From:	Ryan Christensen
To:	Assistance Bill Consultation; [redacted]
Subject:	Submission regarding The Assistance and Access Bill 2018
Date:	Monday, 10 September 2018 10:59:48 PM

To the Minister for Home Affairs, the Department of Home Affairs, and Trent Zimmerman MP.

I am a software engineer from the electorate of North Sydney, working for a statutory body within the NSW Government and I wish to voice my strong concerns to you about the proposed Assistance and Access Bill 2018.

As I understand it, the bill seeks to give government and various agencies the power to require communications providers to provide assistance and access to encrypted data.

To be concise, it is literally impossible to ask carriers and technology firms to assist in providing access to end-to-end encrypted data without fundamentally weakening it.

Granted, there are cases where companies can and do hold the keys for encrypted data stored at rest, i.e. data not in transit. Such data is often that stored in some personal cloud backups, like iCloud or Google Drive.

This is not where my concern lies, as the companies running these services have made it clear that they hold the keys to data stored on their servers and thus can be asked to decrypt it if asked by law enforcement. In fact we know that companies like Apple have in fact complied with law enforcement in the past to decrypt data stored at rest on their servers. What does concern me is the powers this bill gives to government and it's agencies to compel technology manufacturers and software developers to develop "backdoors" into end to end encryption. I have read the bill and I do make note of section 317ZG which states that agencies cannot ask a communications provider to create a systemic weakness or "backdoor". However interception or decryption of in transit data - such as HTTPS website data, or even messages sent over Apple iMessage, Wickr or any similar app - must require a systemic weakening of the security of those systems. End to end encryption is by its very definition end to end, the manufacturers do not hold the keys, and in most cases the keys are generated dynamically and privately.

This is the same technology that keeps HTTPS websites secure, including our internet banking, shopping and web searches. These technologies use advanced mathematics to allow the sender and receiver to negotiate a secret key to encrypt and decrypt messages in a way that even if the negotiations are intercepted there is no way to determine what the key may be.

What this means is that to intercept these messages the only means is to fundamentally weaken the entire system in a way that allows everyone to exploit it, not just law enforcement.

The only alternatives are for agencies to ask for communications providers to cease use of end to end encryption, exposing all of our web traffic to criminals and hackers; or for communications providers to provide a method for accessing the data once it has been decrypted by the senders/receivers; which is the definition of a backdoor. In all cases the security of the data is fundamentally weakened, just at different stages of data transmission and storage.

Additionally, being an employee in an independent state government body focused on the justice system, I am concerned at the lack of independent and judicial oversight in the bill. I find concerning the fact that the powers to request access and assistance to the degree stipulated by the bill rest with the Ministry. These powers, however much I disagree with them, if implemented at all should only rest with the judiciary in order for the process to be even remotely trustworthy.

As much as I respect the Minister for Home Affairs and the Attorney-General, they are not software engineers, or mathematicians, and nor are they information security experts. These areas must be well understood in order to grasp what is at stake when we talk about "assistance and access" to encrypted information.

I sincerely ask that the Minister and the Government reconsider introducing this bill. It is not in the interest of national security to weaken the technologies that keep our most personal information safe.

Best Regards,
Ryan Christensen.