I am writing to express my concerns with various aspects of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill which are extremely problematic. I provided a submission to the original committee, however due to an oversight I did not make it public (by default all submissions were private unless you opted in to make it public via email after submitting). Thus, there is some crossover between my original submission, but it has been updated in response to the final passed legislation.

For some context, I have a Ph.D. in computer science, I have over a decade of experience as a software engineer, and I currently work as a researcher and lecturer in the Faculty of IT at Monash University. For many of my years in this industry, I've also been a contributor to free software projects which focus strongly on personal security, anonymity, and privacy. Despite what some may say, these tools are not designed for criminals. Rather, they are designed for any person looking to protect their communications and personal data from unjust intrusion, interception, and monitoring. Such people may be an average citizen looking to affirm their rights, or an activist, journalist or humanitarian organization looking to safeguard their work in this age of perilous global communication.

Let me start by saying that the discourse around this entire process, the idea of gaining access to communications when both their originator and the telecommunications provider intends for them to be private, is very concerning. Both from a technical perspective and also from a civil liberties perspective.

However, during this submission, I'd like to talk specifically about:

- How these laws will be ineffective in achieving their goals.
- The distrust that this legislation will seed in our technological infrastructure.
- The way in which the legislation makes Australian IT companies uncompetitive on the world stage.
- The process of passing the legislation first and then reviewing afterwards.
- Issues with specific provisions in the legislation.

The nature of many free software projects is such that the current legislation would be ineffective at obtaining the contents of encrypted communications from individuals who choose to use them. There are several reasons for this. Firstly, they are often decentralized and not managed by any organisation. Secondly, their distribution channels ensure that not only is every user confident that they have the original version of the software unmodified from any TCN requests, but also that the source code for such applications can be inspected. Any changes in response to a TCN would result in people being made aware of this and choosing not to use the app any more.

As such, I am not writing from the perspective of somebody worried that this legislation will disrupt the great work done by activists, journalists, and humanitarian organisations around the world working to ensure their protection and privacy. Rather, I am writing because this legislation has some other broad reaching consequences which are unintended, but real and important.

Firstly, I'd like to discuss the idea that what this (and other similar) legislation is doing is just the same as what we have always had, with regards to the ability to tap phone lines. It is certainly true that the rise in online encrypted communication has reduced the ability of police agencies to access communications. However, it is also true that a hugely significant amount of our lives are now conducted using these same online tools, far more than in the past when only landline phones were available. Not only this, but it is also happening at a younger and younger age. Our younger generations will conduct a significant proportion of all of their communication within their social networks in an online environment, often using encrypted communication technologies such as WhatsApp as the younger generation is increasingly becoming more privacy aware.

Thus, it is absolutely **not** the case that this legislation is restoring the ability that police had in the past. It is far broader, simply because so much more of our life is done using modern internet-enabled communication technologies.

One may claim that the government previously had the right to listen in on communications (subject to a warrant), however, when talking about modern internet communication, I don't think the government can claim the same right. Trying to claim this not only causes the population to become complacent about their own privacy and security online but also sets a terrible precedent for other, more untoward governments who wish to justify more broad-reaching surveillance strategies on their citizens. Australia is obviously a very stable democracy, and I am not concerned that the (current) government will abuse these laws to target political enemies. However, we have a responsibility to establish best practice as other countries look to us to set an example. If we enact legislation saying that it is okay to legally request access to encrypted communication, then other more malicious governments will be able to claim the same thing. When these governments enact similar legislation though, it doesn't just result in angry letters or fear of lost jobs as it does in Australia, but rather journalists and activists being imprisoned or executed.

Secondly, I'd like to talk about the technical details of a TCN, and its impact on secure distribution and supply chains. The legislation makes it very clear that a TCN is not allowed to break, weaken, or remove any encryption which is already in place, or introduce systematic weaknesses or vulnerabilities. This is positive because it gives end users confidence that they are not doing business or communicating in a way which may be accessed by nefarious parties. Instead, it effectively forces companies to find other ways to access communications when served with a TCN. Given my experience in this field, the **only** way to do this for modern, end-to-end encrypted channels, is for the apps themselves to access communications **before** they are encrypted, e.g. within the communication app itself, or via higher level tools such as keyloggers. This means that although users of communication services can be confident that their communication is encrypted as anticipated, no user can be sure that their specific operating system/app/account has not been tampered with in response to a TCN. The end result is that although 317ZG prevents mistrust in the encryption ecosystem (as intended), it has now introduced the same level of mistrust in the supply chain, as each user no longer has any ability to be assured that their specific communications are encrypted as they expected (which is unintended and undesirable).

There have also been many claims from local engineers in the IT sector worried about uncertainty with regards to their individual employment or the international success of Australian companies due to this legislation. This is regularly brushed aside by policy makers as trying to introduce fear, uncertainty, and doubt. However, this is the same government which brought into being the Telecommunications Sector Security Reforms which are the reason that the Chinese company Huawei is unable to be involved in a 5G rollout across the country. The TSSR specifically prevents companies which are likely to be susceptible to coercion by foreign governments from taking part in critical infrastructure projects. This is quite similar to what the Australian IT sector faces now when quoting for important jobs in other jurisdictions, as a direct consequence of this legislation. They will face questions about whether or not the Australian security agencies will be able to compel the company to provide access to some of their encrypted communications – and their answer will now have to be "yes" - jeopardising their ability to be competitive on the world stage.

Another aspect of this legislation is that there is a huge amount of uncertainty in the IT sector with regards to many aspects of the bill. For example, a list of over 100 unanswered questions from those in the IT sector is available at https://github.com/alfiedotwtf/AABillFAQ#unsorted-and-unanswered-questions.

Perhaps one of the most glaring issues with this legislation is that it wont help to capture encrypted communications of those who don't want to be caught. There are many freely available communication tools (e.g. Signal / Telegram / Briar Project - to name just a few) which are built by communities of people around the world, and which are specifically designed to be resilient against this type of government interference. If somebody wants to avoid being impacted by this legislation, they need only use one of these decentralised tools which are beyond the reach of this legislation, both technically and legally. As a result, we will be in a situation where most of the law abiding citizens will now be more vulnerable when using their everyday communication apps such as WhatsApp (see my paragraph on "backdoors" above), but the worst criminals seeking to avoid surveillance will still be able to do that without any difficulty whatsoever.

I'd also like to take a step out of my area of expertise to comment on the process of drafting, consulting on, amending, and then passing this this legislation. I would describe the process as farcical, if it wasn't so troubling. While I acknowledge it is not the job of consultation periods to simply count the submissions for or against a policy, I will say that the sheer number and depth of concerned submissions shown from those in the tech sector (including myself) and other areas was staggering. I don't feel that the result of this consultation process reflects the best advice made available to the parliament during this consultation period. The actual timeline of the legislation is equally troubling. There was a lot of discussion about the legislation for quite some time, even back to 2017. However, we were not provided any draft legislation to comment on until the 300 page bill came before parliament, where we were offered a 3 week window to consult. Once the consultation period closed, the PJCIS began a review. In December 2018, the Home Affairs Minister reportedly wrote to the committee asking them to speed up their review of the legislation – something which I feel politicians should not be doing when a committee is doing their best to respond to genuine community concern. Finally, the time between when the legislation was amended, then put to parliament for a vote was only a matter of days or perhaps a week. This did not provide time for anyone to be able to read and understand the amendments, then discuss with their local members prior to them voting on the legislation. The cream on this farcical cake is that that the parliament seemingly passed the bill knowing that there are flaws in the legislation which require amendment. This is evidenced by Labor's promise to amend the legislation in 2019, and reported assurances from the Liberal/National party that they would help Labor to pass some amendments. This is absolutely **not** the way I'd like to see legislation drafted and passed, and sets an extremely troubling precedent for any legislation before parliament in the future.

Although not a lawyer, I did my best to read the legislation and to understand the specifics. Some of my comments about specific provisions are outlined below.

Regarding 317T (5) and 317T (6), the section allows for the minister to extend the things which companies must do to comply with a TCN. However, when discussing all of the things the minister must take into consideration, it doesn't mention anything about the privacy or liberties of the Australian people (or other people for that matter, as this legislation has global consequences). This is of grave concern to me, especially given that most of the time I see members of parliament talking about this type of legislation which finely balances our liberties and privacy against the ability to undertake effective law enforcement, the press conferences usually contain a police/security official, but don't include people who advocate for liberty and privacy. Enshrining this imbalance in legislation is not a step I'm happy to see our parliament take.

Regarding 317U, we will now have a situation where the law enforcement agencies or the minister will be dictating how we as an industry write our software. Software is a very difficult thing to get right, as is evidenced by so many recent security and privacy breaches both government and commercial. Having to serve two masters, the users of our software and technical capability notices from the government, will make this even more difficult. Especially given the nature of TCNs, where the goal is to provide access to things that many companies are intentionally trying to protect in order to preserve privacy and protect themselves from hackers.

Regarding 317V, and with the utmost respect, I don't think the Attorney General is the right person to make a judgment about whether or not a particular modification to a piece of software is practical or technically feasible. Within the industry, even the most experienced engineers are often unable to make this judgment, and making an incorrect decision often leads to catastrophic problems, such as security issues, privacy breaches, or the inability of a software product to function as intended (and hence the inability of a business to function effectively). Even with the best advice from the brightest technical experts, someone external to a software company (i.e. the Attorney General) is always ill-equipped to be able to make such judgements, and always will be.

As with others who have submitted to this committee, my recommendation is to repeal the act completely given the number and severity of flaws, and also given the undemocratic process with which it passed parliament.

Yours sincerely,
Dr Peter Serwylo.