To whom it may concern,

I am emailing to submit comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in regards to the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 as a concerned member of the public.

For at least 15 years I have been employed in technology-related roles, and have for the last 3 years been working for a large multinational cloud software vendor. My role at the company involves developing software, and I am thus very knowledgeable about the internet and software security. Security has always been at the front of my mind when it comes to software development, and it is even more critical nowadays given the current threat environment.

I am passionate about technology, keep up with local and world events, and am particularly interested in the way that these topics intertwine.

I'm writing to convey my serious concerns about:

- The viability of the technical demands placed on companies by this Bill.
- The Bill's impact on the privacy of Australian citizens.
- My career prospects as tech companies decide to no longer expand into/ retreat from the Australian market.
- The quality of life as these companies decide to block access for Australian consumers to avoid the compliance burden.

I have listed my concerns point-by-point below:

1) It is a backdoor

The most secure message is one that cannot be read. Software developers have used this principle to reduce the amount of parties able to read a communication to just two: the sender, and the recipient. The forceful imposition of a third party into the communication channel regardless of the means is a back door as per the Wikipedia definition:

https://en.wikipedia.org/wiki/Backdoor_(computing)

"A backdoor is a method [...] of bypassing [...] encryption in a computer system"

"Backdoors are often used for [...] obtaining access to plaintext in cryptographic systems."

The above is what this law is proposing to do, and therefore by the Wikipedia definition the Bill does introduce a backdoor into encrypted systems. The introduction of a third party into the communication mix will lower the security for Australian companies and citizens in their digital life.

2) Alternate means of communication

Serious criminals will always have alternate, secure means of communication such as the following:

- PGP - https://www.openpgp.org/
- TrueCrypt - http://truecrypt.sourceforge.net/
- Tor - https://www.torproject.org/
- Tails - https://tails.boum.org/

If this law is introduced, serious criminals may move to these alternate communication channels or to non-digital means of communication, and once again law enforcement will "go dark".

For the serious crimes that the Bill is intended to address such as terrorism, criminals have already shown to be avoiding using technology and using pre-digital methods of communication. Criminals doing so would negate the benefits of the Bill, however the negative effects it introduces will remain. For this I refer to an episode of the Australian Broadcasting Corporation's "The Signal" podcast, dated 24 September 2018 entitled "How your tech could land you in jail":
http://www.abc.net.au/radio/programs/the-signal/how-your-tech-could-land-you-in-jail/10296236

In it, a member of the Digital Forensics team at the Australian Federal Police (AFP) is interviewed and is introduced by the show host with the statement:

"Criminals have already started to learn what kinds of things police can crack, and so they're starting to actually do crime differently".

The AFP member then outlines the following:

"I guess I can point to some of our recent terrorist investigations, counter terrorism investigations, we would see back in the day that a lot of people would communicate via email, messaging and so forth. But there has been an um, noticeable, um, sort of drift back towards people not using devices; it is not uncommon now to go into a warrant and so forth and not find any trace of an electronic device and um, that more likely the other skillsets we offer within

the AFP like document examination and so forth come to the fore, uh because they are going back to written communications because they don't trust the electronic devices."

3) It weakens cyber security

Having a secure encryption algorithm is only part of the picture to ensure cyber security. Another incredibly important part is the implementation of that algorithm and the surrounding software processes. Many vulnerabilities have been found in encryption software in the recent years (such as Hearbleed http://heartbleed.com/), and almost all of them have been due to the implementation of the algorithm and the surrounding software processes, rather than the algorithm itself.

Over the years, software developers and security engineers have developed best practices & design patterns for the implementation of encryption algorithms to avoid these issues. Some don't follow them correctly, however when they are followed it generally leads to a secure system.

The introduction of a law which will require Australian companies, and companies operating in Australia to deviate from international best practices & design patterns will open the door to new implementation vulnerabilities that have not been accounted for, and due to Australia's population size and small security research community, it is likely that these vulnerabilities will stay unknown for extended periods of time, allowing malicious actors large windows of time to exploit them.

4) It slows innovation & global competitiveness

Having this law to comply with, the potential for fines and jail sentences, and the decrease in cyber security that is imposed on companies by having to comply with the law, some companies may choose to not enter the Australian market.

This may lead to:

- less jobs in the technology sector
- less skilled Australians getting exposure to innovative technology
- a lack of global competitiveness of local companies who have additional bureaucratic burdens placed on them
- talented Australians who the country has subsidised education for leaving the country for places that are less burdensome for technology companies (such as Silicon Valley)

- less tax revenue as Australian citizens are forced to interact with offshore companies via the internet to purchase services that GST is not charged on (due to there not being any local operation or assets for that company)

5) It's a privacy invasion & risk

Society is changing. Whereas 20 years ago communication was done face to face, nowadays families in the privacy of their home use WhatsApp, Facebook Messenger etc. to chat to each other from the next room. This opens up the inner thoughts of Australian citizens to an even greater risk of privacy invasion, and an increased level of personal and corporate cyber security is needed to protect this.

Some say that "If you've got nothing to hide, you've got nothing to be afraid of" however this argument is weak. One only has to consider the idea of installing a camera in their bathroom to figure out that every Australian citizen actually has a large amount of legal activity they would want to hide.

Privacy is a real concern, and allowing a back-door into communications opens that same door up for potential use by ransom-ware attackers, revenge porn culprits, fraudsters, advanced persistent threat (APT) groups, and other malicious actors.

5) It's not needed & ineffective

50 years ago, before the internet was created, criminals would meet and communicate in places that police did not have access to intercept communications either, yet somehow crime was solved. The situation where law enforcement is allegedly "going dark" is not something new, it's just a "return to the norm". In fact, the access that law enforcement has had over the last 10-20 years has been unprecedented.

Given this unprecedented level of communications access, it really should have resulted in a huge drop in the crime rate. However, this has not happened as per the below publication:
https://aic.gov.au/publications/tandi/tandi359

This history suggests that expanded or reduced access to communications is in no way certain to have any serious impact in the the crime rate.

6) Proper public consultation and discussion has not taken place

The Bill went through a brief public consultation process in which 15,000

submissions were received. Around a week after the public submissions closed, the Bill was introduced to the House of Representatives with almost no changes. Given the amount of public submissions, it is beyond belief that all 15,000 submissions could have been read, let alone considered. The Bill should be withdrawn so that a public discussion can be had around the implications of the bill and how effective it will really be, as I believe this has not happened to a suitable degree during the formulation of the Bill as it stands.

I am happy to provide further detail on any of the above if needed.

Thank you.