From: Paul Bone
To: Assistance Bill Consultation
Cc: Peter Khalil
Subject: Access
Date: Monday, 10 September 2018 10:48:23 PM

To those involved with the proposed Assistance and Access Bill, and also my local MP, Peter Khalil.

I'm writing with regard to the proposed Assistance and Access Bill.

Overall I'm unhappy with any legislation that limits access to encryption. A good summary is in this video, which I'm sure you've seen by now.

https://www.youtube.com/watch?v=eW-OMR-iWOE

I'd also like to share some specific thoughts, but first my credentials. I'm Doctor Paul Bone (PhD). My doctorate is in Computer Science, and although my thesis is unrelated to networking this _is_ something that I have experience with. I learnt my first computer language when I was 12, maybe 11, my first job was as a systems administrator while I was 17 and still in school. I worked on fiance software and my specialisation & doctorate is in computer programming languages and optimisation (making code faster). I now work for Mozilla, the non-profit behind the Firefox web browser, software installed on millions of computers that MUST remain secure for the safety of millions of internet users. (I am not writing on behalf of Mozilla, I will encourage our legal and PR teams to respond separately.)

I understand the claimed need for such a bill, and honestly I have no experience in fighting terrorism. However legalisation like this limits people's freedoms online and will in practice do little to help fight terrorism.

My main concern (although I object to the bill as a whole) is the "technical assistance notice" and "technical capability notice". These can require communications providers to "removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider" and many other "Listed acts or things" (317E). These limit people's access to encrypted services. Services that we all agree are important to protect our personal information, from baking to business deals.

This will not limit criminals' access to encryption. Criminals will be able to switch services endlessly always using those that provide encryption, or using one of the many thousands of end-to-end encryption products (which cannot be accessed by strong-arming a provider). This law also requires providers of end-to-end encryption products to comply. However that software is already available freely.

Software, algorithms and knowledge that is already widely available will always be widely available. I know this act doesn't make this software illegal, even if it did it would not be able to prevent a black market from developing. In fact online, making something illegal or asking people not to share it, often makes it more popular to share, as Barbra Streisand would know (https://en.wikipedia.org/wiki/Streisand_effect).
One example of this
is during the 90s when the USA classed strong encryption algorithms as munitions, and therefore they were illegal to export. Algorithms developed within the USA were illegally exported, some were even printed as designs on

t-shirts, using a legal loophole since t-shirts may be exported.

I am not re-assured by the limitations placed in the proposed Act. I am pleased that warrants are required (just as they would be to search someone's home). But I do not trust the current government of Australia to use these kinds of powers, and if I did, I cannot be sure that I will always trust the government (governments change).

I'm sorry I didn't have time to make my message more coherent and brief, but I only learnt today about this and that the deadline for responses is tonight. I'll summarise:

* The act limits peoples' freedoms
* It may be abused
* It won't be affective in catching criminals using end-to-end encryption
* There will always be a "black" market for software and algorithms that do support strong encryption.

Thank you for your time.

Dr Paul Bone