From: Lindsay Gaines
To: Assistance Bill Consultation
Subject: Assistance and Access Bill 2018
Date: Monday, 10 September 2018 6:23:14 PM

Good evening,

As an Australian citizen and the Technical Director of a Melbourne technology agency (https://monkii.com.au) I would like to voice my concerns and opposition to the current draft of the Assistance and Access Bill.

Despite claims to the contrary, this bill does introduce the possibility, through Technical Assistance Requests, for our government to request keyed back doors to existing communications platforms. And as a technologist, I really don't see any other way that this could work.

When communications are encrypted, they cannot be decrypted by a third party unless the third party has access to:

- an encryption key (a backdoor)
- exfiltration via the endpoint software (a backdoor)
- or the endpoint device itself, unlocked

Giving the Australian government access to either of the first two of these aspects of communications software, even with a warrant, is dangerous for several reasons.

First of all, I am not confident in the technical capabilities of every employee who may have access to these backdoors. As recently reported, almost 1500 Australian officials have "Password123" as their password (https://www.washingtonpost.com/technology/2018/08/22/western-australian-government-officials-used-password-their-password-cool-cool/).

Information security is simply not a core competency of Australian government employees, whereas it certainly is the core competency of all the myriad of attackers (private and state backed) for whom access to these backdoors would be a very valuable prize. When even the NSA can't secure their tools against advanced attackers, there is virtually no hope for our government officials to keep these backdoors only in the hands of "the good guys". It seems clear that we're creating a resource that we're almost guaranteed to be unable to protect.

So even with strict procedural controls via warrants and organisational oversight, the danger of us losing control of our tools is a serious concern.

The second key issue is simply one of future unknowns. We can all agree that better tools to go after sexual predators and criminals is a good thing. However, we can't guarantee what will be illegal in the future. I certainly hope we will never see a future government take a retrograde stance on social issues such as gay marriage, but if backdoors are put in place now to catch criminals, they can be used in the future to catch society's undesirables. I might agree with the current goals of the legislation, but I have no way of knowing whether I would agree with their use in the future.

Giving government and law enforcement this level of access into private communications of individuals is a genie that cannot be put back into the bottle. We must consider with the utmost gravity the consequences it may have to our present security, and our future

freedom.

Put simply, the impact of fringe criminals is dwarfed by the impact this would have on all Australians if we make even a single mistake.

Thank you for your time.

Lindsay Gaines