From:	Edward Giles
To:	Assistance Bill Consultation
Subject:	Submission to consultation on the Assistance and Access Bill 2018
Date:	Wednesday, 5 September 2018 7:56:19 PM

Dear Minister,

I would like to express my concerns with the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.

The main general concern with this legislation is that it forces communications providers to work for Australian law enforcement agencies by either building a backdoor into their systems for law enforcement use, or intercepting and relaying unencrypted communication to law enforcement upon request.

A backdoor can be used by anyone who knows how to access it, and this fact and its consequences are explained better than I ever could by a video from CGP Grey on YouTube: (https://youtu.be/VPBH1eW28mo). Although the limitations in the new Amendment appear to remove the requirement of a backdoor, they might be able to be bypassed through loose interpretation of the term ‘systemic vulnerability’.

The other alternative is relaying unencrypted data to law enforcement upon request. This would require communications providers to retain unencrypted data for a period of time, ready to provide to law enforcement. If a communications provider provides end-to-end encryption, all encryption and decryption is performed on end-user devices. Only encrypted data, which even the communications provider is unable to access, passes through the networks of the communications provider, making it impossible for the provider to give law enforcement access to it without a backdoor. The Amendment would therefore make end-to-end encryption illegal.

My other concern is that even if a perfect backdoor could be opened only for Australian law enforcement, the sort of 'assistance and access' that the Amendment attempts to provide cannot be given without allowing law enforcement to violate the privacy of every Australian, while still not giving them access to encrypted communications from real criminals.

This is because cryptography is easy to do. Anyone (law-abiding or not) with the right knowledge can write a program to encrypt and decrypt any data they want, without requiring a communications provider to manage the encryption. It is therefore possible for criminals to bypass the powers granted to police by the Amendment and exchange secret communications or store secret data, without anyone else being able to decrypt it. This renders the Amendment useless for its stated objective to “enable law enforcement to effectively investigate serious crimes in the digital era.”
Thank you.

Edward Giles
[redacted]