From: Nicholas Watts
To: Assistance Bill Consultation
Subject: Submission to consultation on the Assistance and Access Bill 2018
Date: Wednesday, 5 September 2018 10:26:02 AM

Dear Minister

I'm writing to try and provide you with some professional context for 'The Assistance and Access Bill 2018' before it is voted on. As a software engineer and cryptography enthusiast myself, I think it's important that you understand (a) what can and cannot be achieved by legislation; and (b) what the cost of such legislation will be.

First, it is physically impossible for law enforcement agencies to decrypt all suspicious communications that they might encounter. No piece of legislation can change this. Even if Apple, Microsoft, Google, Amazon and Facebook all jointly agreed to complete cooperation with each other and with the wishes of the government, they would still not be able to bring this about. This is because the technology for securely encrypting messages is widely available, broadly distributed and easy to use. People who wish to share securely-encrypted messages are NOT dependent on any large tech companies to provide them with this service. The software they need in order to do this is freely available and easy to install. In a few minutes, anyone can download the same software that Edward Snowden used to ex-filtrate data from the NSA. The standard, open-source encryption-decryption tools can be easily accessed through a smartphone. For the extra-paranoid, private individuals can even purchase a laptop TODAY that only runs software they have compiled for themselves from source code, so that no "back doors" are even possible. They can then run freely-available encryption-decryption software on this machine to give them total privacy when sending messages around.

What does this mean? It means that you can't stop people sending private messages if they really want to. The only people who are likely to have their mail read by the over-reaching powers of this legislation are regular people who aren't worried about security. You will give law-enforcement the power to snoop on people's personal lives, but they will still not be able read anything that someone has put even a small amount of effort into keeping private.

So then, this bill CAN give the government the power to invade the freedom and privacy of law-abiding citizens. But it CANNOT give the government the power to read messages of anyone who wants to keep their messaging private, and who has done 15 minutes of research on google (or knows someone who has).

In terms of cost, this bill will significantly damage consumer confidence in large technology companies , and thereby make those companies likely to diminish their business dealings and expansion within Australia. Remember, it is the normal consumers who will be affected by these invasions of privacy, but they will not stop anyone genuinely trying to cover their tracks, so that only the consumers will be negatively affected. This will stymie a key sector for economic growth in Australia (tech and big data). That means less jobs, less revenue, and disgruntled voters.

I myself have drawn up product plans for a start-up company in the cryptography-for-business space. But if the Australian government is going to compel me to compromise my customers' data, I would be forced to either migrate to another country or to sell that business to a foreigner in order to retain the customers' trust.

I hope this has shown you that this bill cannot deliver what is promised, and will hurt our

tech economy. Thank you for your consideration.

Nicholas Watts
[redacted]