

**From:** [REDACTED]  
**To:** [Assistance Bill Consultation](#)  
**Subject:** Assistance and Access Bill Concerns  
**Date:** Monday, 3 September 2018 5:37:06 PM

---

G'Day

It is not everyday that I get involved in reading and commenting on Bills before any Parliament, or have much political input aside from voting, however I came across this Bill and did have a few objections to it.

Division 7, Para 317ZG: The term 'systemic' is fairly loose, and leaves open the option to direct 'backdoors' to be built in to parts that do not affect the whole 'system', but may/will still compromise parts. Whether or not this word selection is deliberate is a serious question, as if it is a deliberate 'wriggle' word then the Bill's drafters have set out to wilfully deceive the Australian public. It was stated on the Home Affairs page that no 'backdoors' would be created, however using imprecise language has left the door open for 'catflaps' to be created in subsystems that may be exploited by hostile cyberspace users. In the pursuit of access to information, agencies may accidentally create a path for hackers, state-sponsored or otherwise, to infiltrate the encryption of local and multi-national companies. This in itself is a huge risk. Much of today's economy depends on encryption securing and verifying transactions. Any risk to this will have global implications for businesses.

I understand the need for agencies, in particular Security Services to access criminal's information to prosecute or prevent crime. The examples listed on the Home Affairs page attest to the severity of the threat. However, accidental disclosure of encryption technology, or incidental 'backdoor' creation is too great a risk to undertake.

I am not expecting a response to this email, however please do consider the full ramifications of this law, as I'm sure you do all laws.

To our Security Services, keep up the good work protecting Australia.

Thanks very much for your time,

[REDACTED]