From: [redacted]
To: Assistance Bill Consultation
Subject: The Assistance and Access Bill 2018
Date: Monday, 10 September 2018 10:23:24 PM

To whom it may concern:

I, like many technical experts in Australia, am concerned by the implications of the drafted Assistance and Access Bill 2018.

I strongly believe that this type of legislation is overtly simplified and lacks a basic awareness of some of its wider implications.

I would like to echo the concern raised by some of my friends at Atlassian that this bill will cause doubt and damage to Australian software and hardware. In the same way that Huawei is currently considered an easily compromised organisation, so will Australian software be considered by others. This would directly impact our nascent startup icons, such as my peers at Airwallex (who recently raised > $108M).

Additionally, the idea that a weakness could be safely implemented to be used only by authorised individuals is, at best, laughable. There are countless examples of hackers exploiting weaknesses that were inadvertently introduced, let alone those that are introduced deliberately. I am familiar with PKI techniques and cannot see how this could provide an adequate solution to these problems and are easily defeated and keys rapidly leaked (see DeCSS). I can easily see a jealous husband using these weaknesses and tools against a spouse to prevent her seeking help or preparations to leave, or perhaps just finding another reason to beat her. As you are no doubt aware this is one of the most significant social issues today and in my mind greatly out weights the somewhat overblown example of authorities not being able to prove a paedophile breached the conditions of his parole by texting a teen.

Due to the fact the fundamental mathematics of cryptography cannot be defeated, it will be trivial for criminals to avoid applications which have an obligation to collaborate with the Australian authorities and simply utilise non-commercial and hobbyist authored alternatives. For example, the proliferation of torrents after the shutdown of illegal content on napster. I repeat: this legislation will not have the intended effect, and will simply drive awareness of the ease of compromise and thus encourage criminals to be more aware of their communication mechanisms.

Finally, without transparent and rigorous oversight, this capability will be easily abused (see the multitude of misuses of the LEAP database), with much more insidious consequences than simple disclosure of personal details.

To summarise, this legislation and the proposed introduction of weakening of standard security measures:

- Will be ineffectual at meeting its intended goals;
- Is assured of compromise and use by unauthorised actors;
- Will irrevocably damage the Australian Software and Hardware industry;
- Be misused by authorised individuals;

This is an unfathomable compromise to the foundations of a modern, connected society and as this will affect all Australians, must be recognised as misguided, deeply flawed and abandoned in entirety.