From:	Quentin Zervaas
To:	Assistance Bill Consultation
Subject:	Assistance Bill Feedback
Date:	Wednesday, 5 September 2018 2:02:29 PM

Hello,

Weakening encryption and removing my ability to use end-to-end encryption is a bad idea, and one I strongly oppose.

My private conversations are private, and not for the government to decide they want to read.

Let's assume this is all in good faith and with the best of intentions:

1) There are plenty of examples of bad actors both in government and law enforcement (not to mention hackers/Russians/etc..), and I worry that people will be able to access my private conversations.

2) The government and its departments have shown a high level of incompetence and indifference to issues relating to technology (Ongoing NBN debacle, census fail, ATO hard drive issues, MyHealthRecord privacy issues, the list goes on...). Also, there are numerous examples of police accessing the "mandatory data retention" browsing history data that shouldn't.

You guys (govt) have a terrible I.T. track record, and what you're proposing to do is REALLY difficult. Simply put: you don't have the skills or knowledge. Even the top tech companies in the world - who actually do have the skills - struggle massively with data security. Forcing them to weaken their systems is complete madness.

The whole thing is a weak straw-man argument for lazy law enforcement and lazy policies. The stupidity of the whole thing is that it only impacts law-abiding citizens.

It is SUPER EASY to download encryption software (and/or source code) online and communicate securely, despite whatever the law may state.

So all that ends up happening is, if so-called terrorists want to communicate, they'll stop using the tools provide by mainstream providers (such Apple's iMessage), and instead use their own software. Encryption is just a bunch of clever mathematical formulae concocted by the smartest people in the world and published for all to use, so it's pretty easy to write your own software.

Hence, it only punishes the people (and exposes them to warrantless snooping) that aren't doing anything wrong.

One other note: The example published on your web site from Victoria Police is complete and utter nonsense. The system failed on so many levels before it got the stated issue. These are the same super-weak arguments that get trotted out every time the government wants to ram through some bad legislation in its ongoing pursuit of total control.

Please do not proceed with this nonsense. It will not help, but it will make many things worse.

I'm a software engineer with 20+ years of experience. I'm happy to discuss this further and provide further feedback.

Thanks

Quentin Zervaas
[redacted]