

**From:** Daniella Kicsak  
**To:** [Assistance Bill Consultation](#)  
**Subject:** Submission to consultation on the Assistance and Access Bill 2018  
**Date:** Friday, 7 September 2018 5:23:09 AM

---

Dear Minister,

I have previously studied networking as well as cyber-forensics & information technology. I have very strong concerns regarding the ethical issues regarding the proposed bill titled, "The Assistance and Access Bill 2018".

I understand that that as an Australian, I don't get to enjoy the vast number of privacy protections that other countries such as the United States of America offers, however we are already a nation who believes that phone tapping on the general public is considered the "norm". The incidence that is being referred to was revealed in 2013 by the Inspector-General of Intelligence and Security, Vivienne Thom, that the an undisclosed amount of wrongly targeted Australians were being monitored through their telecommunication devices. The Assistance and Access bill is proposing to give our intelligence organizations even more authority to monitor innocent every day Australians without any consequences.

What concerns me from a networking perspective is that this bill would require that we, as a member of the 'Five Eyes', is the networking backbone limitations of enforcing, "... the enforcement of the criminal laws in force in a foreign country". To my understanding regarding the draft bill, this will force international networking traffic through our tier-1 and tier-2 backbone locations which will greatly increase latency to most of the commonly used internet services in the country. Australia has spent billions of dollars attempting to create the NBN over the past decade, and I fear that re-routing the titanic quantities of international traffic through our access points will undermine any of the throughput gains we have already accomplished. The latency for relatively new technologies such as streaming media will simply become too slow to be a viable option for all Australians.

Digital encryption is a necessity in the modern age of technology. This bill threatens online communications which **MUST** be secure, such as the case with online banking and the financial sector. Weakening the encryption technologies which facilitate many Australians financial transactions is a reckless risk which will not only potentially hurt the good faith that the people have put into the government, but also democracy in the country itself. Forcing companies to up loopholes for end-to-end encryption is very potentially exploitable and should be avoided.

As a private citizen, I deplore you to consider the long lasting and reaching implications this bill will impose on the Australian public who uses and relies on internet technologies for both business and leisure on a daily basis. I don't believe that one of the remaining bastions of personal privacy is worth giving up to public organizations who already publicly abuse their abilities and powers.

Thank you.

Daniella Kicsak  
