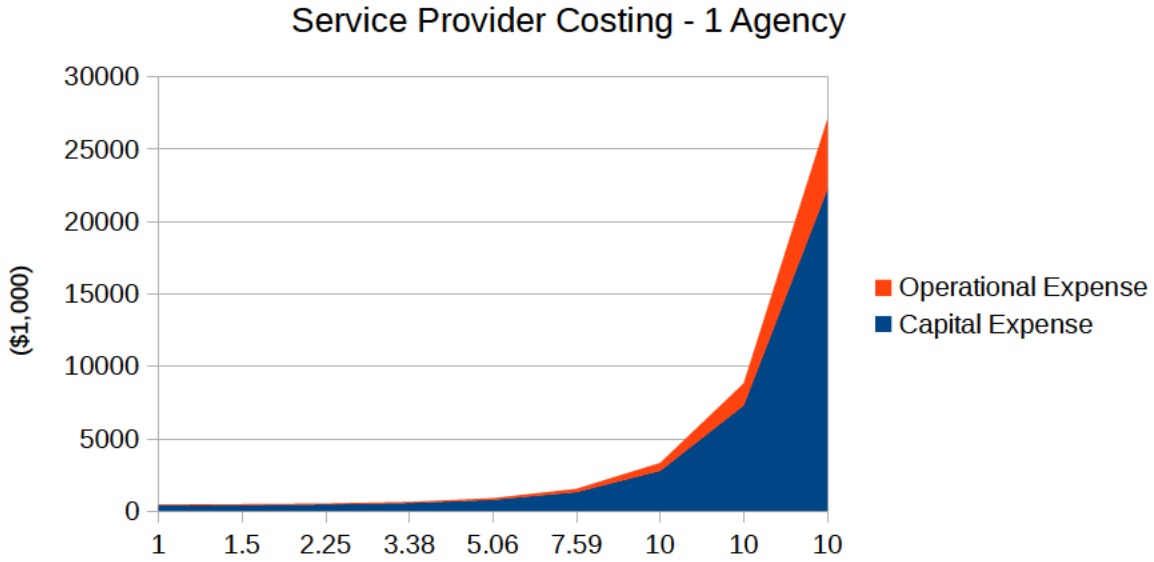
For very large operators, the savings are considerable, unit costs dropping from $50,000 to $37,000 for very large scale software developers, and from $12,000 to $9,000 for very large scale service providers. Where these costs are accrued across an annual 2000 TAN/TARs, there are very

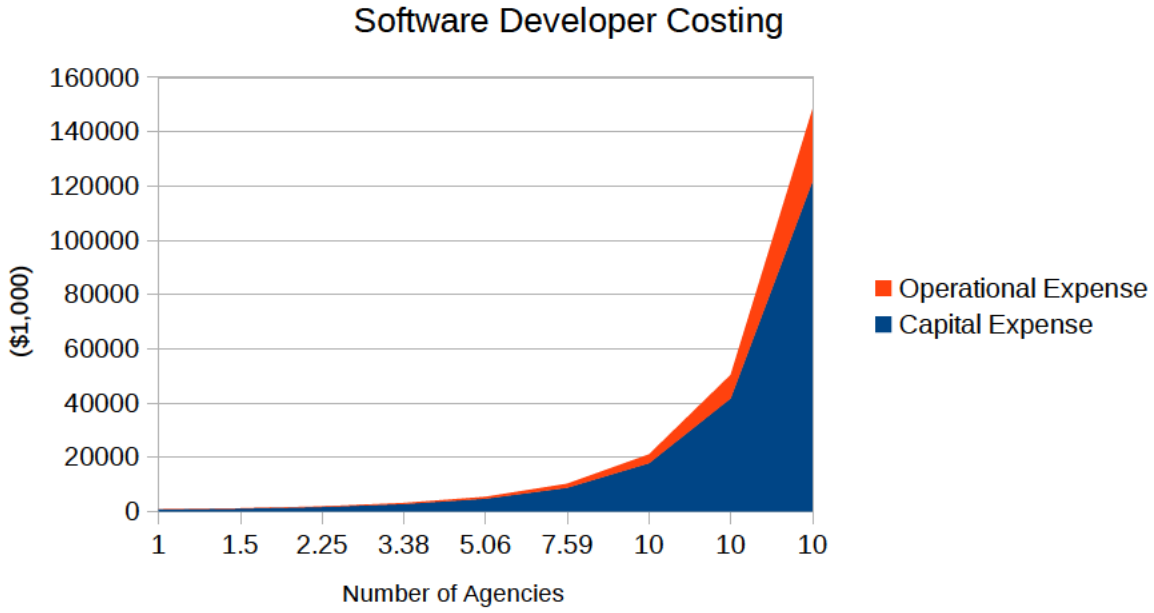
considerable cost savings to be made of the order of $31M annually for software developers, and cost savings of $8M annually for service providers.

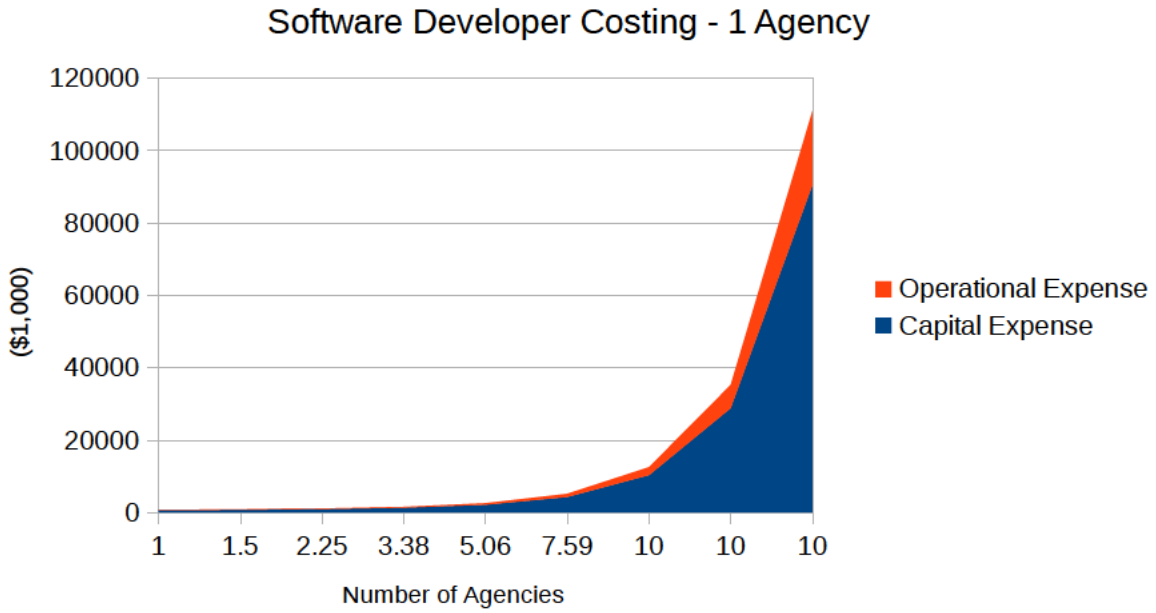
The following graph shows the analysis of annual costs, to service providers and software developers under both regimes.




Service Provider Costing
40000
35000
30000
25000
20000
15000
10000
5000
0
($1,000)
1
1.5
2.25
3.38
5.06
7.59
10
10
10
Number of Agencies
Operational Expense
Capital Expense


Service Provider Costing - 1 Agency
30000
25000
20000
15000
10000
5000
0
($1,000)
1
1.5
2.25
3.38
5.06
7.59
10
10
10
Operational Expense
Capital Expense


Software Developer Costing
160000
140000
120000
100000
80000
60000
40000
20000
0
($1,000)
1
1.5
2.25
3.38
5.06
7.59
10
10
10
Number of Agencies
Operational Expense
Capital Expense



Where the government will be obligated to reimburse for these costs, the public has a right to ask if hundreds of millions of dollars can be saved through creating a centralised enforcement regime, and the money saved could be spent elsewhere, for instance on conventional policing, does the public not have the right to insist that the government adopt the more cost effective framework?

Furthermore, an agency tasked with the specific responsibility of delivering the processes to liaise with industry, to act as custodian for warrant and service provider confidential information, and to disseminate this securely across client government agencies, will provide a better framework for governance, security, and management.

Hence, the government needs to reconsider the whole approach, and instead, consider having one centralised agency acting as a clearing house for TCN/TAN/TARs, and act as custodian of warrant data and service provider confidential data.

The PJCIS should initiate an investigation to establish whether a framework under which a centralised agency acts as a clearing house for warrants and notices would not be more cost effective and produce better outcomes.

The Bill’s Flawed Consultation Process

> "The government has consulted extensively with industry and the public on these measures and has made amendments to reflect the feedback in the legislation now before the parliament."
>
> Minister for Home Affairs - Speech to Parliament 20 Sept 2018

Regardless of a very great public and industry outcry against the legislation, Dep’t of Home Affairs have moved the Bill from public consultation to the PJCIS in a period under 2 weeks (consultation closed 10th September, Bill was before PJCIS 20th September). This makes a mockery of the consultation process, and treats the public and industry with contempt.

It should be noted regarding amendments, there has been nothing of substance altered from the original text. There is the removal of "protecting the public revenue" as an objective of the Bill, which was probably illegal. Other alterations are cosmetic and do not go to address the structural flaws and the evident lack of preparation in the Bill before bringing it to parliament.

Dep’t Home Affairs promised to publish all submissions. A check of their website

https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018

at 5 October 2018 shows that there is still only a limited, and to what degree selective we can’t tell, sampling of submissions accessible.

There are some very important omissions, notably:

- https://www.bsa.org/~/media/Files/Policy/Data/09102018BSACommentsAssistanceandAccessBill2018.pdf

- Digital Industry Group’s submission

It has been reported Home Affairs received over 700 individual submissions, (plus 14,300 from a Digital Rights Watch campaign letter). To sign off on the consultation process, and allow the Bill to progress to PJCIS, while some 600 submissions have not made it into the public arena, adds to the mounting evidence of a suspect consultative process.

The lack of support for public discussion of the Bill's goals and provisions no longer looks to be inadvertent. The parliament, the public and industry have been ambushed with a bill in a manner designed to steamroll through the consultative process. This raises serious questions where when the Minister for Home Affairs claimed before parliament that industry and the public had been widely consulted, whether in doing so he was entirely candid with the House as to the intention and purport of the consultation process.

1 - Any further progress of the Bill should be postponed until all public submissions to the Dep't Home Affairs public consultation be published and time sufficient allowed for due consideration by the public, industry, and parliament.

2 - The minister for Home Affairs should answer to the House as to the actual extent and timing of the public and industry consultation conducted in support of the Bill, and be required to provide evidence to support his 20th September claim to the House that consultation in support of the Bill has been extensive.

The Objectives of the Bill

It is fair to say that technological developments have outdistanced legislation. As a consequence, the “three Cs” - Criminals, Terrorist Conspirators, and Child Molesters, find that while subject to the peril of the rule of law within the jurisdiction of physical space, their activities enjoy comparative immunity within the cyber realm, arising from difficulties in detection of their activities, establishing identity, and evidentiary difficulties in producing proof sufficient to support a prosecution. The present situation is unsupportable, and if not addressed through extending judicial writ to the cyber domain, will get worse, as encryption and anonymising technology moves from geek concept to main stream.

On the other hand, moves to extend these powers to Law Enforcement, not subject to the protections, checks and balances consistent with liberal democracy, not subject to judicial oversight, and not subject to democratic accountability, are to be resisted as overreach and prejudical to the interests of liberal democracy.

> "The bill requires that any obligations within a technical assistance notice and technical capability notice are reasonable, proportionate, practicable and technically feasible. We are not in the business of asking industry to do the impossible."
>
> Minister for Home Affairs - Speech to Parliament 20 Sept 2018

It's very early days to be making representations to the House that TANs/TCNs will in fact be "reasonable, proportionate, practicable, and technically feasible". It's clearly too early to tell, and there's little in the Bill to ensure that TCNs/TANs/TARs in practice will in fact be "reasonable, proportionate, practicable and technically feasible."

Cyber Currency

If there is one competitive advantage enjoyed by cyber currencies over conventional currency, it is the supply of anonymity as a service. Consequently, in order for law enforcement to police money laundering and criminal transactions, they require access to cyber exchanges that would allow the identity of account holders to be identified. Consequently judicial writ ought to have scope for data collection of evidence of suspected criminal activity.

Social Media

Users of social media need to be subject to the rule of law, no less than other activities in the public domain. Consequently judicial writ ought to have scope for data collection of evidence of suspected criminal activity.

Anonymising Services

The purposes of the bill will be very much in opposition to providers of anonymising services, whose business model is predicated on providing strong anonymity. At the same time, there is a certain winking relationship between providers of anonymity as a service, and those using their services for criminal ends. The author anticipates a vocal response from hard line “privacy advocates” some of which will be motivated from criminal profit, or from the proceeds of criminal profit. Judicial writ ought to have scope for data collection of evidence of the use of anonymising services for suspected criminal activity.

Dark Net

Dark Net site operators can be expected to not cooperate with Law Enforcement. The Dark Net sites of interest to Law Enforcement will be operated by criminals, well aware that evidence of their activities will send them to prison, consequently, the application of the Bill to investigation of their operations is extremely limited. The effect of Assistance Notices will likely not extend beyond creating evidence of non compliance with an Assistance Notice.

Crimes of Foreign Origin

Where the Bill calls for cooperation with foreign law enforcement, it raises pregnant possibilities for unhappy outcomes, where Australian Law Enforcement may be compelled to remove the veil of anonymity for users who have broken no Australian law. Such would be the case where a user is pursued by foreign law enforcement for activities that would be lawful within Australia, but in foreign jurisdictions might meet the legal standard for adultery, blasphemy, sedition etc. Australian Law enforcement will then find themselves culpable in particular cases for having identified individuals then pursued by foreign law enforcement for capital crimes, albeit classed as lawful activity within Australia. It is beyond question that the interests of justice will not be served with such outcomes.

Child Recovery

Where technology can be used to assist in Child Recovery, this seems perfectly amenable to public expectations for the protection of democracy and privacy consistent with the rule of law. That said, as a non expert in child recovery, it would surprise the author if the great majority of target perpetrators were not aggrieved parents, consequently not the same profile as criminal collaborators, and therefore unlikely to use any degree of sophistication in their use of technology. Though Recovery Orders are included within the remit of the bill, they do not seem germane to the

proposed data recovery regime. As a consequence, the cooperation required of service providers for the execution of Recovery Orders will be different in kind to that for detection, identification, and prosecution of criminal collaborators. The author does not envisage that Law Enforcement activities for the execution of Child Recovery Orders under the Bill will greatly inconvenience service providers.

Search and Seizure in the Cyber Realm

> "Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute. It is an established principle that appropriate government authorities should be able to seek access to otherwise private information when a court or independent authority has authorized such access based on established legal standards. The same principles have long permitted government authorities to search homes, vehicles, and personal effects with valid legal authority. "
>
> **Five Country Ministerial 2018**

Now it's possible to have sympathy for the intent to ensure judicial writ extends to the cyber domain, while at the same time holding grave concerns that search and seizure of information assets can be so easily conflated with physical search and seizure. It betrays a lack of comprehension of the technical hurdles and complexities of extending judicial reach to IT systems. Without a framework which is specifically designed to cater for judicial reach extending to IT systems, there will be more light than heat, and a great number of unhappy outcomes. Most of this will be to the detriment of the service providers and the right to privacy.

The Crown needs to rethink the approach which presume Law Enforcement should be able to summarily issue Assistance Notices, to be given instant access to data centres. Otherwise there will be inevitable disruption to the businesses of service providers. There will be embarrassment and confusion where law enforcement front data centres with a valid writ, to be refused entry by data centre security officers, for reasons of ignorance of the application of these new powers, or from difficulty in establishing the credentials of law enforcement agents seeking entry, and confusion will ensue. There is the real prospect of security officers being criminalised for simply doing their job, which is to protect the security of the data centre. Law enforcement needs to create a framework that would allow managed entry to data centres, that would include such things as a prior identification of LEA officers with data centre security, and having the design and implementation of systems and processes needed for data extraction in place well before the issuance of Assistance Notices.

Powers of search and seizure within the cyber realm granted under the bill extend beyond judicial writ. Authority for actions by the state to invade privacy properly belongs with the judiciary. It's not acceptable to have authority for exercise of these powers to lie with law enforcement. The bill as drafted affords ample lattitude for the abuse of these powers by law enforcement agences,

particularly given the framework for accountability and oversite (or lack of it). The bill goes as far as to obscure the actions of law enforcement, where the bill empowers law enforcement to gag service providers as to the existence and terms of Assistance/Compliance Notices.

Emergency Powers

It's not clear that service providers may raise objections at any stage of the proceedings. Indeed, consideration of the interests of service providers is abundantly absent in the provisions of the Bill. Particularly in the case where emergency authorisations would circumvent judicial oversite, the legal jeapardy in which service providers find themselves where they would be chancing their arm and more, should they object to an Assistance Notice or equivalent, on grounds of infeasability, technological, security, or business risk, lack of notice given, the form of the capability notice where there is absent detail, or lack of technical competence evident in the Notice.

Given the 10 year custodial sentence that attaches to non compliance with Emergency Assistance Notices (64A(8), in all likelihood service providers will attempt to comply with whatever's in the order. There is the real likelihood of precipitating unhappy outcomes and considerable disruption to a service provider's business, attributable to a combination of cavalier belligerence and lack of preparedness on the part of law enforcement. Indeed, the bill encourages cavalier belligerence, signified where in the bill there is no consideration of a service provider's business management processes, of the necessity to comply with change controls, to manage security and risk, these are no defense for non compliance. Nor is there any requirement on law enforcement for technical competence in the framing of Assistance Notices, which will necessarily see non expert law enforcement officers issuing directions to technical experts who understand the risks and consequences, but have no lattitude whatsoever, no avenue to express objections, and no choice but to act as directed, even to the peril of the service provider's business and the interests of their customers.

The situation is entirely unacceptable where Law Enforcement are to be afforded a 48 hour window for directions to be issued without being subject to any judicial oversite, during such time the power to issue Assistance Notices (and verbal Assistance Notices) would make the Law Enforcement a law unto themselves within the service provider’s data centre, and one can anticipate volatile scenes where a Strike Force team can see no further than the narrow focus of the imminent apprehension (and career credit) of a wanted suspect. This is no idol consideration, where the Bill ensures that even should the direction by law enforcement be unlawful, the data collected regardless will be admissible. One need not be a cynic to see where ambition could trump scruples, to create a crisis in which an emergency 48 window ensues, and the threat of a 10 year custodial sentence might be used to either secure unlawful data access, or to put service providers in an impossible situation where they must comply with directions to the detriment of their business.

Verbal Emergency Powers - Necessity

The government has not made the case for the necessity to issue verbal TANs/TCNs/TARs. The Attorney General cites 200 police investigations in support of the Bill. The supporting documentation does not establish that a police power to issue verbal TANs/TCNs/TARs would produce better outcomes for police investigations, nor does it consider the considerable disruption that verbal orders will cause the business of service providers. It is also nowhere apparent that with adequate preparation by police, that all directions cannot be via the ordinary process. The suggestion that verbal direction powers be issued police, again suggests lack of consideration and appreciation for the security, risk, and management processes of service providers, where verbal inputs to the processes largely guarantee unhappy outcomes.

- **Verbal directions are inconsistent with the technical business processes of service providers, and as such, the power to issue verbal TANs/TCNs/TAR should be removed from the Bill.**

- **Any verbal TANs/TCNs/TAR issued by law enforcement should require the issuing authority to establish that the urgency could not have been avoided through sufficient preparation on the part of law enforcement, and that the same effect could not have been achieved through the process for written orders.**

Verbal Emergency Powers - Accountability

It’s difficult to see that there can ever be sufficient safeguards to ensure accountability for the exercise of the verbal direction police powers. There is an inevitability that where ill advised or unlawful verbal TANs/TCNs/TARs are issued and subsequently produce unfortunate outcomes, there will be no audit trail to establish where responsibility lies.

- **Any verbal TANs/TCNs/TAR issued by law enforcement should require a prior judicial authorisation.**

Accountability and Oversite

It's not acceptable that accounting for exercise of these powers to government and the public constitute no more than a rubber stamp metric annual reporting of the number of Assistance/Capability notices issued. There needs to be detail as to the kind of criminal activity being investigated, the seriousness of the crime, and percentages of Assistance Notices issued that led to successful prosections. There needs to be a separate metric for the number of Capability / Assistance notices issued, where non disclosure formed part of the terms of the notice.

Checks/Balances

Any exercise of the sweeping police powers suggested in the Bill should be subject to judicial oversite, both a priori and post facto the issue of TCNs/TANs/TARs.

There must be instituted a civil process for issuing TCNs/TANs/TARs that includes judicial authorisation, and allows service providers opportunity to object to the fact and/or terms and/or timing of orders issued by law enforcement. Grounds for objection should include at least the following:

- **Technical integrity, validity, and relevance of TCNs/TANs/TARs directions**
- **Direct and indirect costs**
- **Disruption of service provider security management processes and responsibilities**
- **Disruption of service provider risk management processes and responsibilities**
- **Disruption of service provider's business processes and responsibilities**
- **Disparity/conflict of TCN/TAN/TARs with obligations of the service provider under the Privacy Act 1988, other legislation, and common law fuduciary duties**
- **The public interest**

Provision for Destruction of Copies of Restricted Records

The provisions for destruction of restricted records under the Telecommunications (Interception and Access) Act 1979 do not extend to copies of restricted records, (by virtue of the definition of restricted record Part 1-2(5) Interpretation. Given the ease of reproduction of copies of digital

records, the Crown ought to make proper provision to control both restricted records, and any copies, and ensure that where a restricted record is to be destroyed, so too should be all copies.

This process would be significantly more secure if the author's suggestion were adopted, where a unique SSL certificate is assigned to each warrant, and warrant data encrypted such that subsequent access to the record in the usual line of business required authorised use of the SSL certificate's private key.

Specific Provisions

50 After subsection 28(1)

Insert:

(1A) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for access to data held in a computer (the target computer) if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably

suspects that:

(a) an imminent risk of serious violence to a person or substantial damage to property exists; and

(b) access to data held in the target computer is immediately necessary for the purpose of dealing with that risk; and

(c) the circumstances are so serious and the matter is of such urgency that access to data held in the target computer is warranted; and

(d) it is not practicable in the circumstances to apply for a computer access warrant.

59 After subsection 32(2)

(2A) An emergency authorisation for access to data held in a computer may authorise anything that a computer access warrant may authorise.

One might expect the breath taking reach of this emergency power to lie in the hands of at least Deputy Commissioners of Police. However the Bill extends this power (unacceptably in the author’s opinion) to the following:

- 5(c) - a senior executive AFP employee the chief officer authorises undersubsection (5)10(c)
- 10c - a staff memberof ACLEI who is an SES employee the chief officer authorises undersubsection (5)5(c)
- 15(b) - an executive level member of the staff of the ACC the chief officer authorises under subsection (5)
- 5(c) a state or territory police Superintendent or a person holdingequivalent rank10(d)
- 10(d) an executive level officer of ICAC whom the chief officer authorises undersubsection (5)15(b)
- 15(b) - an executive level member of the Staff of the NSW Crime Commission the chief officer authorises undersubsection (5)20
- 20 - executive level member ofstaff of the LECC NSW (within the meaning of thatAct),
- 22(d) - an executive level sworn IBAC Officer (within the meaning of that Act) the chief officer authorises under subsection (5)
- 25 - a CCCQ senior executive officer (within the meaning of that Act)
- 35 - an ICAC SA executive level member of the staff of the Commissioner the chief officer authorises under subsection (5)

Surveillance Devices Act 2004 - Authorising Officers - 6A

This is wholly unacceptable to the author, where a police task force have a 48 hour remit to act as a law unto themselves, to compel compliance with their directions in the interests of the mission of the task force, potentially trumping and riding rough shod over established business practices for risk, security, and change management, regardless of the technical risks to the service provider’s business, technical ignorance, and the lack of preparedness and planning on behalf of Law Enforcement agencies. One would hope that technical ignorance could be confined to the ranks of Deputy Commissioner or above.

50(1)(g), (h) and (I)

Nothing in these paragraphs reflects the severity of the crimes committed, nor reflects their nature - money laundering, drug trafficking, child exploitation, etc. The public have a right to know not only the number of arrests and prosecutions, but to what ends these law enforcement actions were exercised. There ought also to be specific quantitative disclosure of prosecutions within the realm of free speech prosecuted as terrorism, hate speech, harassment, child exploitation etc. and also

quantitave reporting of the prosecution of journalists. There should also be provision for quantitave reporting of custodial sentences delivered, both number and length of custodial sentence.

64A

Provisions do not extend to securing cooperation in gaining physical access to computers, such as might be required to secure a physical connection to target computers. The author suspects this betrays ignorance on the part of the bill's authors of some of the methods that could be employed by law enforcement in the execution of data warrants. Or perhaps they didn't think it necessary, as covered under warrants for physical access. Though probably best to clarify, because if there's a gap at the interface, between physical access, and computer access, this may be grounds for defence council to challenge the legality of the subsequent evidentiary chain.

This would also be relevant where non cooperative service providers may have deliberately restricted administrative access according to the location of computer terminals, or made provision to restrict access to those with local knowledge or unique cryptographic devices, in an attempt to impede the execution of warrants.

Another consideration is where terminal access is controlled by a systems administrator or network administrator other than the system administrator who administers the target computer.

Another consideration is where systems other than the target computer control authorisation and access to the target computer.

37 Subsection 6(1)

data held in a computer includes:

> (b) data held in a data storage device on a computer network of which the computer forms a part.

It's an open question to what extent this definition can be legally enforced. This could be read as an overreaching attempt to provide for search of the data of any computer connected to the internet, as all the data on all these computers meet the standard of "data held in a data storage device on a

computer network of which the computer forms a part". There is the same problem at organisational and corporate boundaries, and within government departments. This is an extremal definition.

A minimalist definition would be to restrict the scope of any computer network to one within the computer network's "immediate circle" (as defined by the Telecommunications Act 1997).

The jurisdiction of writs/notices ought to lie somewhere between the 2 positions, recognising that cloud and virtual file systems means that a computer's data storage may lie beyond the computer's "immediate circle", but to employ a definition where all the internet is within the purview of a single writ/notice is overreach, and the courts would be well within their right to take a prejudicial view. One unanticipated consequence would be where an Emergency Assistance Notice is used to effect the discovery of a proxy chain, and the 48 hour suspension of judicial oversite used to follow the proxy chain wherever it leads, hoping to arrive at the ultimate destination within the 48 hour interval. If on the other hand, this particular drafting is intentional, it should not be allowed to stand.

317ZS Annual reports

A private citizen will only ever see the number of Capability/Assistance Notices issued. Which is meaningless. There needs to be correlation to investigations and prosecutions, and their type and seriousness. There needs to be further provision for specific reporting of the number of Assistance Notices issued where non disclosure formed a part of the notice.

3F(2)(2a)(b)

> if necessary to achieve the purpose mentioned in paragraph (a)—to add, copy, delete or alter other data in the computer or device mentioned in subparagraph (a)(i); and

There will be circumstances where the data that needs to be added/copied/deleted/altered to secure access resides on a different computer (hypervisor/virtual machine/firewall/proxy/cryptographic vault). Indeed, the Bill creates this eventuality where such measures are employed to frustrate such access. A chain of virtual machines across data centres and jurisdictions, being one possibility. It's not even clear that if a virtual machine's sole purpose is to provide secure access to a computer which is used for criminal purposes, whether the Bill will service to afford jurisdiction.

3F(2)(2a)(c) - Confidential

See separate submission.

3F(2)(2C)

Subsections (2A) and (2B) do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer; unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or

(b) cause any other material loss or damage to other persons lawfully using a computer.

The phraseology is problematic and at cross purposes. On the one hand, (b) disallows material loss. Where (a) (ii) permits material interference in the prosecution of the warrant.

1 - (b) should extend to disallow material loss for the service provider

2 - (a)(ii) Fails to recognise that “lawful use by other persons” may number hundreds or thousands, and that it may be quite impossible for law enforcement to even know of the importance to their interests of reliability of service, or of the consequences of an interruption of that service.

6A At the end of section 3K 6 (vii)

(vii) a deceased person who, before the person’s death, used the relevant computer;

Probably “used, or is reasonably suspected of having used or had in their posession, the relevant computer” may be preferable, on the grounds that a deceased person may be a result of unlawful death, and the computer may furnish evidence of their unlawful death.

9 Paragraphs 201A(1)(a), and (c)

(a) access data held in, or accessible from, a computer or data storage device that:

(i) is on warrant premises; or

…

(c) convert into documentary form or another form intelligible to an executing officer:

(i) data held in, or accessible from, a computer, or data storage device, described in paragraph (a); or

Which extend to any computer reachable via the internet. All under the jurisdiction of a premises warrant. This has every appearance of being an ambit claim and can only make for bad law. Similar to concerns of 37 Subsection 6(1), there ought to be a limitation to judicial reach of a writ somewhat beyond immediate circle, but less than the global internet.

13 At the end of paragraph 201A(2)(b)

(vi) a person who is or was a system administrator for the system including the computer or device; and

Arguably those who maintain network devices (network administrators) are beyond the purview of this clause. Not only because they're arguably not system administrators, but more importantly, they do not administer the computer, but rather control network access to the computer. Similar considerations apply to security devices, which may require modification to non target systems to enable access to the computer.

21A Voluntary assistance provided to the Organisation

1(d) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and

Possibly directly contradicts the Privacy Act 1988.

34AAA 1(b)

(b) copy data held in, or accessible from, a computer, or data storage device, described in paragraph

Here, the issue of the overreach of the global internet raised against 37 Subsection 6(1), does not apply. Given the combined gravity of the Director General's and the Attorney General's imprimatur,

across heads of government, jurisdictional reach within the purview of the order in this instance is perfectly appropriate.

However, note that in 37 Subsection 6(1) and elsewhere, the combined Director General's and Attorney General's authorisation is not required, and so this provision serves to undermine the justification for the judicial reach of 37 Subsection 6(1).

34AAA 2a(v)

> 2a(v) access by the Organisation to data held in, or accessible from, the computer or data storage device will be for the purpose of obtaining foreign intelligence relating to a matter specified in the relevant notice under subsection 27A(1); and

Again the problem of overreach, regardless of the imprimatur of the Attorney General's authorisation, the authorisation does not span heads of government. Consequently the warrant can issue entirely from within the government. The extension of judicial warrant to the global internet is overreach. If a 27A warrant applies, a request should come from the Director General, as provided for under 34AAA 1.

Appendix A - Cost Analysis Workings & Assumptions

TCN Costings

Service Provider TCN - New Agency											Sunk Cost	Annual Cos
Specification			5	na		10	2.5					
Design		20	10	na		2						
Implementation	10	20	5	na		1						
#### Total ####	**10**	**60**	**60**	**na**		**32.5**	**12.5**	**50**	**20**	**225**	**30**	
Service Provider TCN - New Capability												
Specification		10	10	na		5	5					
Design		10	10	na		2						
Implementation	20	50	20	na		2						
#### Total ####	**20**	**105**	**120**	na		**22.5**	**25**	**10**	**10**	**302.5**	**30**	
Service Provider TCN - Cabability Extension												
Specification		2	2	na		2	2					
Design		2		na		1						
Implementation	4	10		na		1						
#### Total ####	**4**	**21**	**6**	**0**		**10**	**10**	**2**	**2**	**53**	**6**	
Software Developer TCN - New Agency												
Specification		na	10	5		10	5					
Design		na	15	10		2						
Implementation	5	na	15	50		1						
#### Total ####	**5**	**na**	**120**	**162.5**		**32.5**	**25**	**50**	**25**	**395**	**30**	
Software Developer TCN - New Capability												
Specification		na	10	5		5	5					
Design		na	15	10		2						
Implementation	1	na	15	50		2						
#### Total ####	**1**	**na**	**120**	**162.5**		**22.5**	**25**	**200**	**100**	**531**	**101**	
Software Developer TCN - Capability Extension												
Specification		na	5	2.5		2.5	2					
Design		na	7.5	5		1						
Implementation	0 5	na	7.5	25		1						
#### Total ####	**0.5**	**na**	**60**	**81.25**		**11.25**	**10**	**20**	**50**	**183**	**50.5**	
Assumptions	Admin	Network En	Architect	S/W Dev	Security	Test	BDM	Legal	Capital	Annual Operating Costs		
Charge Rates ($k/day)	1	1.5	3	2.5			2.5	5				

TAN / TAR Costings

Service Provider TAN|TAR - New Agency											Sunk Cost	Annual Cos
Specification			0.5	na			1	2.5				
Design		1	2	na			0.5					
Implementation	5	3	0	na			0.5					
#### Total ####	**5**	**6**	**7.5**	**na**			**5**	**12.5**	**50**	**10**	**86**	**15**
Service Provider TAN|TAR - New Capability												
Specification			0.5	na			1	2.5				
Design		1	2	na			0.5					
Implementation	3	3	0	na			0.5					
#### Total ####	**3**	**6**	**7.5**	na			**5**	**12.5**	**5**	**5**	**39**	**8**
Service Provider TAN|TAR - Cabability Extensio												
Specification		0	0.1	na			0.2					
Design		0.2	0.4	na								
Implementation	0.6	0.6	0	na								
#### Total ####	**0.6**	**1.2**	**1.5**	**0**			**0.5**	**0**	**1**	**1**	**4.8**	**1.6**
Software Developer TAN|TAR - New Agency												
Specification		na	0.5	2			1	2.5				
Design		na	2	4			0.5					
Implementation	5	na		15			0.5					
#### Total ####	**5**	**na**	**7.5**	**52.5**			**5**	**12.5**	**25**	**12**	**107.5**	**17**
Software Developer TAN|TAR - New Capability												
Specification		na	0.5	2			2	2.5				
Design		na	2	4			1					
Implementation	3	na #		15			0.5					
#### Total ####	**3**	**na**	**7.5**	**52.5**			**8.75**	**12.5**	**100**	**50**	**184.25**	**53**
Software Developer TAN|TAR - Capability Exten												
Specification		na	0.1	0.4			0.5					
Design		na	0.4	0.8								
Implementation	0.6	na		3								
#### Total ####	**0.6**	**na**	**1.5**	**10.5**			**1.25**	**0**	**5**	**5**	**18.85**	**5.6**
Assumptions	Admin	Network En	Architect	S/W Dev	Security	Test	BDM	Legal	Capital	Annual Operating Costs		
Charge Rates	1	1.5	3	2.5			2.5	5				

Total and Unit Costs

Service Provider	Sunk	Annual		Sunk	Annual
TCN New Agency	**225**	**30**	TAN|TAR New Agency	**86**	**15**
TCN New Capability	**302.5**	**30**	TAN|TAR New Capabili	**39**	**8**
TCN Capability Extension	**53**	**6**	TAN|TAR Capability Ext	**4.8**	**1.6**
Software Developer					
TCN New Agency	**395**	**30**	TAN|TAR New Agency	**107.5**	**17**
TCN New Capability	**531**	**101**	TAN|TAR New Capabili	**184.25**	**53**
TCN Capability Extension	**183**	**50.5**	TAN|TAR Capability Ext	**18.85**	**5.6**

Service Provider Profile	Agencies	Annual TCN	Annual TAN | TAR	Capitalised Cost	Annual Costs	Total Annual Cost	Annual Cost/ # TAN|TAR
As Proposed	1	0.5	0.6529129225	355 3419442227	50.6625249463	406.0044691691	621 8355544746
	1.5	0.73928914	1.5435218196	536 8153378215	77.1675176521	613.9828554736	397.7804833572
	2.25	1.114681684	3.809370002	817 952458657	119.1463149472	937.0987736041	245 9983601243
	3.375	1.715553358	9.8358197441	1264 202822523	188.3178844308	1452.5207069538	147 6766293757
	5.0625	2.697865309	26.6296730767	2003 632013504	310.1250362849	2313.7570497893	86 8864233943
	7.59375	4.339773853	75.7790004012	3322 845005124	547.9178112622	3870.7628163863	51.0796235883
	10	7.148851501	227.2171255928	5534 977746877	1019.0167139364	6553.9944608134	28 8446323917
	10	12.07379817	719.7436803175	9967.445619249	2163.6457485056	12131.0913677544	16 8547382902
	10	20.93302197	2415.1910962016	24594 59987313	6035.8654400169	30630.4653131461	12 6824189445

Software Developer Profile	Annual TCN	Annual TAN | TAR	Capitalised Cost	Annual Costs	Total Annual Cost	Annual Cost/ # TAN|TAR
As Proposed	1	0.5	0.6529129225	634 5065883263	81.5261196184	716.0327079446	1096 6741249868
	1.5	0.73928914	1.5435218196	969 3924118915	127.5275273427	1096.9199392342	710 6604683549
	2.25	1.114681684	3.809370002	1508 21627507	207.0594533475	1715.2757284175	450 2780584472
	3.375	1.715553358	9.8358197441	2417 674682033	355.6263651698	2773.3010472031	281 9593200527
	5.0625	2.697865309	26.6296730767	4073 925444421	663.1547375117	4737.0801819324	177 8872826676
	7.59375	4.339773853	75.7790004012	7442 880944339	1381.5355516716	8824.4164960108	116.4493652502
	10	7.148851501	227.2171255928	14623 23393165	3216.5437795109	17839.777711161	78 5142302308
	10	12.07379817	719.7436803175	33126.40208699	8582.8491426039	41709.2512295933	57 950145823
	10	20.93302197	2415.1910962016	95057 82507905	26605.905305009	121663.730384063	50 3743702001

Service Provider Profile	Agencies	Annual TCN	Annual TAN | TAR	Capitalised Cost	Annual Costs	Total Annual Cost	Annual Cost/ # TAN|TA	Cost Differential
1 Agency Model	1	0.5	0.6529129225	347 9879631253	49.8535928111	397.8415559364	609 3332544715	2.0518000472
	1	0.73928914	1.5435218196	369.4532834883	53.2864437018	422.73972719	273 8799813656	45.2389770781
	1	1.114681684	3.809370002	408.78278195	60.3396985261	469.1224804761	123 1496232257	99.7556741798
	1	1.715553358	9.8358197441	487 3570426243	76.2367580835	563.5938007078	57 3001351562	157.7247487693
	1	2.697865309	26.6296730767	661.0019028171	115.5536025299	776.555505347	29 1612857248	197.9512776431
	1	4.339773853	75.7790004012	1088.467985624	221.7420525105	1310.2100381348	17 289882833	195.4307098652
	1	7.148851501	227.2171255928	2258 254539638	532.7286119455	2790.9831515837	12 2833309518	134.8274462744
	1	12.07379817	719.7436803175	5787.063293785	1513.8392130048	7300.90250679	10 1437535423	66.1587914162
	1	20.93302197	2415.1910962016	17404.48364958	4832.8846628717	22237.3683124539	9 2072914427	37.7432117091

Software Developer Profile	Annual TCN	Annual TAN | TAR	Capitalised Cost	Annual Costs	Total Annual Cost	Annual Cost/ # TAN|TAR	
1 Agency Model	1	0.5	0.6529129225	620.4069984574	78.7162159921	699.1232144495	1070.7755818379	2.4186714367
	1	0.73928914	1.5435218196	692 5138554071	98.5026755517	791.0165309588	512.4751208006	38.6721890508
	1	1.114681684	3.809370002	829 1923238578	136.4666751915	965.6589990493	253.4957220057	77.6274782409
	1	1.715553358	9.8358197441	1113.044324327	216.3587001483	1329.4030244754	135 1593521501	108.6125122438
	1	2.697865309	26.6296730767	1765 348941705	402.2928024155	2167.6417441207	81 3994876273	118.5361208687
	1	4.339773853	75.7790004012	3427 317170983	881.0751417425	4308.3923127252	56 8546997178	104.8192424341
	1	7.148851501	227.2171255928	8097 25828688	2236.9883418159	10334.2466286962	45.481812173	72.6277526765
	1	12.07379817	719.7436803175	22441 53776268	6423.5702798822	28865.1080425576	40 1047050942	44.4971249306
	1	20.93302197	2415.1910962016	70197.46013124	20406.046526543	90603.5066577798	37 5140115415	34.2814807859

Cost Assumptions

- Estimates are for modal costs of TCN/TAN/TAR
- Technical effort for a service capability extension is 1/5 the effort of implementing the capability
- Technical effort for a software capability extension is ½ the effort of implementing the capability
- Cost for a service assumes a 10k user base.
- 1 out of 10 requests require development of a new capability
- 9 out 10 requests require only an extension of a current capability
- In the 1 agency model, the 1/10 capability extension ratio, moves out to 1/20

* Disclaimer: These cost estimates are supplied for the exclusive use of the PJCIS in its appraisal of the Assistance and Access Bill 2018. The author makes no express or implied warranty as to the validity or usefulness of these cost estimates.