To whom it may concern,

I am writing to submit comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in regards to a review being conducted on the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 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 and a half years been working for a large multinational cloud software vendor. My role at the company involves developing web-based 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 and practicality of the technical demands placed on companies by this Act.
- The Act 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 absolutely a backdoor

Throughout the extremely brief public process, Australian citizens were told by the government that the Bill is not intended to allow introduction of backdoors into computer systems.

Another intention of this law is to allow police and security agencies access to the content of encrypted communications, which they are denied access to due to the system's security features.

Here are some commonly accepted definitions of what a backdoor is:

> *a "deliberate and hidden weakness in a system that is designed to allow*

certain people to bypass the security of the system".
https://blog.1password.com/does-australias-access-and-assistance-law-impact-1password/

"a method [...] of bypassing [...] encryption in a computer system"
"Backdoors are often used for [...] obtaining access to plaintext in cryptographic systems."
https://en.wikipedia.org/wiki/Backdoor_(computing)

Given these definitions, it clearly puts the dual intentions of the Act into conflict. The Act should be immediately repealed until a suitable replacement Bill can be passed which satisfies both intentions.

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 will 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 Act 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 Act, 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."

Given the intentions of this law is to allow police and security agencies access to serious criminals (e.g. terrorists) encrypted communications, any "serious" criminal would have learnt the above lesson already and will have already shunned digital devices in favour of

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 Heartbleed 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 requires Australian companies, and companies operating in Australia to deviate from international best practices & design patterns opens 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.

Furthermore, if a member of the research community was to find a vulnerability, the process for reporting that could be treacherous as it's illegal to reveal the existence of a capability introduced as a result of a Technical Capability Notice. This will have a chilling effect on the security research community in Australia, and will lead to a vulnerable state for the nation's public and private cyber infrastructure.

Recommendation: The secrecy provisions in the Act must be removed.

This will allow white hat hackers and bug bounties to continue to operate and find flaws in the software, and point them out to the developers so that they can be closed before they are exploited by cyber criminals.

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 will 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) It is likely to decrease the quality of life of Australian citizens

The Brazilian government has had run-ins with WhatsApp in the past related to encryption. It has actually lead to the service being blocked in Brazil three times since December 2015, due to their unwillingness to change their product to allow surveillance of their users by the Brazilian government.
https://www.digitaltrends.com/mobile/whatsapp-brazil-6-million-facebook-cash-frozen-1467391510-2

Brazil has 211 million people living in it, Australia has 25 million people living in it. Australia is insignificant to WhatsApp (and other tech companies), when compared to Brazil. Yet WhatsApp was willing to sacrifice their business in Brazil to ensure the security of their users.

It is without a doubt that multiple tech companies will stop offering products and services, and choose not to expand in Australia given the introduction of this Act.

7) Government officials and intelligence agencies have been deceptive

A common statistic thrown about through the media by the government and intelligence agencies is that "About 95 per cent of people currently being surveilled by security agencies are using encrypted messages".
https://www.news.com.au/technology/online/security/inprinciple-deal-struck-on-controversial-encryption-bill/news-story/75492c0ee5a389a0ada7955733529af4

This is a very deceptive and misleading statistic. I'm sure that almost 100% of the people being surveilled also drive cars, and eat at McDonalds. Given the pervasiveness of WhatsApp throughout Australia (and thus encryption), I feel sorry for the other 5% as they must have no friends at all!

Correlation does not mean causation, and similar to banning people from driving cars because terrorists use them, it is unproven whether allowing access to encrypted communications will have any benefit at all. As outlined in point 5, expanded or reduced access to communications is in no way certain to have any serious impact in the the crime rate.

Furthermore, the citizens of Australia were told that the Act was apparently needed immediately to ensure they are safe over the Christmas break. Given the considerable consultation period, and the time it would take to code, test, and deploy a backdoor into an encrypted service, there is absolutely no way that it would be of benefit over the Christmas break and thus the premise for these laws being rushed through was baseless.

Lastly, a common statement by the government and police and intelligence agencies is that they used to have access to SMS and phone call tapping, so why shouldn't they have access to those same things just because they are encrypted? To equate SMS and phone call tapping to having backdoor access to a device you carry with you 24/7 with in built GPS, microphone, camera, contacts list, password store, bank logins, and inner thoughts, is absolutely despicable.

8) Modern software development practices are incompatible with the secrecy provisions

A company/individual that receives a Technical Capability Notice (TCN) must keep it a secret, and it is a crime to reveal the existence of such a notice.

Modern tech companies have global teams responsible for developing software. Companies which are exclusively Australian will have no problem complying with the above requirement. However, for international companies this will be impossible. The reason being is that for modern software development generally there is a central code repository which contains all the source code for the application/service. This can be accessed by all. For a company with 1000 developers, all located around the world, it would be impossible to ensure that any code changes to allow such a capability to be used be kept secret.

Recommendation: The secrecy provisions in the Act must be removed.

If a company/individual receives a TCN. This will ensure that Australian citizens receiving a TCN are not stuck in the treacherous position of having to implement a capability directed in the TCN, but also having to keep it secret, even though modern software processes require the capability be published within the company.

9) 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.

Furthermore, amendments were made to the Bill overnight prior to them being voted through the Senate, with absolutely no public consultation and no consideration by industry done on the amendments.

—

Given the above points, and the absolutely farcical process that lead to this Act ascending, I strongly decry it, and demand that the committee recommend that it be repealed until a proper, community wide discussion & consultative process can be had.

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

Thank you.